



**POLYTECHNIQUE  
MONTRÉAL**

UNIVERSITÉ  
D'INGÉNIERIE

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

Ethernet adapter Local Area Connection:		Ethernet adapter Local Area Connection:	
Connection-specific DNS Suffix	: localdomain	Connection-specific DNS Suffix	: localdomain
Description	: Intel(R) PRO/1000 MT Network Connection	Description	: Intel(R) PRO/1000 MT Network Connection
Physical Address	: 00-0C-29-EC-EB-CC	Physical Address	: 00-0C-29-26-06-31
DHCP Enabled	: Yes	DHCP Enabled	: Yes
Autoconfiguration Enabled	: Yes	Autoconfiguration Enabled	: Yes
Link-local IPv6 Address	: fe80::3ddb:3292:b056:2d15%10<Preferred>	Link-local IPv6 Address	: fe80::bd2e:ded0:c439:f42f%10<Preferred>
IPv4 Address	: 192.168.11.132<Preferred>	IPv4 Address	: 192.168.11.129<Preferred>
Subnet Mask	: 255.255.255.0	Subnet Mask	: 255.255.255.0
Lease Obtained	: Monday, March 15, 2021 3:04:20 PM	Lease Obtained	: Monday, March 15, 2021 3:04:26 PM
Lease Expires	: Monday, March 15, 2021 3:34:14 PM	Lease Expires	: Monday, March 15, 2021 3:34:19 PM
Default Gateway	: 192.168.11.2	Default Gateway	: 192.168.11.2
DHCP Server	: 192.168.11.254	DHCP Server	: 192.168.11.254
DHCPv6 IAID	: 234884137	DHCPv6 IAID	: 234884137
DHCPv6 Client DUID	: 00-01-00-01-14-BF-D5-2A-00-0C-29-66-D9-90	DHCPv6 Client DUID	: 00-01-00-01-14-BF-D5-2A-00-0C-29-66-D9-90
DNS Servers	: 192.168.11.2	DNS Servers	: 192.168.11.2
Primary WINS Server	: 192.168.11.2	Primary WINS Server	: 192.168.11.2
NetBIOS over Tcpip	: Enabled	NetBIOS over Tcpip	: Enabled

Machine A

MachineB

## 8. Partie DHCP (Dynamic Host Configuration Protocol)

### 1.

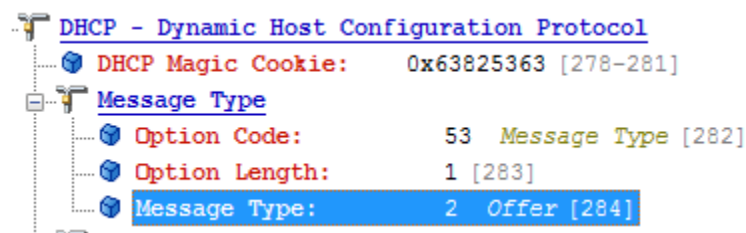
1	0.0.0.0	IP Broadcast	346	0.000000	DHCP	C DISCOVER 192.168.11.132 test-PC	
5	192.168.11.254	192.168.11.132	346	1.000278	DHCP	R OFFER 192.168.11.132	
6	0.0.0.0	IP Broadcast	356	1.000552	DHCP	C REQUEST 192.168.11.132 test-PC	
7	192.168.11.254	192.168.11.132	346	1.000754	DHCP	R ACK	DHCP Low Lease Time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

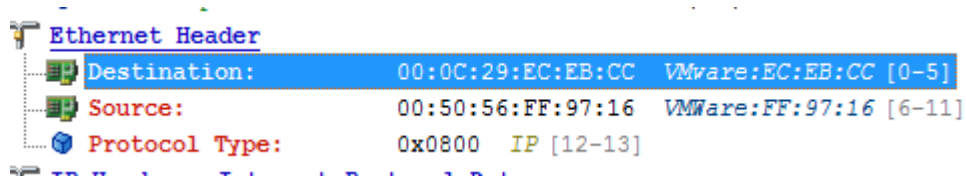
4.



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\

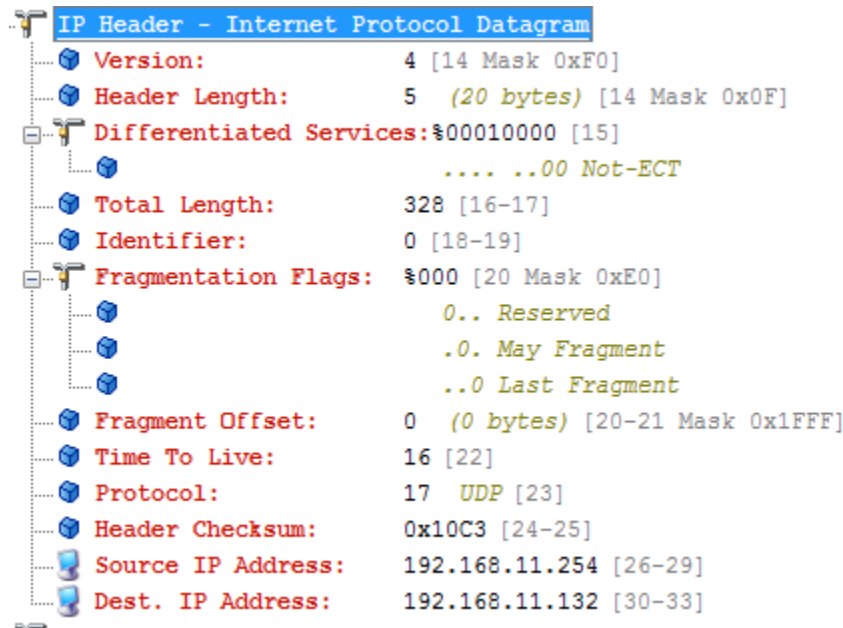


7.

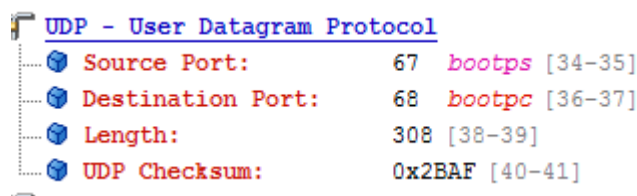


La destination est la machine A. La Source est le Serveur DHCP

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 à qui envoyer la trame.
- 2.

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

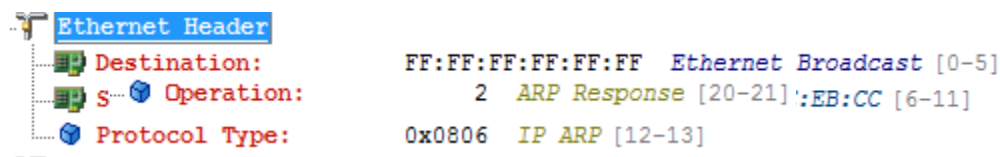
Avant

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



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



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

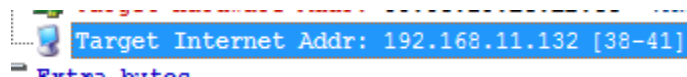
8. Le nœud qui correspond à la destination de la réponse ARP est notre machine locale (machine A).

9.

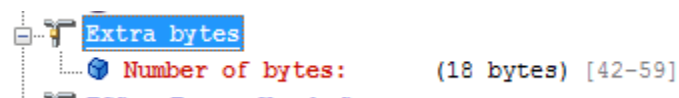


La séquence est un Ethernet Header, le message ARP, un padding et le frame check sequence

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.

ICMP - Internet Control Messages Protocol	ICMP - Internet Control Messages Protocol
ICMP Type: 8 <i>Echo Request</i> [34]	ICMP Type: 3 <i>Destination Unreachable</i> [34]
ICMP Code: 0 [35]	ICMP Code: 3 <i>Port Unreachable</i> [35]
ICMP Checksum: 0x43ED [36-37]	ICMP Checksum: 0x9511 [36-37]
Identifier: 0xB412 [38-39]	Unused (must be zero): 0x0000 [38-39]
Sequence Number: 0x0000 [40-41]	Next-Hop MTU: 0 [40-41]
ICMP Data Area: (20 bytes) [42-61]	
Réponse	Requête

- La version IP est IPV4
- 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.
- 
- 

<b>Packet Info</b>	
Packet Number:	16
Flags:	0x00000000
Status:	0x00000000
Packet Length:	66
Timestamp:	16:07:22.281986600 03/15/2021
<b>Ethernet Header</b>	
Destination:	00:0C:29:EC:EB:CC VMware:EC:EB:CC [0-5]
Source:	00:50:56:FE:89:64 VMware:FE:89:64 [6-11]
Protocol Type:	0x0800 IP [12-13]
<b>IP Header - Internet Protocol Datagram</b>	
Version:	4 [14 Mask 0xF0]
Header Length:	5 (20 bytes) [14 Mask 0x0F]
Differentiated Services:	%00000000 [15]
	0000 00.. Default
	.... ..00 Not-ECT
Total Length:	48 [16-17]
Identifier:	5077 [18-19]
Fragmentation Flags:	%000 [20 Mask 0xE0]
	0.. Reserved
	.0. May Fragment
	..0 Last Fragment
Fragment Offset:	0 (0 bytes) [20-21 Mask 0xFFFF]
Time To Live:	128 [22]
Protocol:	1 ICMP - Internet Control Message Protocol [23]
Header Checksum:	0x8E25 [24-25]
Source IP Address:	192.168.11.254 [26-29]
Dest. IP Address:	192.168.11.132 [30-33]
<b>ICMP - Internet Control Messages Protocol</b>	
ICMP Type:	8 <i>Echo Request</i> [34]
ICMP Code:	0 [35]
ICMP Checksum:	0x43ED [36-37]
Identifier:	0xB412 [38-39]
Sequence Number:	0x0000 [40-41]
ICMP Data Area:	(20 bytes) [42-61]
<b>FCS - Frame Check Sequence</b>	
FCS:	0xF1B03B90 Calculated

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