Département d'informatique

INF3405

Réseaux informatiques

TP1

Section de laboratoire < **05** >

Soumis à Liliane-Caroline Demers

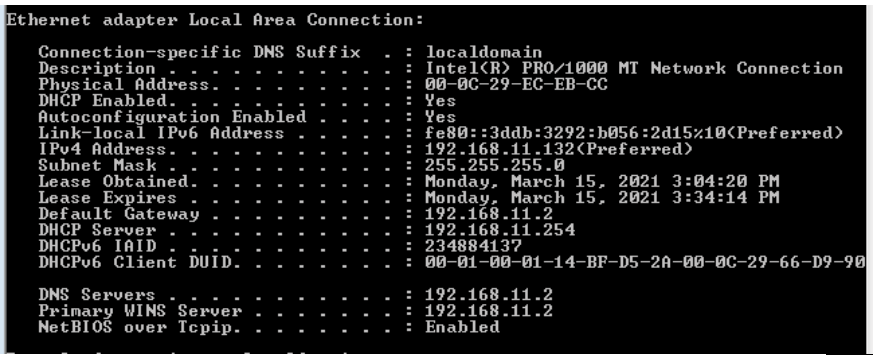
<Maximiliano Falicoff, Corentin Glaus, Anthony Marcelo Guzman Soto>

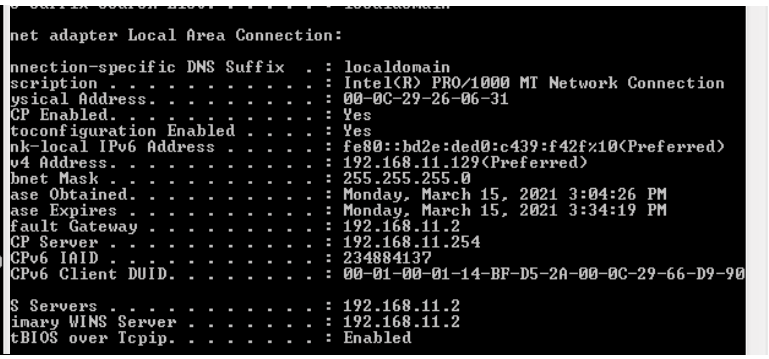
<2013658, 2021624, 2019666>

Remis le 2 Avril 2021 (Session H21)

6. Préparation de l’environnement de travail client virtuel

1. Poste L4708-20





Machine A MachineB

8. Partie DHCP (Dynamic Host Configuration Protocol)

1.

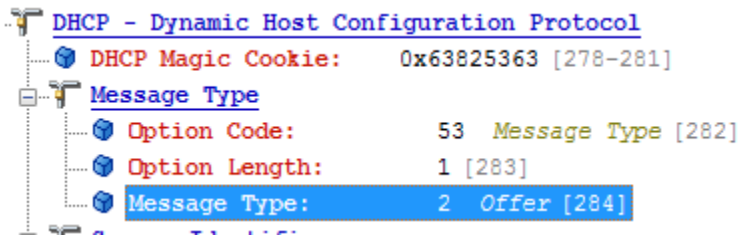
1	0.0.0.0	IP Broadcast	346	0.000000	DHCP	C DISCOVER 192.168.11.132 test-PC	
5	192.168.11.254	192.168.11.132	346	1.000278	DHCP	R OFFER 192.168.11.132	
6	0.0.0.0	IP Broadcast	356	1.000552	DHCP	C REQUEST 192.168.11.132 test-PC	
7	192.168.11.254	192.168.11.132	346	1.000754	DHCP	R ACK	DHCP Low Lease Time (30 minutes,...

    1. Cherche un DHCP server qui est disponible
    2. Le DHCP lui répond son adresse IP et lui offre une nouvelle adresse IP
    3. Il affirme qu’il veut la nouvelle adresse IP
    4. Le DHCP server lui assigne la nouvelle adresse IP et lui envoie les données de configuration
2. La première opération est faite en broadcast car la machine ne connaît pas qui est le serveur DHCP. La troisième opération est aussi faite en broadcast dans le but que s’il avait reçu plusieurs “OFFER” de différent serveur DHCP, il informe quel serveur il choisit (basé sur la distance) dans le but que les autres serveurs DHCP suppriment les données de configuration de la machine.

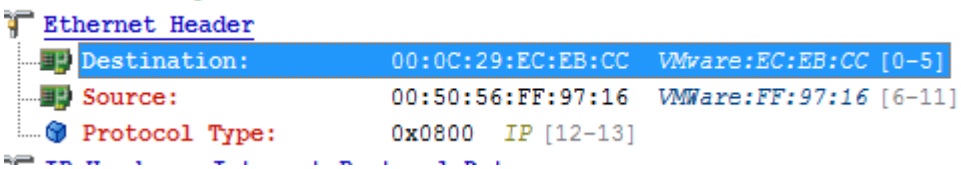
3. Le DHCP ne peut pas utiliser le protocole TCP comme protocole de transport puisque le TCP a besoin que nous ayons deux différentes adresses IP uniques qui se communiquent. Cependant, les adresses 0.0.0.0 et 255.255.255.255 (broadcast) ne sont pas uniques vu que plusieurs machines peuvent l’utiliser. De plus, le protocole TCP a un packet size de 20 octets alors que le UDP utilise un de 8 octets.

4.

5. La trame DHCP OFFER envoie un message à l'ordinateur client. Ce message contient les informations du réseau, dont le client aura besoin pour faire le DHCP REQUEST.
6. DHCP -> Message Type -> Message Type: 2 = offer\

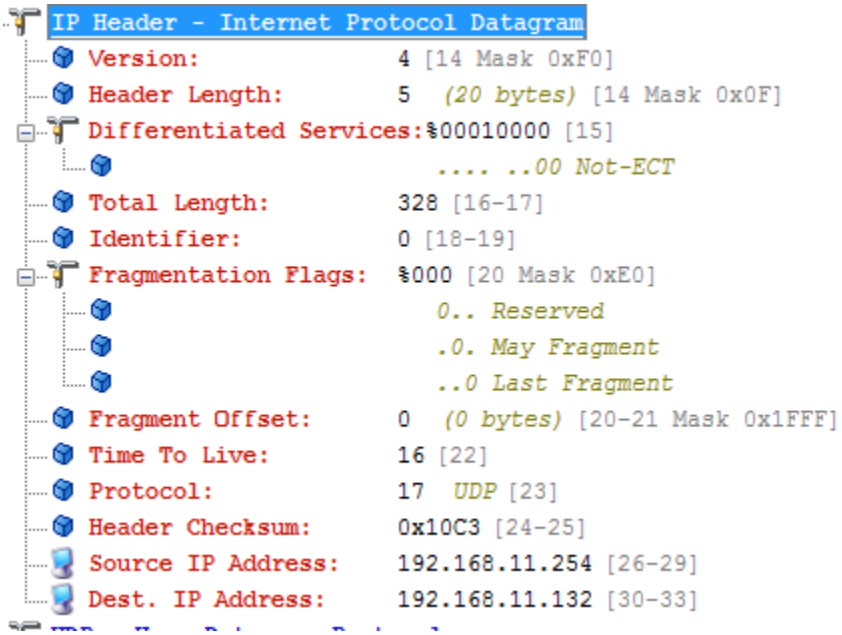


7.

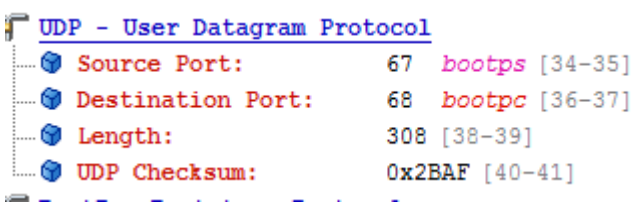


La destination est la machine A. La Source est le Serveur DHCP

8. L'adresse IP Source appartient au Serveur DHCP.
9. La taille de l'entête Ethernet est de 14 bytes
10. La valeur du champ Protocole Type est 0x0800 Ip et cela signifie que l'on utilise l'en tête IPV4
11. De savoir quelle adresse IP nous a été donnée par la passerelle par défaut.
12. Ce champ design l'adresse ip qui a été donnée par le serveur. L'utilité est de connaître la nouvelle adresse IP qui a été donnée par le serveur. Cette information sera utilisée lors du DHCP request.
13. Il correspond à l'entête du protocole IP



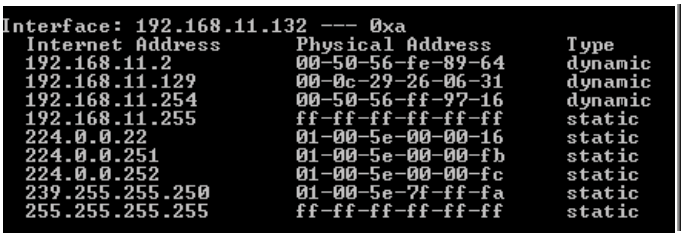
14. 20 octets
15. Il correspond à l'entête du protocole UDP



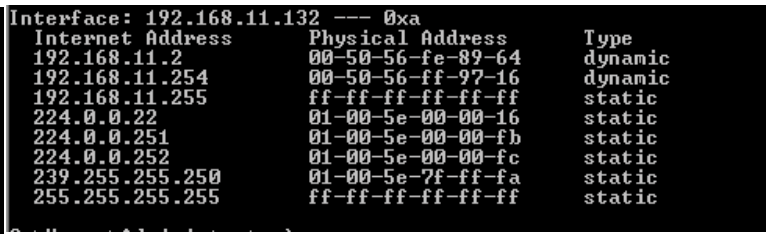
16. 8 octets
17. 30 minutes (1800 s)

9. Partie ARP (Address Resolution Protocol)

1. La cache se construit au fur et à mesure que notre ordinateur fait des requêtes. Cela évite dans le futur de faire des broadcasts pour savoir a qui envoyer la trame.
2.



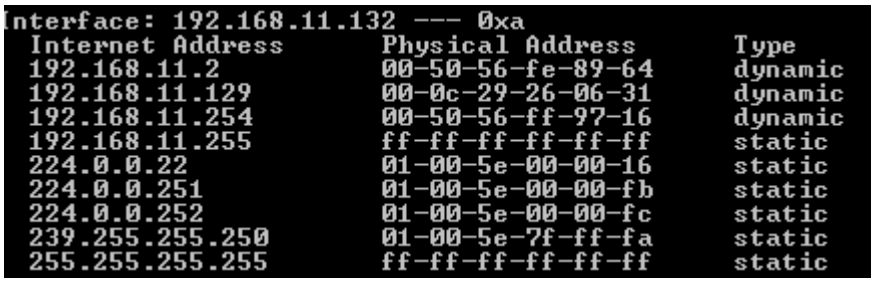
```
Interface: 192.168.11.132 --- 0xa
  Internet Address      Physical Address      Type
  192.168.11.2          00-50-56-fe-89-64     dynamic
  192.168.11.129        00-0c-29-26-06-31     dynamic
  192.168.11.254        00-50-56-ff-97-16     dynamic
  192.168.11.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```



```
Interface: 192.168.11.132 --- 0xa
  Internet Address      Physical Address      Type
  192.168.11.2          00-50-56-fe-89-64     dynamic
  192.168.11.254        00-50-56-ff-97-16     dynamic
  192.168.11.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

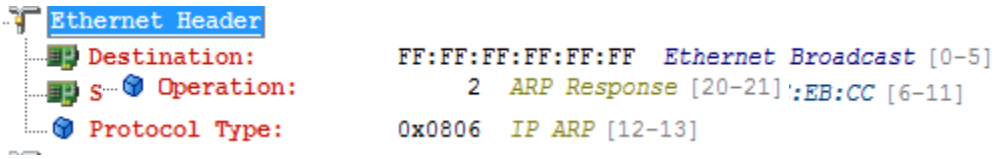
Avant Après

3. On remarque que l’adresse est réapparue



```
Interface: 192.168.11.132 --- 0xa
  Internet Address      Physical Address      Type
  192.168.11.2          00-50-56-fe-89-64     dynamic
  192.168.11.129        00-0c-29-26-06-31     dynamic
  192.168.11.254        00-50-56-ff-97-16     dynamic
  192.168.11.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

4. La longueur d’une trame ARP est de 64 octets
5. La valeur numérique est 08 06 en hexadécimal



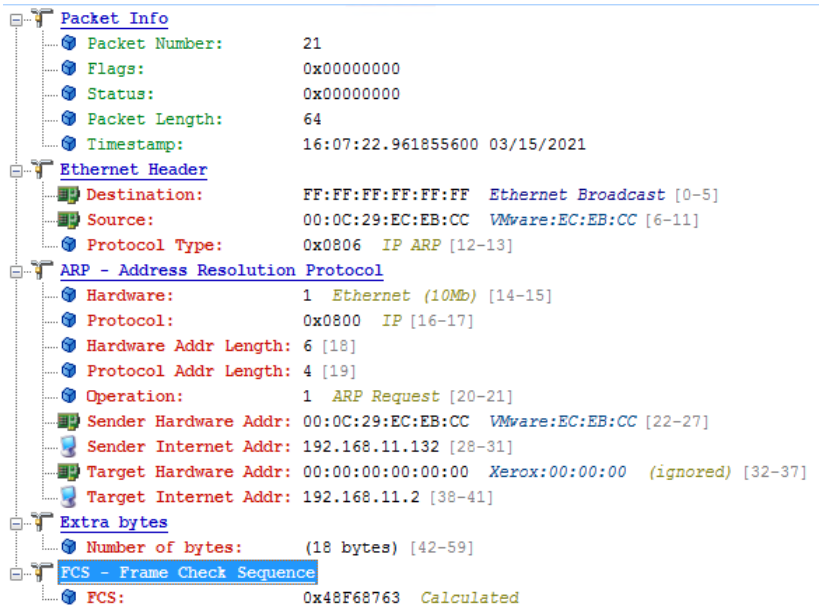
```
Ethernet Header
    Destination:        FF:FF:FF:FF:FF:FF  Ethernet Broadcast [0-5]
    Operation:               2  ARP Response [20-21]':EB:CC [6-11]
    Protocol Type:      0x0806  IP ARP [12-13]
```

6. Ce qui différencie les deux est le mode d'opération dans la section ARP du trame

```
Operation:              1  ARP Request [20-21]
```

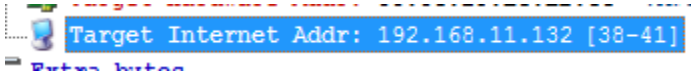
7. Le nœud qui correspond à la source de la réponse ARP est la passerelle par défaut.

8. Le nœud qui correspond à la destination de la réponse ARP est notre machine locale (machine A).

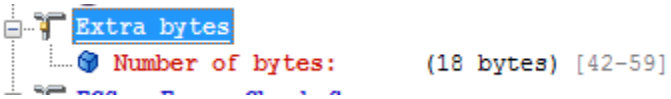
9. 

La séquence est un Ethernet Header, le message ARP, un padding et le frame check sequence

10. Le Target Internet Address sous la section ARP de la trame

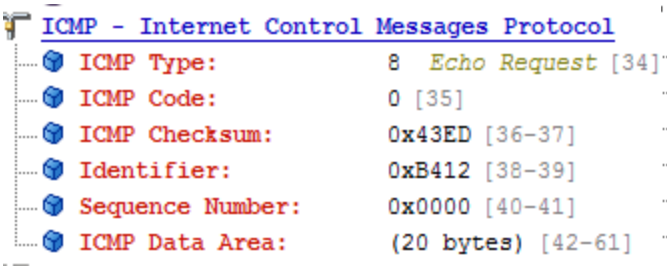


11. On remarque un champ extra bytes, on peut le considérer comme un padding, il contient 18 octets, donnant 18/64 = 28,125%

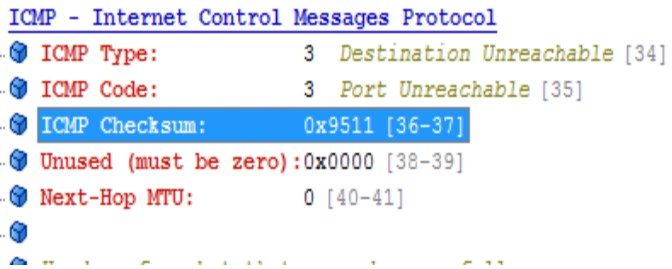


10. Partie Ping

1. La différence entre le champ ICMP pour une requête et une réponse est le ICMP Type et le ICMP Code. Dans le cas de notre requête, vu que la Machine B n'est pas dans la table ARP la destination n'est pas atteignable.



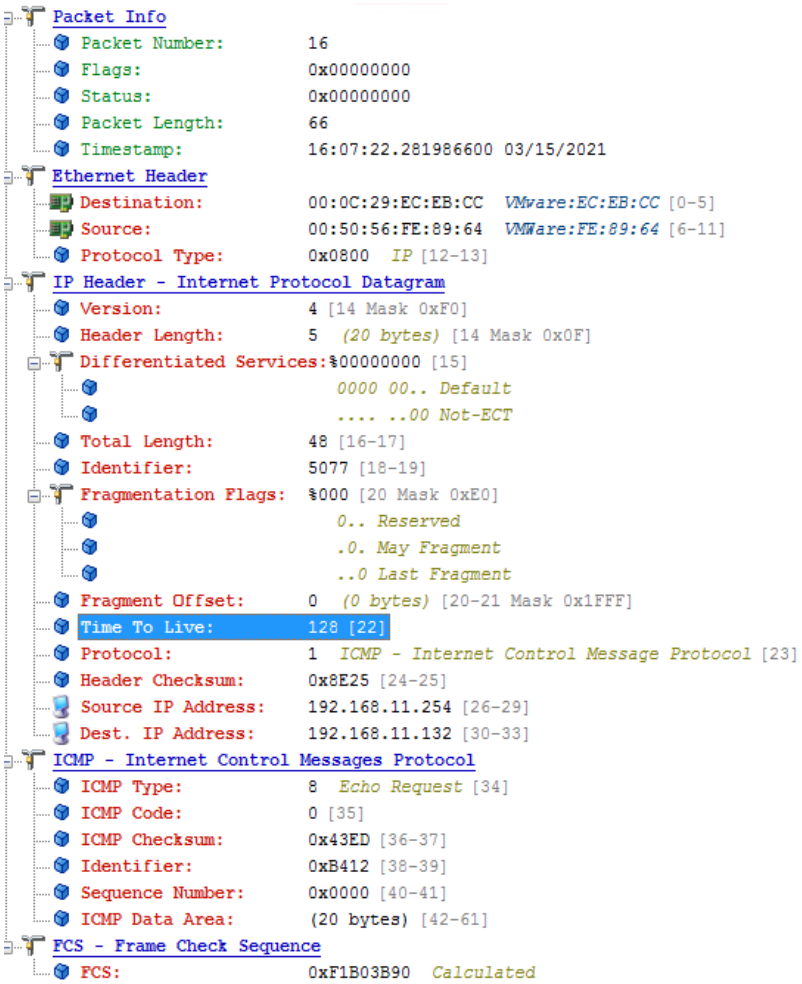
Réponse



Requête

2. La version IP est IPV4
3. Time to live est le nombre de “sauts” (nombre de passages à travers les passerelles) que peut faire le paquet avant qu’il soit jeté.

4.



La trame ICMP est encapsulée par le Ethernet Header, le IP Header, et le message ICMP, à la fin on a le frame check sequence.

11.Partie théorique

1. Lien 5

MAC Destination: A6.B7.C8.D9.E1.F2	MAC Source: A1:B2:C3:D4:E5:F6
IP Source: 132.207.29.102	IP Destination:132.207.29.103

Lien 6

MAC Destination: A6.B7.C8.D9.E1.F2	MAC Source: A1:B2:C3:D4:E5:F6
IP Source: 132.207.29.102	IP Destination: 132.207.29.103

Lien 4

MAC Destination: N/A	MAC Source: N/A
IP Source: N/A	IP Destination: N/A

Puisque l'adresse réseau du pc A est la même que celle du pc C, on peut envoyer directement l'information d'un pc vers l'autre.

2. Lien 5

MAC Destination: A2:B4:C4:D5:E6:F7	MAC Source: A1:B2:C3:D4:E5:F6
IP Source: 132.207.29.102	IP Destination:132.207.30.102

Lien 4

MAC Destination: A2:B4:C4:D5:E6:F7	MAC Source: A1:B2:C3:D4:E5:F6
IP Source: 132.207.29.102	IP Destination: 132.207.30.102

Lien 3

MAC Destination: A3:B4:C5:D7:E7:F8	MAC Source: A2:B4:C4:D5:E6:F7
IP Source: 132.207.29.102	IP Destination: 132.207.30.102

Lien 2

MAC Destination: A4:B5:C6:D7:E8:F9	MAC Source: A3:B4:C5:D7:E7:F8
IP Source: 132.207.29.102	IP Destination: 132.207.30.102

Lien 1

MAC Destination: A5:B6:C7:D9:E9:F1	MAC Source: A4:B5:C6:D7:E8:F9
IP Source: 132.207.29.102	IP Destination: 132.207.30.102