Network Virtualization With Network Virtualization

Cécile Chomienne - Séverin Seux

Part 1: Bridged mode

1)

```
Carte réseau sans fil Wi-Fi :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::294c:f4c2:2c63:6f9b%26
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.1.13
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 192.168.1.1
```

2)

```
pomona@chourave: ~
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
16:51 pomona@chourave ~% ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:f0:83:f6
          inet adr:192.168.1.75  Bcast:192.168.1.255  Masque:255.255.255.0
          adr inet6: fe80::4649:c8b4:8d5c:c2bc/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Packets reçus:144 erreurs:0 :0 overruns:0 frame:0
          TX packets:157 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          Octets reçus:13935 (13.9 KB) Octets transmis:15412 (15.4 KB)
```

3)

Both host and virtual machine are on the same network 192.168.168.1/24
In bridge mode, the virtual machine has directly access to the network card of the host machine.

4)

The DHCP used is the one of the router, so the IP address of the DHCP server is 192.168.1.1.

5)

We still have 192.168.1.13.

6)

As we are working on our personal network we are the only ones asking for connection so we are given each time the same IP address. If we were at school it might not be the case because a lot of people are asking for connection.

7)

We still have 192.168.1.75.

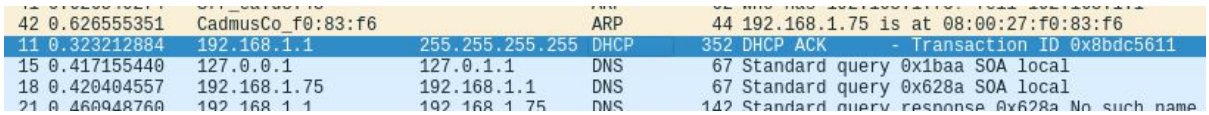
8)

As previously in question 6, we are the only ones who work on the network, so the address is not reserved by anyone else.

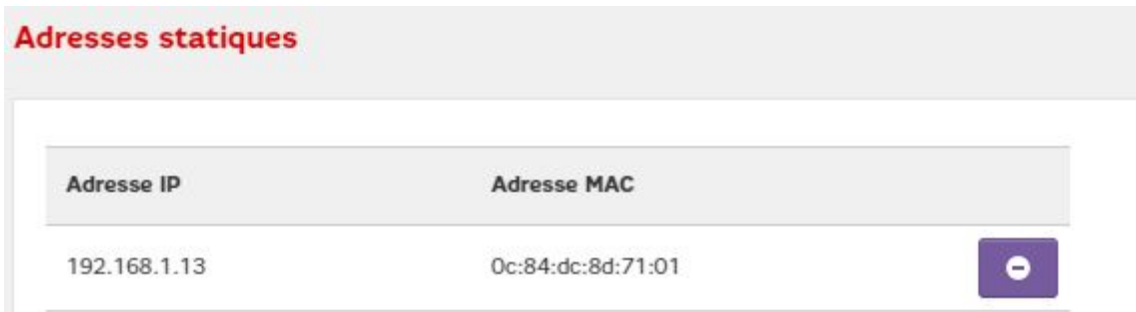
9)

In this question, we had to deal with quite a strange issue :

After the process, we had only one result on wireshark :



We tried to find why there wasn't all 'classical scheme' of DHCP requests and attributions. After a while, we found a way to explain this situation. As we work on Séverin's network, we managed to enter in the admin system of the router. We discovered that the PC of Séverin is registered in DHCP server as a "static address".



We ended up with this conclusion : as the DHCP server associated the PC with a static address, that's why there is just one DHCP ACK packet during the process of the connexion of the virtual machine in bridge mode.

We tried with Séverin's mobile with shared connexion, and you can see the steps of the DHCP server, as we thought (obviously, the mobile doesn't have the PC linked with a static address).

```
 11 0.042516911   192.168.43.1          255.255.255.255 DHCP      344 DHCP NAK      - Transaction ID 0xe0e1e001
 29 2.801092670   192.168.43.1          255.255.255.255 DHCP      353 DHCP Offer    - Transaction ID 0x7a20f51f
 31 2.816904676   192.168.43.1          255.255.255.255 DHCP      363 DHCP ACK      - Transaction ID 0x7a20f51f
```

Finally, we saw that the IP addresses of the DHCP ACK (for xample) are from 192.168.43.1 to the broadcast adress 255.255.255.255. The source port is 67 and the destination port is 68.

```
└  31 2.816904676   192.168.43.1          255.255.255.255 DHCP      363 DHCP ACK      - Transaction ID 0x7a20f51f
▸ Frame 31: 363 bytes on wire (2904 bits), 363 bytes captured (2904 bits) on interface 0
▾ Linux cooked capture
    Packet type: Broadcast (1)
    Link-layer address type: 1
    Link-layer address length: 6
    Source: d0:13:fd:5c:9c:09 (d0:13:fd:5c:9c:09)
    Protocol: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 192.168.43.1, Dst: 255.255.255.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 347
    Identification: 0xe266 (57958)
  ▸ Flags: 0x00
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (17)
  ▸ Header checksum: 0xab82 [validation disabled]
    Source: 192.168.43.1
    Destination: 255.255.255.255
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▾ User Datagram Protocol, Src Port: 67 (67), Dst Port: 68 (68)
    Source Port: 67
    Destination Port: 68
    Length: 327
  ▸ Checksum: 0x9b94 [validation disabled]
    [Stream index: 0]
▸ Bootstrap Protocol (ACK)
```

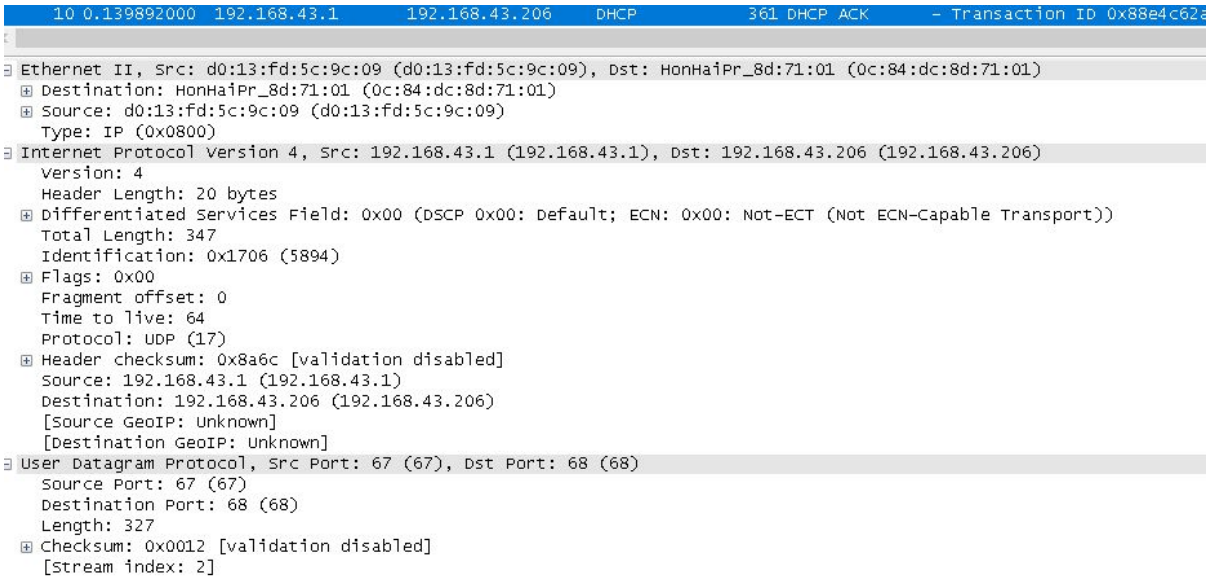
10)

Like the previous question, we didn't capture any DHCP Discover, offer or request.

We had :

5	0.007013000	0.0.0.0	255.255.255.255	DHCP	343 DHCP Request	- Transaction ID 0x88e4c62a
10	0.139892000	192.168.43.1	192.168.43.206	DHCP	361 DHCP ACK	- Transaction ID 0x88e4c62a

And the info of the DHCP ACK are :

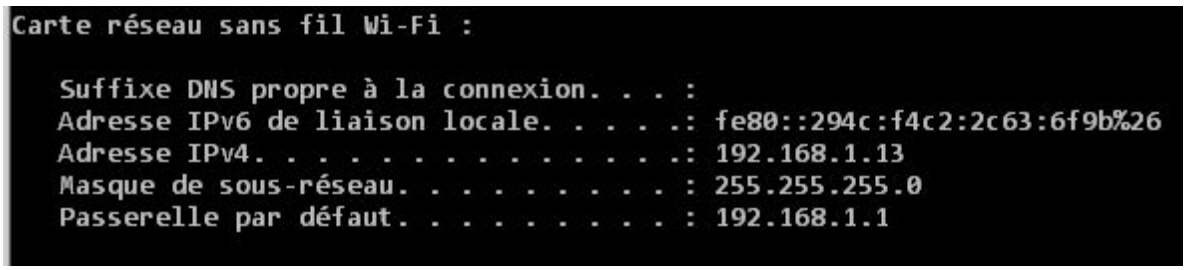


```
10 0.139892000  192.168.43.1      192.168.43.206    DHCP        361 DHCP ACK      - Transaction ID 0x88e4c62a

Ethernet II, Src: d0:13:fd:5c:9c:09 (d0:13:fd:5c:9c:09), Dst: HonHaiPr_8d:71:01 (0c:84:dc:8d:71:01)
  Destination: HonHaiPr_8d:71:01 (0c:84:dc:8d:71:01)
  Source: d0:13:fd:5c:9c:09 (d0:13:fd:5c:9c:09)
  Type: IP (0x0800)
Internet Protocol Version 4, Src: 192.168.43.1 (192.168.43.1), Dst: 192.168.43.206 (192.168.43.206)
  Version: 4
  Header Length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 347
  Identification: 0x1706 (5894)
  Flags: 0x00
  Fragment offset: 0
  Time to live: 64
  Protocol: UDP (17)
  Header checksum: 0x8a6c [validation disabled]
  Source: 192.168.43.1 (192.168.43.1)
  Destination: 192.168.43.206 (192.168.43.206)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 67 (67), Dst Port: 68 (68)
  Source Port: 67 (67)
  Destination Port: 68 (68)
  Length: 327
  Checksum: 0x0012 [validation disabled]
  [Stream index: 2]
```

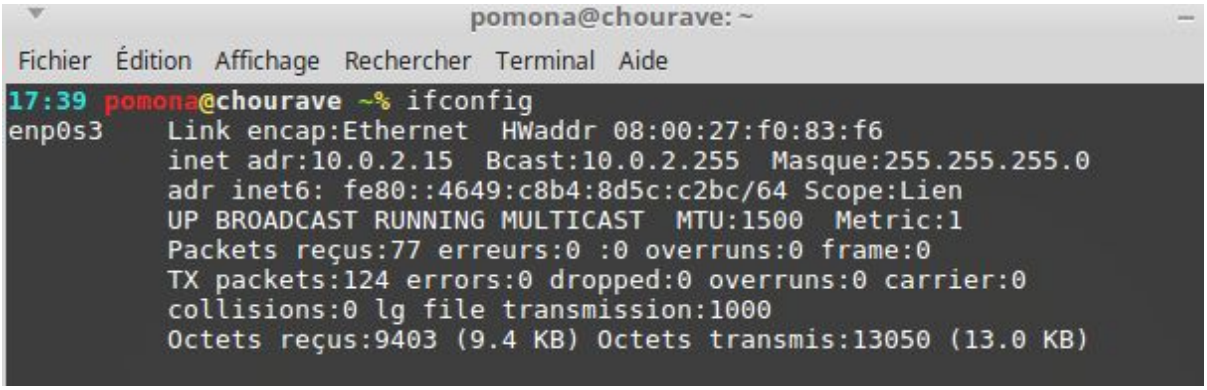
(The difference seems to be the destination of the DHCP ACK, which was to the broadcast address on the virtual machine, and directly the IP address of the PC on the host)

Part 2: NAT mode

11)



12)



13)

As we are in NAT mode, the virtual machine is in a virtual network, and doesn't appear anymore as a detached devise for the router. All the traffic works passing the host machine. That's why the virtual and host machines are not on the same network (192.168.1.1/24 != 10.0.2.1/24)

14)

The DHCP server is virtual and depends of the configuration of vmware (or virtualbox for our case). So the DHCP server is on the host machine. The DHCP server IP address is : 10.0.2.1

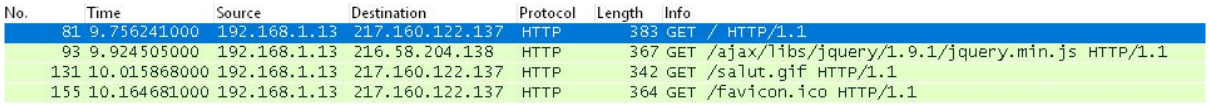
15)

The IP address of the NAT device is 10.0.2.15.

16)

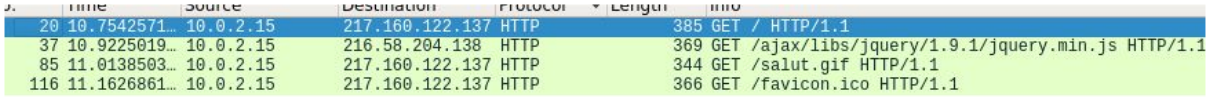
The oracle website seems to be in https which can influence the access of the data.
We tried on another website http://www.salutcestcool.com/ :

We can notice that the host hides from the destination the virtual machine existence and apply his own IP address as the source.



No.	Time	Source	Destination	Protocol	Length	Info
81	9.756241000	192.168.1.13	217.160.122.137	HTTP	383	GET / HTTP/1.1
93	9.924505000	192.168.1.13	216.58.204.138	HTTP	367	GET /ajax/libs/jquery/1.9.1/jquery.min.js HTTP/1.1
131	10.015868000	192.168.1.13	217.160.122.137	HTTP	342	GET /salut.gif HTTP/1.1
155	10.164681000	192.168.1.13	217.160.122.137	HTTP	364	GET /favicon.ico HTTP/1.1

The virtual machine doesn't have to know the NAT situation because this is the host which changes the packets info (IP source).



No.	Time	Source	Destination	Protocol	Length	Info
20	10.7542571…	10.0.2.15	217.160.122.137	HTTP	385	GET / HTTP/1.1
37	10.9225019…	10.0.2.15	216.58.204.138	HTTP	369	GET /ajax/libs/jquery/1.9.1/jquery.min.js HTTP/1.1
85	11.0138503…	10.0.2.15	217.160.122.137	HTTP	344	GET /salut.gif HTTP/1.1
116	11.1626861…	10.0.2.15	217.160.122.137	HTTP	366	GET /favicon.ico HTTP/1.1

So having a NAT device can hide it from the host network and protect it from attacks.

Part 3: Host Only mode

17)

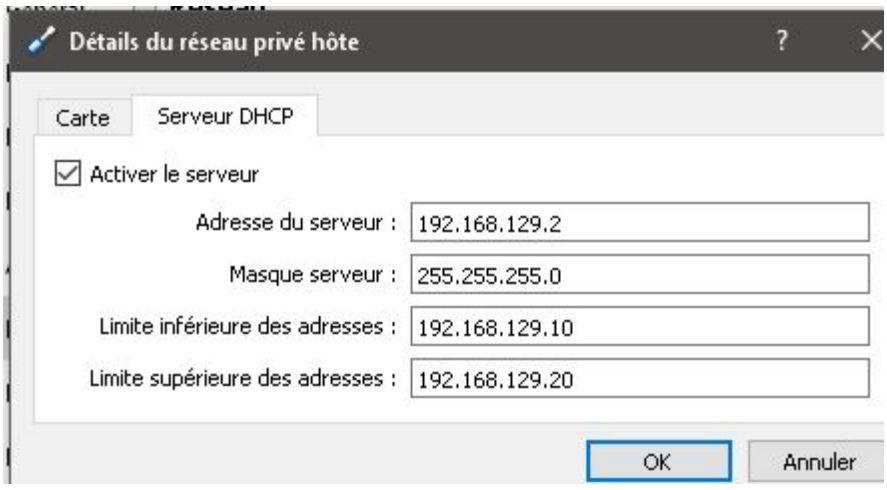
```
Carte Ethernet VirtualBox Host-Only Network :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::8ca3:3fe8:3889:de2b%15
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.129.1
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . :
```

18)

```
pomona@chourave: ~
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
18:32 pomona@chourave ~% ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:f0:83:f6
          inet adr:192.168.129.10  Bcast:192.168.129.255  Masque:255.255.255.0
          adr inet6: fe80::4649:c8b4:8d5c:c2bc/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Packets reçus:29 erreurs:0 :0 overruns:0 frame:0
          TX packets:42 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          Octets reçus:7440 (7.4 KB) Octets transmis:6382 (6.3 KB)
```

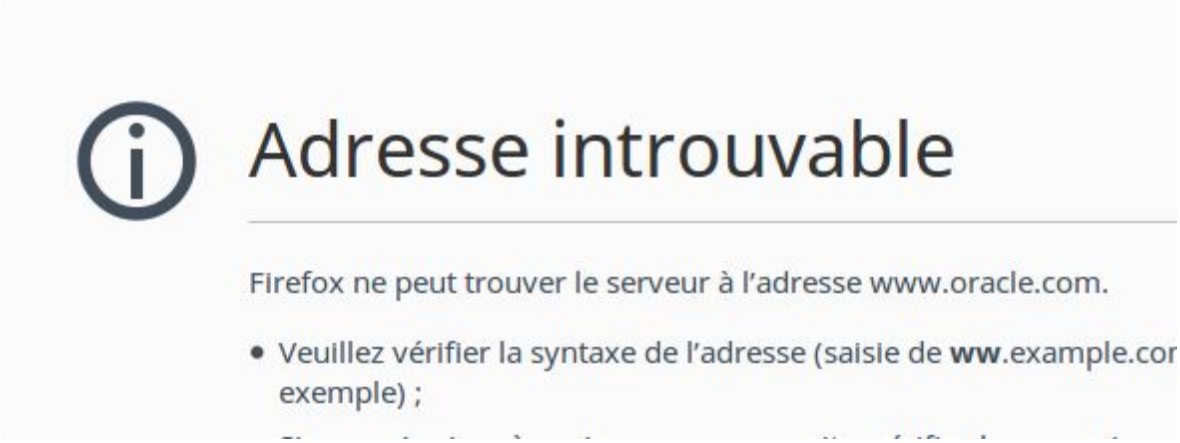
19)

The IP address of the virtual machine is 192.168.129.10 because of our configuration of the virtual host only device on virtualBox.
We configure the DHCP server to be at 192.168.129.2 (in the same virtual network of the virtual device created by virtualbox)



20)

As we tried to connect to the oracle website, we obtained an error :



This is because of the main goal of the host only network :

The virtual machine can only speak to the host and other virtual machines which could be connected to the virtual device.
The virtual machine cannot access the outside (internet and host network) and no device can access the virtual device.
This configuration allows a machine to be “disconnected” to the internet and increases the security of the machine.