PHALAVANDISHVILI Demetre - JAMET Félix - Groupe 601B

TP5 Partie 1

Câblage et configuration de base

Pour segmenter la plage réseau en deux parties, on ajoute un bit à la partie réseau de l'adresse, celle ci passant sur 22 bits. On créé de cette manière la plage 194.85.44.2/22 et la plage 194.85.40.2/22.

`ifconfig eth0 194.85.44.2/22` donne une erreur lorsque tapé une fois. En effet, l'adresse commençant par 194, ifconfig s'attend à une adresse de classe C avec un masque de sous réseau d'au moins 24 bits. En retapant la commande, elle est acceptée

On configure les machines du réseau LAN1 comme suit :

```
# ifconfig eth0 194.85.40.x/22
```

On configure les machines du réseau LAN2 comme suit :

```
# ifconfig eth0 194.85.44.x/22
```

Où x est le numéro de la machine

Utilisation des alias de carte

Ajoutons m5 au réseau LAN3 :

```
# ifconfig eth0:lan3 10.10.10.5/24
```

Même chose pour m6 :

```
# ifconfig eth0:lan3 10.10.10.6/24
```

On teste les connexions :

$m5 \rightarrow m1$ (sur LAN1)

```
m5 -> m1
 ping -c 5 194.85.40.1
PING 194.85.40.1 (194.85.40.1) 56(84) bytes of data.
64 bytes from 194.85.40.1: icmp_seq=1 ttl=64 time=9.02 ms
64 bytes from 194.85.40.1: icmp_seq=2 ttl=64 time=2.86 ms
64 bytes from 194.85.40.1: icmp_seq=3 ttl=64 time=2.27 ms
64 bytes from 194.85.40.1: icmp_seq=4 ttl=64 time=7.20 ms
64 bytes from 194.85.40.1: icmp_seq=5 ttl=64 time=4.17 ms

--- 194.85.40.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4029ms
rtt min/avg/max/mdev = 2.273/5.108/9.026/2.596 ms
```

$m6 \rightarrow m5$ (sur LAN3)

```
 ping -c 5 10.10.0.5
PING 10.10.0.5 (10.10.0.5) 56(84) bytes of data.
64 bytes from 10.10.0.5: icmp_seq=1 ttl=64 time=3.77 ms
64 bytes from 10.10.0.5: icmp_seq=2 ttl=64 time=1.39 ms
64 bytes from 10.10.0.5: icmp_seq=3 ttl=64 time=2.82 ms
64 bytes from 10.10.0.5: icmp_seq=4 ttl=64 time=1.52 ms
64 bytes from 10.10.0.5: icmp_seq=5 ttl=64 time=1.27 ms

--- 10.10.0.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4044ms
rtt min/avg/max/mdev = 1.273/2.157/3.775/0.983 ms
```

$m1 \rightarrow m2$ (respectivement sur LAN1 et LAN2)

```
m1 -> m2
 ping 194.85.44.2
connect: Network is unreachable
```

On constate que les deux premiers pings sont un succès tandis que le dernier ping ne fonctionne pas. La raison de ce comportement est que les machines m1 et m2 ne sont pas sur le même réseau et qu'aucune passerelle entre ces réseaux n'est configurée.

Polarité MDI/MDI-X

- $m1 \rightarrow m6$

```
 ping 194.85.40.6
 [...]
64 bytes from 194.85.40.1: icmp_seq=14 ttl=64 time=1.92 ms
64 bytes from 194.85.40.1: icmp_seq=15 ttl=64 time=1.87 ms
64 bytes from 194.85.40.1: icmp_seq=16 ttl=64 time=1.82 ms
64 bytes from 194.85.40.1: icmp_seq=17 ttl=64 time=2.16 ms
64 bytes from 194.85.40.1: icmp_seq=18 ttl=64 time=2.04 ms
64 bytes from 194.85.40.1: icmp_seq=19 ttl=64 time=2.92 ms
64 bytes from 194.85.40.1: icmp_seq=20 ttl=64 time=7.55 ms
64 bytes from 194.85.40.1: icmp_seq=21 ttl=64 time=2.24 ms
64 bytes from 194.85.40.1: icmp_seq=22 ttl=64 time=1.98 ms
64 bytes from 194.85.40.1: icmp_seq=23 ttl=64 time=1.92 ms
From 194.85.40.6 icmp_seq=24 Destination Host Unreachable
From 194.85.40.6 icmp_seq=25 Destination Host Unreachable
From 194.85.40.6 icmp_seq=26 Destination Host Unreachable
From 194.85.40.6 icmp_seq=27 Destination Host Unreachable
From 194.85.40.6 icmp_seq=28 Destination Host Unreachable
From 194.85.40.6 icmp_seq=29 Destination Host Unreachable
From 194.85.40.6 icmp_seq=30 Destination Host Unreachable
From 194.85.40.6 icmp_seq=31 Destination Host Unreachable
From 194.85.40.6 icmp_seq=33 Destination Host Unreachable
From 194.85.40.6 icmp_seq=34 Destination Host Unreachable
From 194.85.40.6 icmp_seq=35 Destination Host Unreachable
From 194.85.40.6 icmp_seq=36 Destination Host Unreachable
From 194.85.40.6 icmp_seq=37 Destination Host Unreachable
From 194.85.40.6 icmp_seq=38 Destination Host Unreachable
64 bytes from 194.85.40.1: icmp_seq=39 ttl=64 time=1025 ms
64 bytes from 194.85.40.1: icmp_seq=40 ttl=64 time=19.7 ms
64 bytes from 194.85.40.1: icmp_seq=41 ttl=64 time=2.02 ms
64 bytes from 194.85.40.1: icmp_seq=42 ttl=64 time=2.17 ms
64 bytes from 194.85.40.1: icmp_seq=43 ttl=64 time=1.80 ms
64 bytes from 194.85.40.1: icmp_seq=44 ttl=64 time=1.92 ms
64 bytes from 194.85.40.1: icmp_seq=45 ttl=64 time=2.55 ms
64 bytes from 194.85.40.1: icmp_seq=46 ttl=64 time=7.11 ms
64 bytes from 194.85.40.1: icmp_seq=47 ttl=64 time=3.51 ms
64 bytes from 194.85.40.1: icmp_seq=48 ttl=64 time=2.55 ms
```

On constate que quand on remplace un câble croisé par un cable droit entre le switch 1 et 2, on n'arrive pas à joindre la machine 6 (m6) depuis m1. Le ping refonctionne normalement en rebranchant le câble croisé

Non Etanchéité

Broadcast *ARP*

Quand on lance la commande de ping de m1 → m5, on voit sur le ***tcpdump*** de la machine 4 une trame ARP demandant à qui correspond l'adresse de la machine 5 :

```
12:57:07.818536 arp who-has 194.85.40.5 tell 194.85.40.1
```

Broadcast DHCP

En suivant les etapes décrites dans la feuille de TP, nous avons défini la plage des adresses IP sur m1 & m2 :

- m1 :

```
subnet 194.85.40.0 netmask 255.255.252.0
{
  194.85.40.51 192.85.40.99
}
ddns-update-style none;
```

- m2

```
subnet 194.85.44.0 netmask 255.255.252.0
{
  194.85.44.51 192.85.44.99
}
ddns-update-style none;
```

Ensuite, nous avons ajouté les machines m7, m8 et m9. La machine m7 est branchée sur le switch 1, m8 sur le switch 3 et m9 sur le switch 2.
Puis nous avons lancé une demande d'affectation d'adresse ip avec la commande suivante :

```
dhclient eth0
```

On obtient comme résultats :

- m7

```
Internet Systems Consortium DHCP Client V3.0.5
Copyright 2004-2006 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/

Listening on LPF/eth0/02:04:06:e6:f6:28
Sending on   LPF/eth0/02:04:06:e6:f6:28
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 7
DHCPOFFER from 194.85.44.2
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPNAK from 194.85.40.1
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 5
receive_packet failed on eth0: Network is down
DHCPOFFER from 194.85.44.2
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPNAK from 194.85.40.1
DHCPACK from 194.85.44.2
SIOCADDRT: Network is unreachable
bound to 194.85.44.98 -- renewal in 263 seconds.
```

- m8

```
Internet Systems Consortium DHCP Client V3.0.5
Copyright 2004-2006 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/

Listening on LPF/eth0/02:04:06:02:07:90
Sending on   LPF/eth0/02:04:06:02:07:90
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 7
DHCPOFFER from 194.85.40.1
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPNAK from 194.85.44.2
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 6
receive_packet failed on eth0: Network is down
DHCPOFFER from 194.85.40.1
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPNAK from 194.85.44.2
DHCPACK from 194.85.40.1
SIOCADDRT: Network is unreachable
bound to 194.85.40.98 -- renewal in 267 seconds.
```

- m9

```
Internet Systems Consortium DHCP Client V3.0.5
Copyright 2004-2006 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/

Listening on LPF/eth0/02:04:06:f0:af:a7
Sending on   LPF/eth0/02:04:06:f0:af:a7
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 3
DHCPOFFER from 194.85.40.1
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPNAK from 194.85.44.2
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 4
receive_packet failed on eth0: Network is down
DHCPOFFER from 194.85.40.1
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPNAK from 194.85.44.2
DHCPACK from 194.85.40.1
SIOCADDRT: Network is unreachable
bound to 194.85.40.96 -- renewal in 260 seconds.
```

On voit que ces adresses IP vont être renouvelées dans un certain temps(ici en moyenne 260 secondes). De plus on voit que la machine m7 et m9 appartient au LAN_1 et la machine m8 appartient au LAN_2.

TP 5 partie 2

Câblage et configuration de base

Pour segmenter la plage réseau en deux parties, on ajoute un bit à la partie réseau de l'adresse, celle ci passant sur 22 bits. On créé de cette manière la plage 195.12.56.0/22 et la plage 195.12.60.2/22.

`ifconfig eth0 195.12.60.2/22` donne une erreur lorsque tapé une fois. En effet, l'adresse commençant par 194, ifconfig s'attend à une adresse de classe C avec un masque de sous réseau d'au moins 24 bits. En retapant la commande, elle est acceptée.

On configure les machines du réseau LAN1 comme suit :

```
# ifconfig eth0 195.12.56.x/22
```

On configure les machines du réseau LAN2 comme suit :

```
# ifconfig eth0 195.12.60.x/22
```

Où x est le numéro de la machine

Test de la connexion

- sur Lan2
  - m2 $\longrightarrow$ m4

    ```
    ping -c 5 195.12.60.4
    PING 195.12.60.4 (195.12.60.4): 56 data bytes
    64 bytes from 195.12.60.4: icmp_seq=0 ttl=64 time=21.599 ms
    64 bytes from 195.12.60.4: icmp_seq=1 ttl=64 time=1.364 ms
    64 bytes from 195.12.60.4: icmp_seq=2 ttl=64 time=1.724 ms
    64 bytes from 195.12.60.4: icmp_seq=3 ttl=64 time=2.261 ms
    64 bytes from 195.12.60.4: icmp_seq=4 ttl=64 time=1.987 ms
    --- 195.12.60.4 ping statistics ---
    5 packets transmitted, 5 packets received, 0% packet loss
    round-trip min/avg/max/stddev = 1.364/5.787/21.599/7.912 ms
    ```

- Lan2 $\longrightarrow \mathit{Lan1}$
  - m2 $\longrightarrow$ m1

```
LAN2 -> LAN1
m2 -> m1
ping -c 5 195.12.56.1
PING 195.12.56.1 (195.12.56.1): 56 data bytes
ping: sendto: Network is unreachable
ping: sendto: Network is unreachable
ping: sendto: Network is unreachable
ping: sendto: Network is unreachable
ping: sendto: Network is unreachable

--- 195.12.56.1 ping statistics ---
0 packets transmitted, 0 packets received,
```

- sur Lan1
  - m1 ⟶ m3

```
ping -c 5 195.12.56.3
PING 195.12.56.3 (195.12.56.3): 56 data bytes
64 bytes from 195.12.56.3: icmp_seq=0 ttl=64 time=21.464 ms
64 bytes from 195.12.56.3: icmp_seq=1 ttl=64 time=1.867 ms
64 bytes from 195.12.56.3: icmp_seq=2 ttl=64 time=2.112 ms
64 bytes from 195.12.56.3: icmp_seq=3 ttl=64 time=1.943 ms
64 bytes from 195.12.56.3: icmp_seq=4 ttl=64 time=2.302 ms
--- 195.12.56.3 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.867/5.938/21.464/7.765 ms
```

- Lan1 ⟶ Lan2
  - m1 ⟶ m5

```
ping -c 5 195.12.60.5
PING 195.12.60.5 (195.12.60.5): 56 data bytes
ping: sendto: Network is unreachable
ping: sendto: Network is unreachable
ping: sendto: Network is unreachable
ping: sendto: Network is unreachable
ping: sendto: Network is unreachable
--- 195.12.60.5 ping statistics ---
0 packets transmitted, 0 packets received,
```

Les résultats obtenu entre les différents LANs est tout à fait logique, car aucune passerelle n'as été configurée.

Constater la non étanchéité

Comme dans la partie 1, on modifie le fichier */etc/dhcp.conf* sur les machines 1 et 2,appartenant au LAN_1 et au LAN_2 respectivement.

- sur la machine 1 on fait les modifications suivantes:

```
subnet 195.12.56.0 netmask 255.255.252.0
{
        195.12.56.51 195.12.56.99
}
ddns-update-style none;
```

- sur la machine 2 on fait les modifications suivantes:

```
subnet 195.12.60.0 netmask 255.255.252.0
{
        195.12.60.51 195.12.60.99
}
ddns-update-style none;
```

Tests d'étanchéité

Diffusion ARP

Pour tester l'étanchéité de notre réseau, on lance un ping de la machine m3 vers la machine m5 et on observe le résultat dans le terminal de la machine m2, en utilisant le programme *tcpdump* dont voici les captures :

- ping m3->m5

```
PING 195.12.56.5 (195.12.56.5) 56(84) bytes of data.
64 bytes from 195.12.56.5: icmp_seq=1 ttl=64 time=38.2 ms
64 bytes from 195.12.56.5: icmp_seq=2 ttl=64 time=12.0 ms
64 bytes from 195.12.56.5: icmp_seq=3 ttl=64 time=8.16 ms

--- 195.12.56.5 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2020ms
rtt min/avg/max/mdev = 8.164/19.470/38.219/13.351 ms
```

- capture de *tcpdump* sur la machine m2

```
22:05:15.837319 arp who-has 195.12.56.5 tell 195.12.56.3
```

- capture de *tcpdump* sur la machine m5

```
        0x0010:  0000                                        ..
22:05:15.837357 arp who-has 195.12.56.5 tell 195.12.56.3
22:05:15.837403 arp reply 195.12.56.5 is-at 02:04:06:28:01:b7 (oui Unknown)
22:05:15.842665 IP 195.12.56.3 > 195.12.56.5: ICMP echo request, id 41987, seq 1,
length 64
22:05:15.842738 IP 195.12.56.5 > 195.12.56.3: ICMP echo reply, id 41987, seq 1,
length 64
22:05:16.827469 IP 195.12.56.3 > 195.12.56.5: ICMP echo request, id 41987, seq 2,
length 64
22:05:16.827539 IP 195.12.56.5 > 195.12.56.3: ICMP echo reply, id 41987, seq 2,
length 64
22:05:17.835689 IP 195.12.56.3 > 195.12.56.5: ICMP echo request, id 41987, seq 3,
length 64
22:05:17.835765 IP 195.12.56.5 > 195.12.56.3: ICMP echo reply, id 41987, seq 3,
length 64
22:05:20.844352 arp who-has 195.12.56.3 tell 195.12.56.5
```

Le ping est lancé entre les machines m3 et m5 qui appartiennent au LAN_1. Cependant, on voit la demande *arp* sur la machine m2 qui n'appartient pas au LAN_1. On peut donc en déduire que notre réseau n'est pas étanche.

Diffusion DHCP

Après avoir configuré un DHCP basique, on lance `dhclient etho` sur la machine 2. On voit que cette demande est diffusée sur LAN_1 et LAN_2 car dans le *tcpdump* lancé sur les machines m3 et m5, on observe la demande DHCP. Voici les captures :

- machine m2 :

```
 dhclient eth0
Internet Systems Consortium DHCP Client V3.0.5
Copyright 2004-2006 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/

Listening on LPF/eth0/02:04:06:ca:c4:6e
Sending on   LPF/eth0/02:04:06:ca:c4:6e
Sending on   Socket/fallback
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPNAK from 195.12.60.2
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 3
receive_packet failed on eth0: Network is down
DHCPOFFER from 195.12.56.1
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPNAK from 195.12.60.2
DHCPACK from 195.12.56.1
SIOCADDRT: Network is unreachable
bound to 195.12.56.99 -- renewal in 301 seconds.
```

- machine m3 :

```
22:16:57.990989 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request
from 02:04:06:ca:c4:6e (oui Unknown), length 300
22:16:57.998492 IP 195.12.60.2.bootps > 255.255.255.255.bootpc: BOOTP/DHCP, Reply,
length 300
22:16:58.394889 IP6 :: > ff02::16: HBH ICMP6, multicast listener report v2, 1 group
record(s), length 28
22:16:58.972436 IP6 :: > ff02::1:ffca:c46e: ICMP6, neighbor solicitation, who has
fe80::4:6ff:feca:c46e, length 24
22:16:59.174275 IP6 :: > ff02::16: HBH ICMP6, multicast listener report v2, 1 group
record(s), length 28
22:16:59.400700 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request
from 02:04:06:ca:c4:6e (oui Unknown), length 300
22:16:59.414644 IP 195.12.60.2.bootps > 195.12.60.99.bootpc: BOOTP/DHCP, Reply,
length 300
22:16:59.445465 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request
from 02:04:06:ca:c4:6e (oui Unknown), length 300
22:16:59.449362 IP 195.12.60.2.bootps > 255.255.255.255.bootpc: BOOTP/DHCP, Reply,
length 300
```

- machine m5 :

```
22:16:58.002489 IP 195.12.60.2.bootps > 255.255.255.255.bootpc: BOOTP/DHCP, Reply,
length 300
22:16:58.394626 IP6 :: > ff02::16: HBH ICMP6, multicast listener report v2, 1 group
record(s), length 28
22:16:58.972498 IP6 :: > ff02::1:ffca:c46e: ICMP6, neighbor solicitation, who has
fe80::4:6ff:feca:c46e, length 24
22:16:59.174462 IP6 :: > ff02::16: HBH ICMP6, multicast listener report v2, 1 group
record(s), length 28
22:16:59.400839 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request
from 02:04:06:ca:c4:6e (oui Unknown), length 300
22:16:59.439100 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request
from 02:04:06:ca:c4:6e (oui Unknown), length 300
22:16:59.450286 IP 195.12.60.2.bootps > 255.255.255.255.bootpc: BOOTP/DHCP, Reply,
length 300
```

On voit que le réseau n'est pas étanche car DHCP est diffusé sur LAN2.

Configurer les VLANs

Pour modéliser les VLANs on utilise la commande suivante dans le terminal du switch s1:

```
vlan/create 1
vlan/create 2
```

En tapant ces deux commandes, on a crée deux LANs différents : LAN_1 et LAN_2. On affecte ensuite aux LANs leur ports respectifs. Pour éviter l'inversion de deux leds voisines, nous avons pris un switch avec 12 ports et nous avons utilisé tous les ports avec un numéro impair.

Nous associons les LANs aux ports avec la commande *port/setvlan* :

- LAN1

```
port/setvlan 1 1
port/setvlan 5 1
port/setvlan 9 1
```

- LAN2

```
port/setvlan 3 2
port/setvlan 7 2
port/setvlan 11 2
```

Test d'etanchéité

Diffusion ARP

Pour tester l'étanchéité du réseau, on lance un ping de la machine m3 vers la machine m5 et on observe le traffic sur m2 avec *tcpdump*

- ping 195.12.56.99

```
PING 195.12.56.99 (195.12.56.99) 56(84) bytes of data.
From 195.12.56.1 icmp_seq=1 Destination Host Unreachable
From 195.12.56.1 icmp_seq=2 Destination Host Unreachable
From 195.12.56.1 icmp_seq=3 Destination Host Unreachable
From 195.12.56.1 icmp_seq=4 Destination Host Unreachable
From 195.12.56.1 icmp_seq=5 Destination Host Unreachable
From 195.12.56.1 icmp_seq=6 Destination Host Unreachable

--- 195.12.56.99 ping statistics ---
8 packets transmitted, 0 received, +6 errors, 100% packet loss, time 7051ms
, pipe 4
```

- capture de *tcpdump* sur la machine m2 : aucune diffusion d'ARP sur LAN 2
- capture de *tcpdump* sur la machine m5

```
23:02:21.896022 arp who-has 195.12.56.99 tell 195.12.56.1
23:02:22.889429 arp who-has 195.12.56.99 tell 195.12.56.1
23:02:23.889935 arp who-has 195.12.56.99 tell 195.12.56.1
23:02:24.918982 arp who-has 195.12.56.99 tell 195.12.56.1
23:02:25.922833 arp who-has 195.12.56.99 tell 195.12.56.1
23:02:26.920674 arp who-has 195.12.56.99 tell 195.12.56.1
```

Le ping est lancé entre deux machine de LAN_1. On ne voit pas la requête *arp* sur la machine m2 qui n'appartient pas au LAN_1. On peut donc en déduire que notre réseau est étanche.

Diffusion DHCP

Après avoir configuré un DHCP basique on lance `dhclient eth0` sur la machine 2. Voici les captures :

- machine m6

```
dhclient eth0
Internet Systems Consortium DHCP Client V3.0.5
Copyright 2004-2006 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/

Listening on LPF/eth0/02:04:06:6d:e6:ba
Sending on   LPF/eth0/02:04:06:6d:e6:ba
Sending on   Socket/fallback
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPACK from 195.12.60.2
SIOCADDRT: Network is unreachable
bound to 195.12.60.98 -- renewal in 281 seconds.
```

- sur la machine m3

```
23:08:17.026177 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request
from 02:04:06:6d:e6:ba (oui Unknown), length 300
23:08:17.364066 IP 195.12.60.2.bootps > 195.12.60.98.bootpc: BOOTP/DHCP, Reply,
length 300
```

- sur la machine m1 on ne voit aucune trames arriver vie `dhclient eth0` .

On voit que le réseau est étanche car la requête DHCP n'est diffusée que sur LAN1. De plus, il n'y a plus de "course" entre deux serveurs *DHCP* comme il y avait avant.

Bonus : présentation du protocole DHCP

DHCP (Dynamic Host Configuration Protocol) est un protocole permettant de configurer automatiquement les machines d'un réseau. DHCP permet notamment de gérer les aspects de configuration suivants :

- l'attribution d'adresse IP
- l'adresse de la passerelle par défaut
- l'adresse des serveurs DNS

Attribution d'adresse IP

Un client souhaitant se connecter au réseau peut faire une demande de configuration auprès du serveur DHCP avec la commande *dhclient*.

Le serveur est à même de satisfaire les demandes d'attribution d'adresses car il conserve à chaque instant une base de données des adresses disponibles.
Il attribue une adresse au client en fonction du réseau auquel il appartient.
Lors de la déconnexion d'un client, l'adresse qu'il utilisait est rajoutée à la base de données des adresses et est donc prête à être remise en service.

DHCP dispose de trois différents mécanismes pour allouer des adresses IP

Allocation dynamique

Les adresses IP sont assignées pour une durée limitée.

Allocation automatique

Une adresse IP est associée à un client d'une manière permanente. Le serveur conserve une table des associations entre clients et adresses, permettant ainsi d'assigner à un client l'adresse qu'il a déjà eu par le passé.

Allocation manuelle/statique

L'administrateur réseau établit manuellement une correspondance entre les adresses MAC des clients et l'adresse IP leur étant attribuée.

Réatribution des adresses DHCP

Une fois une adresse IP attribuée par DHCP, elle possède une durée de vie limitée. Lorsqu'un client redémarre, il tente d'obtenir un bail pour la même adresse avec le serveur DHCP d'origine, en émettant un DHCPREQUEST. Si la tentative se solde par un échec, le client continue à utiliser la même adresse IP s'il lui reste du temps sur son bail. Si à 50% le bail n'a pu être renouvelé, le client tente de contacter l'ensemble des serveurs DHCP (diffusion) lorsqu'il atteint 87,5% de son bail, avec un DHCPREQUEST, les serveurs répondent soit par DHCPACK soit par DHCPNACK (adresse inutilisable). Lorsque le bail expire ou qu'un message DHCPNACK est reçu le client doit cesser d'utiliser l'adresse IP et et demander un nouveau bail (retour au processus de souscription). Lorsque le bail expire et que le client n'obtient pas d'autre adresse la communication TCP/IP s'interrompt. Une fois les adresses IP est attribué par dhcp, cette adresse IP possede une durée de vie de 280 à 300 secondes. Puis lorsqu'un client redémarre, il tente d'obtenir un bail pour la même adresse avec le serveur DHCP d'origine, en émettant un DHCPREQUEST. Si la tentative se solde par un échec, le client continue à utiliser la même adresse IP s'il lui reste du temps sur son bail. Si à 50% le bail n'a pu être renouvelé, le client tente de contacter l'ensemble des serveurs DHCP (diffusion) lorsqu'il atteint 87,5% de son bail, avec un DHCPREQUEST, les serveurs répondent soit par DHCPACK soit par DHCPNACK (adresse inutilisable). Lorsque le bail expire ou qu'un message DHCPNACK est reçu le client doit cesser d'utiliser l'adresse IP et et demander un nouveau bail (retour au processus de souscription). Lorsque le bail expire et que le client n'obtient pas d'autre adresse la communication TCP/IP s'interrompt.

Sources

http://cisco.goffinet.org/s1/dhcp#.WL6VZ3qTRN0
https://www.slideshare.net/truptikini/dhcp-presentation-22195996
https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol