ECE PARIS · LYON
ÉCOLE D'INGÉNIEURS

ING4 SI01

Network Security

Network Virtualization

Lab 1

Author(s):
Gabriel PADIS
Anastasia DUCHESNE

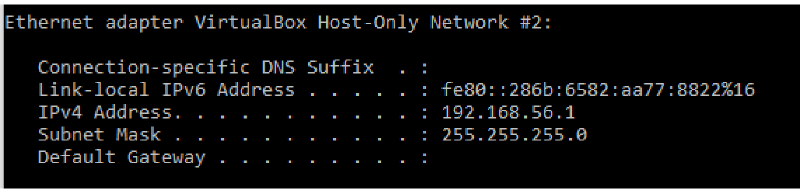
Teacher:
Mr. Nahle

Paris - Semester 7 - March 5, 2019

Contents

1 NAT mode

1.1 Host



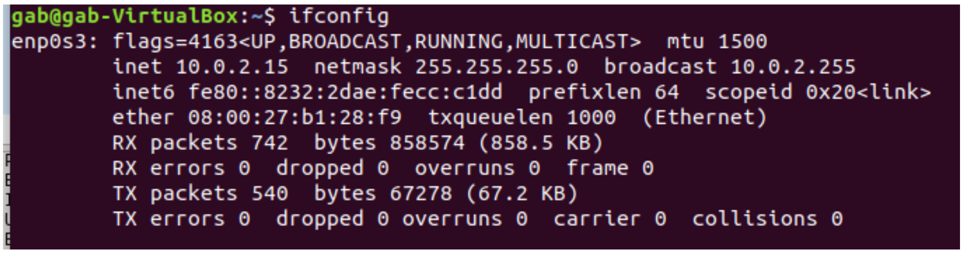
```
Ethernet adapter VirtualBox Host-Only Network #2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::286b:6582:aa77:8822%16
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

Figure 1: Host IP

The configuration of the host machine is the following :

- **IP:** 192.168.56.1
- **Netmask:** 255.255.255.0
- **Default gateway:** -

1.2 Virtual machine



```
gab@gab-VirtualBox:~$ ifconfig
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::8232:2dae:fecc:c1dd  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b1:28:f9  txqueuelen 1000  (Ethernet)
        RX packets 742  bytes 858574 (858.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 540  bytes 67278 (67.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 2: VM ip

The configuration of the virtual machine is the following :

- **IP**: 10.0.2.15
- **Netmask:** 255.255.255.0
- **Default Gatewway:** -

1.3 Conclude

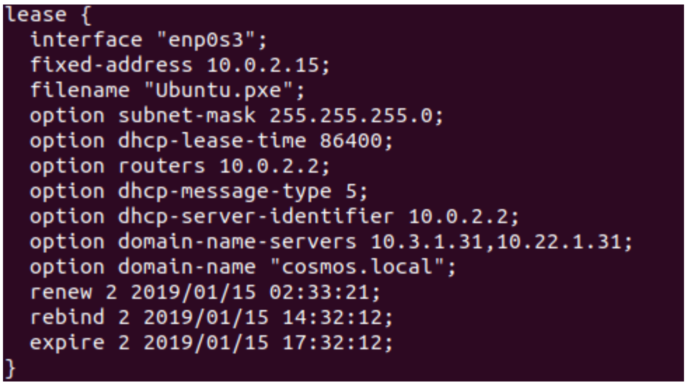
We have two different machines on two different networks. The host has the address 192.168.56.1 on the network 192.168.56.0/24. The VM has the IP address 10.0.2.15 on the network 10.0.2.0/24. The NAT network mode allows the virtual machine to access the external networks through a router. In our case, the Oracle VM VirtualBox networking engine works as the router, and connects the virtual machine to the host.

1.4 DCHP server

In order to have the DCHP server information for our VM we look into the configuration file of dhclient of our network: enp0s3.

cat /var/lib/dchp/dhclient.leases

The ip address of the dchp is on the line "option dhcp-server-identifier" which has value: 10.0.2.2

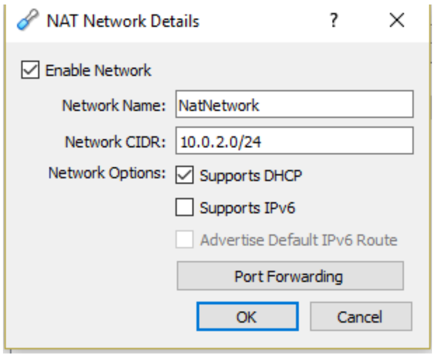


```
lease {
  interface "enp0s3";
  fixed-address 10.0.2.15;
  filename "Ubuntu.pxe";
  option subnet-mask 255.255.255.0;
  option dhcp-lease-time 86400;
  option routers 10.0.2.2;
  option dhcp-message-type 5;
  option dhcp-server-identifier 10.0.2.2;
  option domain-name-servers 10.3.1.31,10.22.1.31;
  option domain-name "cosmos.local";
  renew 2 2019/01/15 02:33:21;
  rebind 2 2019/01/15 14:32:12;
  expire 2 2019/01/15 17:32:12;
}
```

Figure 3: Host IP

1.5 NAT

We created our own NAT for this exercise and it has been assigned an IP address and network by Virtual Box.
The IP address of the NAT device is : 10.0.2.0/24



☑ Enable Network

Network Name: NatNetwork

Network CIDR: 10.0.2.0/24

Network Options: ☑ Supports DHCP

☐ Supports IPv6

☐ Advertise Default IPv6 Route

Figure 4: NAT IP

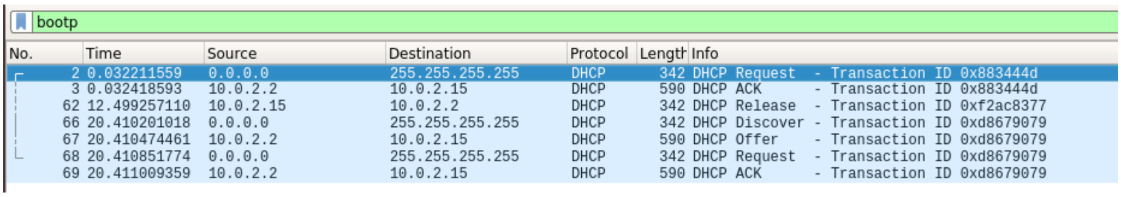
1.6 DHCP on VM

We did the following commands to stop and start again the DHCP server:

dhclient -r
dhclient enp0s3

The first one release and stop the running DHCP. The second one relaunch the enp0s3 interface which is the VM interface one the NAT.

We obtain the following DHCP packets:



bootp

No.	Time	Source	Destination	Protocol	Length	Info
2	0.032211559	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x883444d
3	0.032418593	10.0.2.2	10.0.2.15	DHCP	590	DHCP ACK - Transaction ID 0x883444d
62	12.499257110	10.0.2.15	10.0.2.2	DHCP	342	DHCP Release - Transaction ID 0xf2ac8377
66	20.410201018	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xd8679079
67	20.410474461	10.0.2.2	10.0.2.15	DHCP	590	DHCP Offer - Transaction ID 0xd8679079
68	20.410851774	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xd8679079
69	20.411009359	10.0.2.2	10.0.2.15	DHCP	590	DHCP ACK - Transaction ID 0xd8679079

Figure 5: DHCP on VM

At the beginning, the DHCP client sends a request to the server (**DHCP request**). Once the virtual machine is acknowledged (**DHCP ACK**) by the DHCP server, it asks it to release all the previous DHCP information (**DHCP Release**).

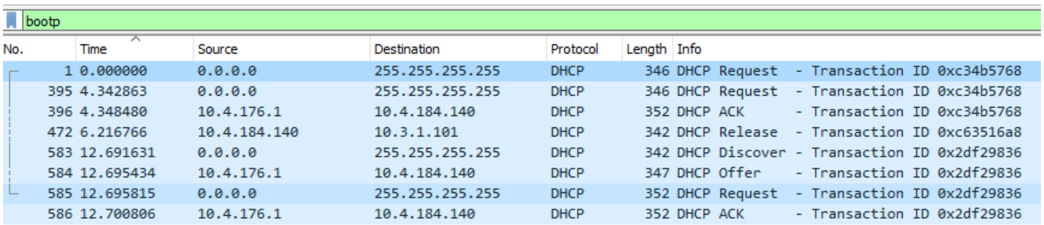
1.7 DHCP on Host

Did the following commands:

```
ipconfig /release
ipconfig /renew
```

Which is self explanatory.

We obtain the follwoing DHCP packets:



bootp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	346	DHCP Request - Transaction ID 0xc34b5768
395	4.342863	0.0.0.0	255.255.255.255	DHCP	346	DHCP Request - Transaction ID 0xc34b5768
396	4.348480	10.4.176.1	10.4.184.140	DHCP	352	DHCP ACK - Transaction ID 0xc34b5768
472	6.216766	10.4.184.140	10.3.1.101	DHCP	342	DHCP Release - Transaction ID 0xc63516a8
583	12.691631	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x2df29836
584	12.695434	10.4.176.1	10.4.184.140	DHCP	347	DHCP Offer - Transaction ID 0x2df29836
585	12.695815	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0x2df29836
586	12.700806	10.4.176.1	10.4.184.140	DHCP	352	DHCP ACK - Transaction ID 0x2df29836

Figure 6: DHCP host

1.8 DHCP sequence diagram

To assign an IP to our machines, the Dynamic Host Configuration Protocol (DHCP) goes through 4 steps.

DHCP Discover The DHCP client (our host or virtual machine) broadcasts a discovery message on the port 67, usign the limited broadcast address 255.255.255.255. It seeks for a DHCP server to assign it an IP address. The discovery message contains the MAC address of the client.

DHCP Offer When a DHCP Server receives the message from the client, if the server can respond to the lease request, it sends back a lease offer to the client on its port 68. This offer contains the IP address of the server, but also the IP address, the subnet mask and the lease duration the DHCP server is offering.

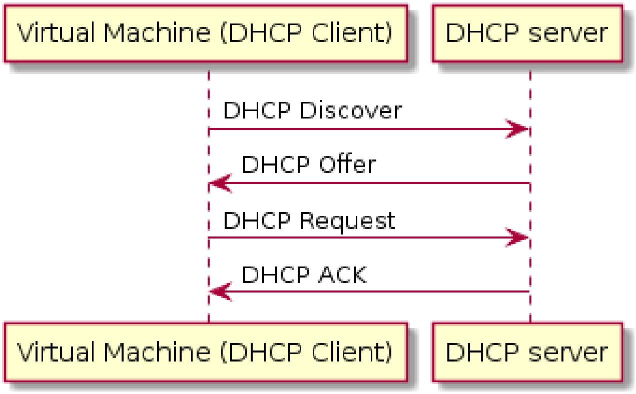


Figure 7: DHCP sequence diagram

DHCP Request The client can receive several DHCP offers. When it chooses one, it broadcasts a DHCP request message on the server using the limited broadcast address. It requests the IP address it has choosen, and informs all the others servers which offer it has accepted, this way they can withdraw theirs.

DHCP Ack The DHCP Server acknowledges that it received the request from the client. It sends back a packet to the client, which contains all the configuration information needed as the lease duration, the assigned IP address...

1.9 Visit www.oracle.com

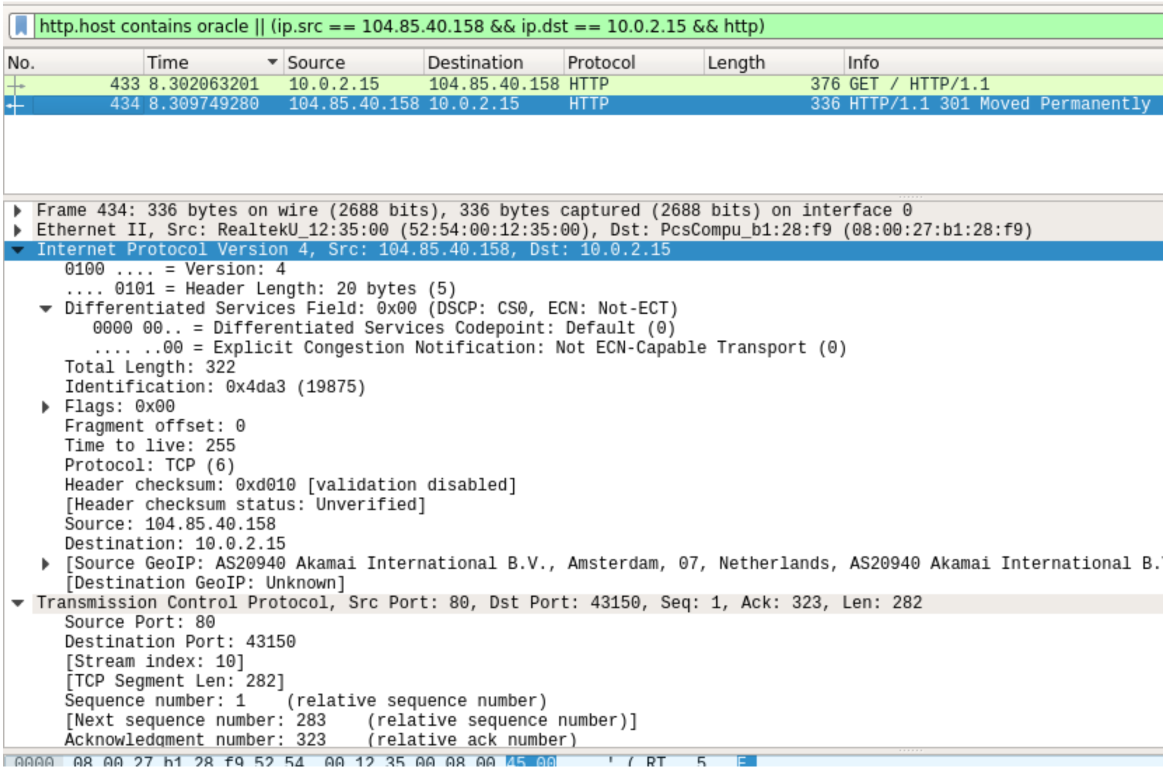
When trying to visit oracle.com from the virtual machine we succeed. It is possible to access the internet from the VM because it is connected via the NAT to the host network which makes the request to www.oracle.com, then this response is forwarded back to the NAT and then to our VM that made the request.

We filter the traffic using :

http.host contains oracle || (ip.src == 104.85.40.158 && ip.dst == 192.168.1.18 && http)

VM :

We can see here the VM making a call to the IP address 104.85.40.158, which is the one of oracle.com out of the port 80. It comes from the VM so it's ip address is 10.0.2.15 and the port it goes out of is : 43150.

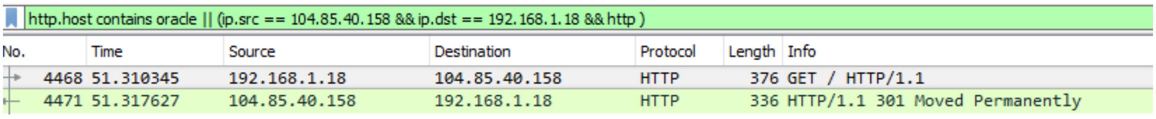


```
http.host contains oracle || (ip.src == 104.85.40.158 && ip.dst == 10.0.2.15 && http)

No.          Time            Source         Destination    Protocol       Length        Info
         433 8.302063201    10.0.2.15      104.85.40.158  HTTP                       376 GET / HTTP/1.1
         434 8.309749280    104.85.40.158  10.0.2.15      HTTP                       336 HTTP/1.1 301 Moved Permanently

▶ Frame 434: 336 bytes on wire (2688 bits), 336 bytes captured (2688 bits) on interface 0
▶ Ethernet II, Src: RealtekU_12:35:00 (52:54:00:12:35:00), Dst: PcsCompu_b1:28:f9 (08:00:27:b1:28:f9)
▼ Internet Protocol Version 4, Src: 104.85.40.158, Dst: 10.0.2.15
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 322
    Identification: 0x4da3 (19875)
  ▶ Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: TCP (6)
    Header checksum: 0xd010 [validation disabled]
    [Header checksum status: Unverified]
    Source: 104.85.40.158
    Destination: 10.0.2.15
  ▶ [Source GeoIP: AS20940 Akamai International B.V., Amsterdam, 07, Netherlands, AS20940 Akamai International B.
    [Destination GeoIP: Unknown]
▼ Transmission Control Protocol, Src Port: 80, Dst Port: 43150, Seq: 1, Ack: 323, Len: 282
    Source Port: 80
    Destination Port: 43150
    [Stream index: 10]
    [TCP Segment Len: 282]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 283    (relative sequence number)]
    Acknowledgment number: 323    (relative ack number)
0000  08 00 27 b1 28 f9 52 54  00 12 35 00 08 00 45 00     ' ( RT   5   E
```

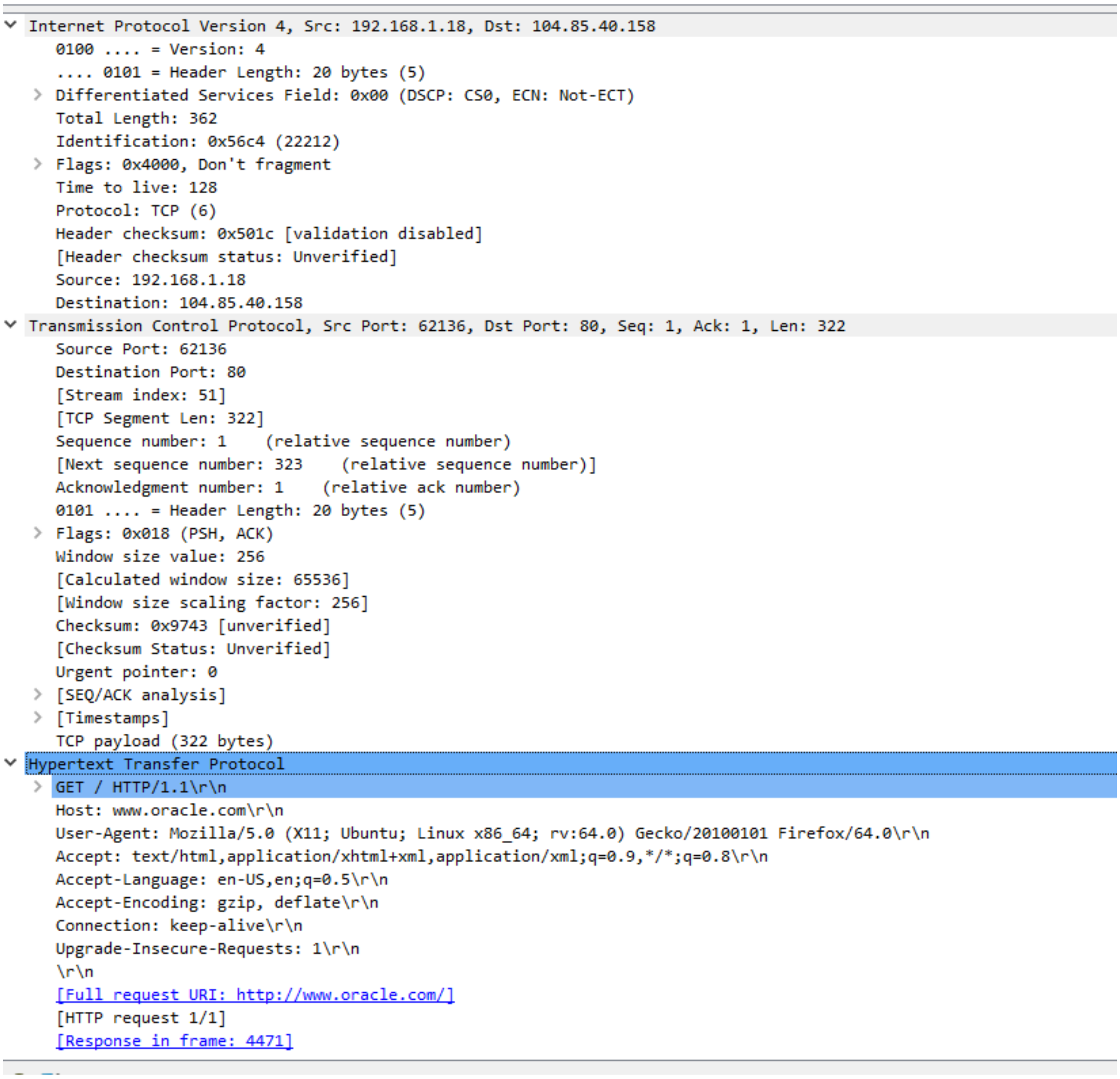
Figure 8: VM call to oracle.com

HOST:

We can see here the host making a call to the IP address 104.85.40.158, out of the port 62136.



```
http.host contains oracle || (ip.src == 104.85.40.158 && ip.dst == 192.168.1.18 && http )
No.   Time        Source          Destination     Protocol  Length Info
 4468 51.310345   192.168.1.18    104.85.40.158   HTTP         376 GET / HTTP/1.1
 4471 51.317627   104.85.40.158   192.168.1.18    HTTP         336 HTTP/1.1 301 Moved Permanently
```



```
v Internet Protocol Version 4, Src: 192.168.1.18, Dst: 104.85.40.158
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 362
    Identification: 0x56c4 (22212)
  > Flags: 0x4000, Don't fragment
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x501c [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.18
    Destination: 104.85.40.158
v Transmission Control Protocol, Src Port: 62136, Dst Port: 80, Seq: 1, Ack: 1, Len: 322
    Source Port: 62136
    Destination Port: 80
    [Stream index: 51]
    [TCP Segment Len: 322]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 323    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window size value: 256
    [Calculated window size: 65536]
    [Window size scaling factor: 256]
    Checksum: 0x9743 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
    TCP payload (322 bytes)
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: www.oracle.com\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:64.0) Gecko/20100101 Firefox/64.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://www.oracle.com/]
    [HTTP request 1/1]
    [Response in frame: 4471]
```

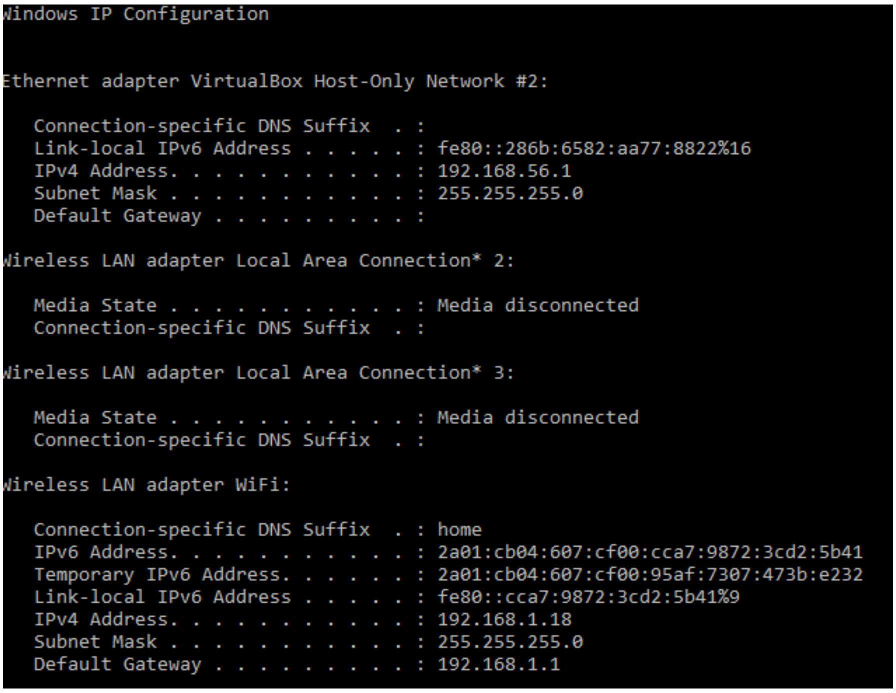
Figure 9: Host call to oracle.com

What happens in the NAT mode is that the VM makes the call but it is transmitted to the Host which is the one to make the request on another port. The response is for the Host on the port 62136 and is then transmitted to the VM on the port 43150 since it is the one that made the request for the website.

2 Host-Only mode

2.1 Host configuration

- **IP**: 192.168.56.1
- **Netmask:** 255.255.255.0
- **Default Gatewway: -**



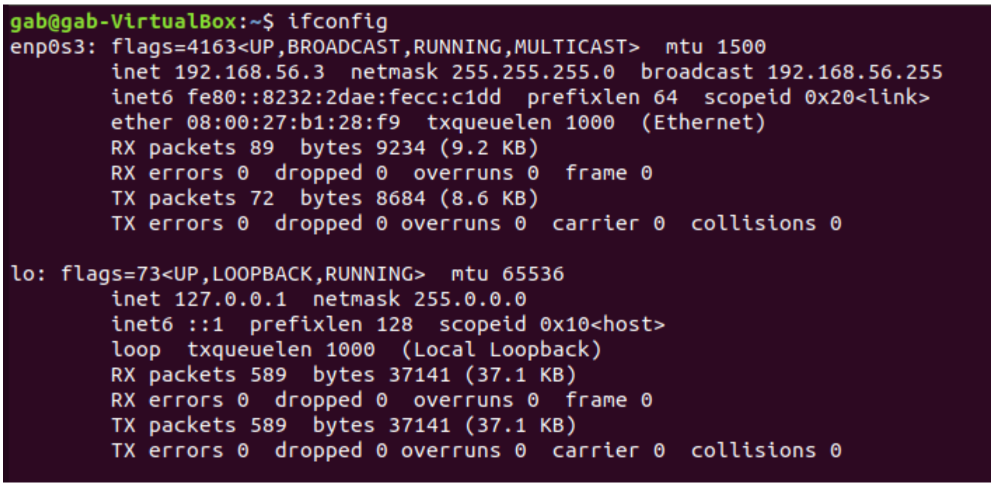
```
Windows IP Configuration


Ethernet adapter VirtualBox Host-Only Network #2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::286b:6582:aa77:8822%16
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter WiFi:

   Connection-specific DNS Suffix  . : home
   IPv6 Address. . . . . . . . . . . : 2a01:cb04:607:cf00:cca7:9872:3cd2:5b41
   Temporary IPv6 Address. . . . . . : 2a01:cb04:607:cf00:95af:7307:473b:e232
   Link-local IPv6 Address . . . . . : fe80::cca7:9872:3cd2:5b41%9
   IPv4 Address. . . . . . . . . . . : 192.168.1.18
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
```

Figure 10: Host

2.2 VM configuration

- **IP**: 192.168.56.3
- **Netmask:** 255.255.255.0
- **Default Gatewway: -**

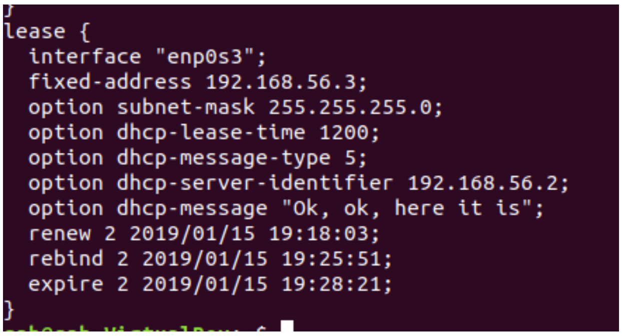
Compared to the NAT network mode, the host and virtual machines are in the same network : 192.168.56.....



```
gab@gab-VirtualBox:~$ ifconfig
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::8232:2dae:fecc:c1dd  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b1:28:f9  txqueuelen 1000  (Ethernet)
        RX packets 89  bytes 9234 (9.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 72  bytes 8684 (8.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 589  bytes 37141 (37.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 589  bytes 37141 (37.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 11: VM

2.3 DHCP



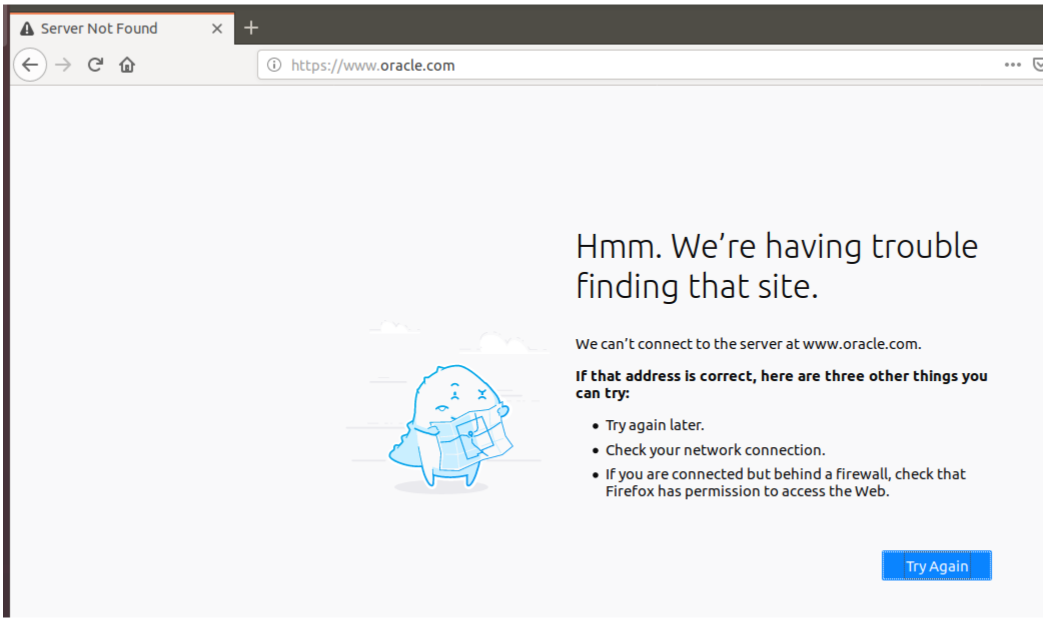
```
}
lease {
  interface "enp0s3";
  fixed-address 192.168.56.3;
  option subnet-mask 255.255.255.0;
  option dhcp-lease-time 1200;
  option dhcp-message-type 5;
  option dhcp-server-identifier 192.168.56.2;
  option dhcp-message "Ok, ok, here it is";
  renew 2 2019/01/15 19:18:03;
  rebind 2 2019/01/15 19:25:51;
  expire 2 2019/01/15 19:28:21;
}
```

Figure 12: DHCP server

2.4 Commentary and conclusion

In the host-only mode the VM is on the virtual network created by the host for the virtual machine so they can interact.

The VM is not connected to the internet since it is only on the virtual network, so it can't access www.oracle.com for example. Indeed only the host on the network can access to external networks such as Internet.



Server Not Found

https://www.oracle.com

Hmm. We're having trouble finding that site.

We can't connect to the server at www.oracle.com.

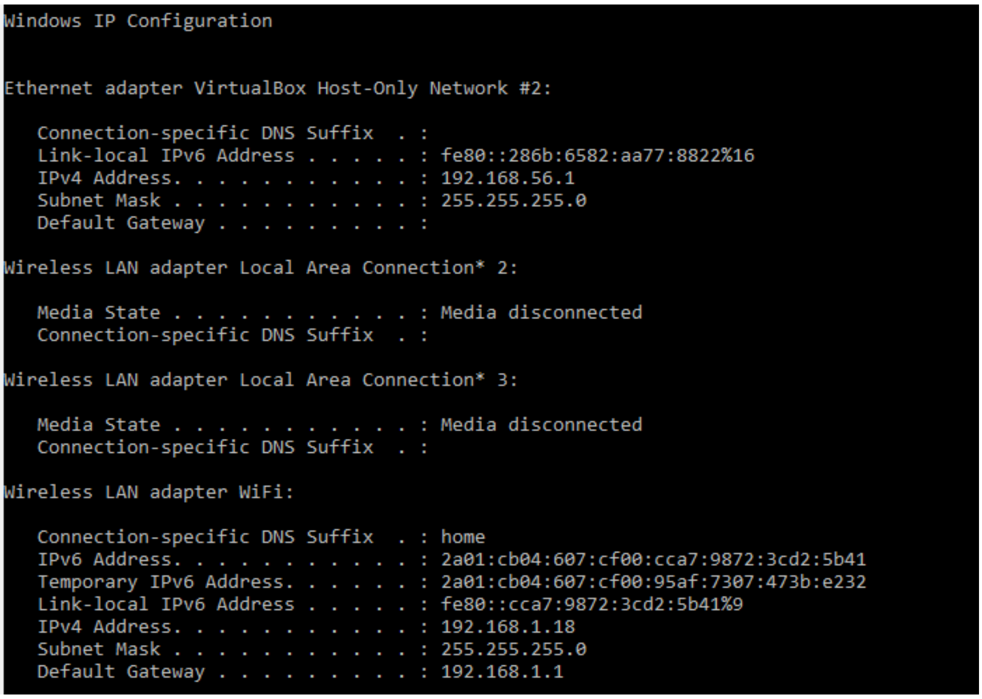
If that address is correct, here are three other things you can try:

- Try again later.
- Check your network connection.
- If you are connected but behind a firewall, check that Firefox has permission to access the Web.

3 Bridged mode

3.1 Configuration of the host machine

- **IP**: 192.168.56.1
- **Netmask:** 255.255.255.0
- **Default Gatewway:** 0

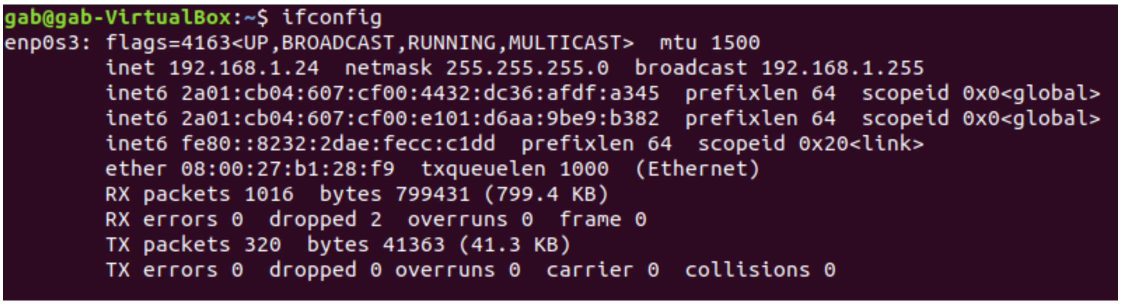


```
Windows IP Configuration


Ethernet adapter VirtualBox Host-Only Network #2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::286b:6582:aa77:8822%16
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter WiFi:

   Connection-specific DNS Suffix  . : home
   IPv6 Address. . . . . . . . . . . : 2a01:cb04:607:cf00:cca7:9872:3cd2:5b41
   Temporary IPv6 Address. . . . . . : 2a01:cb04:607:cf00:95af:7307:473b:e232
   Link-local IPv6 Address . . . . . : fe80::cca7:9872:3cd2:5b41%9
   IPv4 Address. . . . . . . . . . . : 192.168.1.18
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
```

Figure 13: Host

3.2 Configuration of the virtual machine

- **IP**: 192.168.1.24
- **Netmask:** 255.255.255.0
- **Default Gatewway:** 0



```
gab@gab-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.24  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 2a01:cb04:607:cf00:4432:dc36:afdf:a345  prefixlen 64  scopeid 0x0<global>
        inet6 2a01:cb04:607:cf00:e101:d6aa:9be9:b382  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::8232:2dae:fecc:c1dd  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b1:28:f9  txqueuelen 1000  (Ethernet)
        RX packets 1016  bytes 799431 (799.4 KB)
        RX errors 0  dropped 2  overruns 0  frame 0
        TX packets 320  bytes 41363 (41.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 14: VM

3.3 Comparison

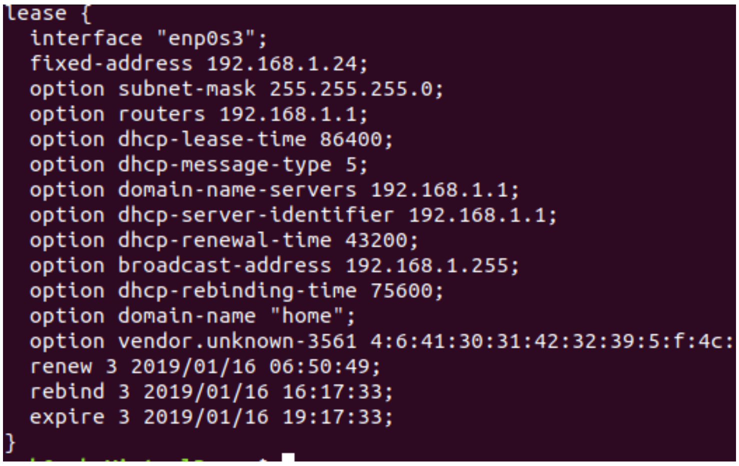
The two machines are on the same network (192.168....) so they can communicate. The bridge allows the Virtual Machine to communicate to the external world without having the need to pass by the host, because this network is directly connected to the outside world, so the VM can access oracle.com. It has the same behaviour of the NAT but in more straightforward way. Compared to the Host-Only it allows to have a internet connection.

3.4 DHCP server

The IP address of the DHCP server is : 192.168.1.1

3.5 New configuration of the host machine

The new configuration doesn't change, it is the same as the previous one.



```
lease {
  interface "enp0s3";
  fixed-address 192.168.1.24;
  option subnet-mask 255.255.255.0;
  option routers 192.168.1.1;
  option dhcp-lease-time 86400;
  option dhcp-message-type 5;
  option domain-name-servers 192.168.1.1;
  option dhcp-server-identifier 192.168.1.1;
  option dhcp-renewal-time 43200;
  option broadcast-address 192.168.1.255;
  option dhcp-rebinding-time 75600;
  option domain-name "home";
  option vendor.unknown-3561 4:6:41:30:31:42:32:39:5:f:4c:
  renew 3 2019/01/16 06:50:49;
  rebind 3 2019/01/16 16:17:33;
  expire 3 2019/01/16 19:17:33;
}
```

Figure 15: DHCP

3.6 New IP of host

The IP doesn't change, it is still 192.168.56.1.

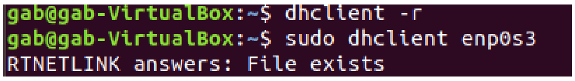
3.7 Conclusion

Even though we disconnected the machine there was no change in the ip address. The DHCP give the same address every time since it is the first one available in the list of the network.

3.8 New configuration of the VM

The new configuration of the VM is the same as the previous one. It is still 192.168.1.24.

3.9 Conclusion



```
gab@gab-VirtualBox:~$ dhclient -r
gab@gab-VirtualBox:~$ sudo dhclient enp0s3
RTNETLINK answers: File exists
```

Figure 16: DHCP lease

Even though we disconnected the machine there was no change in the ip address. The DHCP give the same address every time since it is the first one available in the list of the network.

4 TCP

TCP segments echange of data

We are the source on : 192.168.1.9 and the server on PC1 is on : 192.168.1.10 In the exchange each advertise their window size value, so their capacity.

We tell at first the server that our window size is 65535 on the first syn ack segment The server respond by saying that it's window size is 29 200. The source then update their own window size, it's value is now 32 768. This new value is less than before but it still greater then the server's one, so there's no problem and that it's fitted. This value are kept during the whole exchange here on.