



**POLYTECHNIQUE
MONTRÉAL**

LE GÉNIE
EN PREMIÈRE CLASSE

INF3405 – Réseaux informatiques
TP 2

Frédéric Quenneville, 1714871
Samuel Rondeau, 1723869

Présenté à
Saida MAAROUFI

10 mai 2016
Polytechnique de Montréal

Poste de travail

L4708-04

N.B. : nous avons utilisé l'adresse IP 192.168.44.172 puisque nous avons eu des problèmes techniques avec l'adresse proposée dans l'énoncé du laboratoire.

Question 8.1

ipconfig /all (client)

```
C:\Windows\system32\cmd.exe
C:\Users\Administrator>ipconfig /all

Windows IP Configuration

Host Name . . . . . : test-PC
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address. . . . . : 00-0C-29-34-C1-D1
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::a3:db57:3198:859b%10<Preferred>
IPv4 Address. . . . . : 192.168.44.116<Preferred>
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, May 10, 2016 12:28:51 PM
Lease Expires . . . . . : Tuesday, May 10, 2016 4:28:51 PM
Default Gateway . . . . . :
DHCP Server . . . . . : 192.168.44.198
DHCPv6 IAID . . . . . : 234884137
DHCPv6 Client DUID. . . . . : 00-01-00-01-14-BF-D5-2A-00-0C-29-66-D9-90

DNS Servers . . . . . : fec0:0:0:ffff::1%1
                       fec0:0:0:ffff::2%1
                       fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter Local Area Connection* 11:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Teredo Tunneling Pseudo-Interface
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

Tunnel adapter 6T04 Adapter:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft 6to4 Adapter
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

Tunnel adapter isatap.{86C604D3-6490-455F-B6F2-5371E39B744D}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft ISATAP Adapter #3
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

C:\Users\Administrator>
```

Nom de l'hôte : test-PC

Adresse IPV4 : 192.168.44.116

Masque de sous-réseau : 255.255.255.0

Adresse MAC : 00-0C-29-34-C1-D1

Passerelle par défaut : 192.168.44.198

ipconfig /all (serveur)

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ipconfig /all

Windows IP Configuration

Host Name . . . . . : ServeurWindows
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address. . . . . : 00-0C-29-46-7D-CF
DHCP Enabled. . . . . : No
IP Address. . . . . : 192.168.44.172
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.44.198

C:\Documents and Settings\Administrator>
```

Nom de l'hôte : ServeurWindows

Adresse IPV4 : 192.168.44.172

Masque de sous-réseau : 255.255.255.0

Adresse MAC : 00-0C-29-46-7D-CF

Passerelle par défaut : 192.168.44.198

Question 9.3

Packet	Source	Destination	Flags	Size	Relative Time	Protocol	Summary	Expert
20	192.168.44.116	192.168.44.198		346	0.000000	DHCP	C RELEASE	
112	0.0.0.0	IP Broadcast		346	16.278851	DHCP	C DISCOVER 192.168.44.116 test-PC	
118	192.168.44.198	192.168.44.116		346	17.204099	DHCP	R OFFER 192.168.44.116	
119	0.0.0.0	IP Broadcast		356	17.204940	DHCP	C REQUEST 192.168.44.116 test-PC	
120	192.168.44.198	192.168.44.116		346	17.214544	DHCP	R ACK	

Les différents types de trames sont « Release », « Discover », « Offer », « Request », « Ack » et « Inform » (ce dernier absent de la présente capture d'écran mais figurant dans un de nos précédents tests).

Question 9.4

```
..... Fragment Offset:      0  (0 bytes) [20-21 Mask 0x1FFF]
..... Time To Live:         16 [22]
..... Protocol:             17  UDP [23]
..... Header Checksum:      0xCF0A [24-25]
..... Source IP Address:    192.168.44.198 [26-29]
..... Dest. IP Address:     192.168.44.116 [30-33]
..... UDP - User Datagram Protocol
```

La trame DHCP « offer » envoie une confirmation de la passerelle à la machine requérante de l'adresse IP attribuée (192.168.44.116).

Question 9.5

```
..... Ethernet Header
..... Destination:          00:0C:29:34:C1:D1  VMware:34:C1:D1 [0-5]
..... Source:               00:19:D1:25:2E:45  Intel:25:2E:45 [6-11]
..... Protocol Type:        0x0800  IP [12-13]
```

La valeur du champ destination est l'adresse MAC du client, c'est-à-dire 00:0C:29:34:C1:D1. C'est une adresse physique.

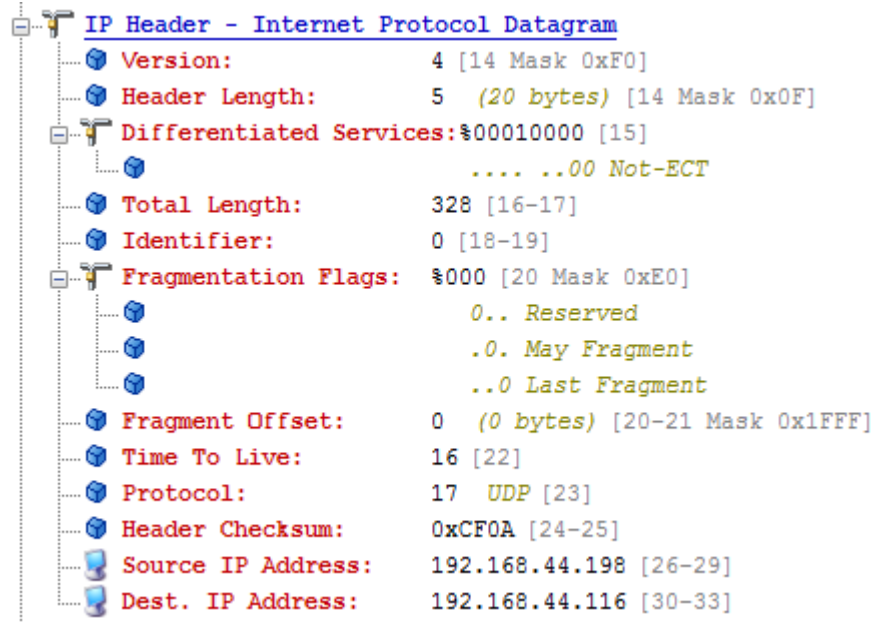
Question 9.6

La valeur du champ source est l'adresse MAC de la passerelle (routeur), c'est-à-dire 00:19:D1:25:2E:45. C'est une adresse physique.

Question 9.7

La valeur du type de protocole est 0x0800 ce qui signifie que la trame utilise le protocole IP.

Question 9.8



The image shows a Wireshark packet capture of an IP header. The packet is expanded to show the following fields:

IP Header - Internet Protocol Datagram	
Version:	4 [14 Mask 0xF0]
Header Length:	5 (20 bytes) [14 Mask 0x0F]
Differentiated Services:	%00010000 [15]00 Not-ECT
Total Length:	328 [16-17]
Identifier:	0 [18-19]
Fragmentation Flags:	%000 [20 Mask 0xE0] 0.. Reserved .0. May Fragment ..0 Last Fragment
Fragment Offset:	0 (0 bytes) [20-21 Mask 0x1FFF]
Time To Live:	16 [22]
Protocol:	17 UDP [23]
Header Checksum:	0xCF0A [24-25]
Source IP Address:	192.168.44.198 [26-29]
Dest. IP Address:	192.168.44.116 [30-33]

C'est l'entête IP.

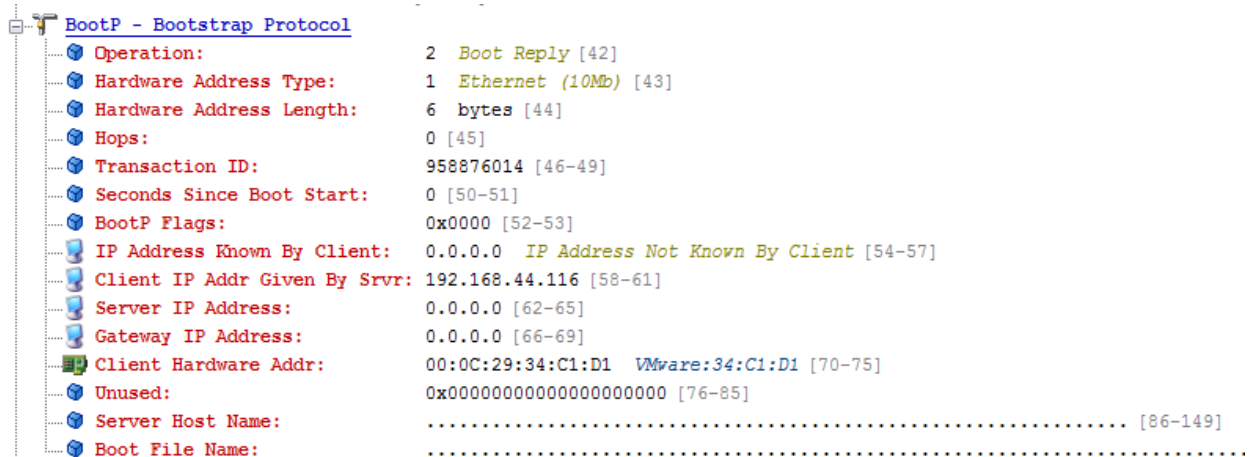
Question 9.9

L'adresse IP source est 192.168.44.198. C'est l'adresse IP de la passerelle.

Question 9.10

La valeur de TTL est 16 et la valeur du protocole est 17 soit UDP.

Question 9.11



The image shows a Wireshark packet capture of a BootP packet. The packet is expanded to show the following fields:

BootP - Bootstrap Protocol	
Operation:	2 Boot Reply [42]
Hardware Address Type:	1 Ethernet (10Mb) [43]
Hardware Address Length:	6 bytes [44]
Hops:	0 [45]
Transaction ID:	958876014 [46-49]
Seconds Since Boot Start:	0 [50-51]
BootP Flags:	0x0000 [52-53]
IP Address Known By Client:	0.0.0.0 IP Address Not Known By Client [54-57]
Client IP Addr Given By Srwr:	192.168.44.116 [58-61]
Server IP Address:	0.0.0.0 [62-65]
Gateway IP Address:	0.0.0.0 [66-69]
Client Hardware Addr:	00:0C:29:34:C1:D1 VMware:34:C1:D1 [70-75]
Unused:	0x00000000000000000000 [76-85]
Server Host Name: [86-149]
Boot File Name:

Le protocole de niveau 4 est Bootstrap (utilise UDP).

Question 9.12

La valeur de ce champ est 192.168.44.116. C'est l'adresse IP privée du client sur le réseau local, laquelle le serveur utilise pour communiquer avec le client.

Question 9.13



Il s'agit du champ « Message Type ». Sa valeur est de 2, signifiant que c'est un message de type « Offer ».

Question 9.14

Les champs sont « Message Type », « Server Identifier », « IP Adress Lease Time » et « Subnet Mask ».

Question 9.15

La valeur de option code est de 54. Cela signifie, combiné avec la valeur de « Option Length », que les quatre prochains octets sont l'identifiant du serveur. On en déduit qu'il s'agit de l'adresse IP de la passerelle, 192.168.44.198.

Question 9.16

La valeur de ce champ signifie la durée en secondes pendant laquelle l'adresse IP est réservée. À la fin de cette durée, une nouvelle adresse pourrait être attribuée par le serveur.

Question 9.17

14400 secondes.

Question 10.1

```
Administrator: C:\Windows\system32\cmd.exe
Connection-specific DNS Suffix . : 
Link-local IPv6 Address . . . . . : fe80::a3:db57:3198:859b%10
IPv4 Address. . . . . : 192.168.44.116
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 

Tunnel adapter isatap.{86C604D3-6490-455F-B6F2-5371E39B744D}:

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

Tunnel adapter Local Area Connection* 11:

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

Tunnel adapter 6T04 Adapter:

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

C:\Users\Administrator>arp -a

Interface: 192.168.44.116 --- 0xa
 Internet Address      Physical Address      Type
 169.254.33.2          00-0c-29-8e-fa-f1     dynamic
 192.168.44.27         00-0c-29-05-57-bf     dynamic
 192.168.44.104        90-e2-ba-46-32-03     dynamic
 192.168.44.172        00-0c-29-46-7d-cf     dynamic
 192.168.44.198        00-19-d1-25-2e-45     dynamic
 192.168.44.255        ff-ff-ff-ff-ff-ff     static
 224.0.0.22            01-00-5e-00-00-16     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

C:\Users\Administrator>_
```

La dernière ligne de donnée dynamique sont les adresses IP et physique de la passerelle.

Question 10.2

```
Administrator: C:\Windows\system32\cmd.exe
Connection-specific DNS Suffix . : 
Link-local IPv6 Address . . . . . : fe80::a3:db57:3198:859b%10
IPv4 Address. . . . . : 192.168.44.116
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 

Tunnel adapter isatap.{86C604D3-6490-455F-B6F2-5371E39B744D}:

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

Tunnel adapter Local Area Connection* 11:

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

Tunnel adapter 6T04 Adapter:

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

C:\Users\Administrator>arp -a

Interface: 192.168.44.116 --- 0xa
Internet Address      Physical Address      Type
169.254.33.2          00-0c-29-8e-fa-f1    dynamic
192.168.44.27         00-0c-29-05-57-bf    dynamic
192.168.44.104        90-e2-ba-46-32-03    dynamic
192.168.44.172        00-0c-29-46-7d-cf    dynamic
192.168.44.198        00-19-d1-25-2e-45    dynamic
192.168.44.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    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

C:\Users\Administrator>arp -d 192.168.44.172

C:\Users\Administrator>arp -a

Interface: 192.168.44.116 --- 0xa
Internet Address      Physical Address      Type
169.254.33.2          00-0c-29-8e-fa-f1    dynamic
192.168.44.27         00-0c-29-05-57-bf    dynamic
192.168.44.104        90-e2-ba-46-32-03    dynamic
192.168.44.198        00-19-d1-25-2e-45    dynamic
192.168.44.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    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

C:\Users\Administrator>_
```


Question 10.4

```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>ping 192.168.44.172

Pinging 192.168.44.172 with 32 bytes of data:
Reply from 192.168.44.172: bytes=32 time<1ms TTL=128
Reply from 192.168.44.172: bytes=32 time<1ms TTL=128
Reply from 192.168.44.172: bytes=32 time<1ms TTL=128
Reply from 192.168.44.172: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.44.172:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>arp -a

Interface: 192.168.44.116 --- 0xa
Internet Address      Physical Address      Type
169.254.33.2          00-0c-29-8e-fa-f1    dynamic
192.168.44.27         00-0c-29-05-57-bf    dynamic
192.168.44.104        90-e2-ba-46-32-03    dynamic
192.168.44.172        00-0c-29-46-7d-cf    dynamic
192.168.44.198        00-19-d1-25-2e-45    dynamic
192.168.44.255        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

C:\Users\Administrator>_
```

L'adresse IP et physique du serveur est revenue dans la cache ARP. C'est normal puisque nous avons fait « ping » juste avant. Ainsi la traduction de l'adresse logique vers physique a été à nouveau ajoutée dans la cache ARP.

On remarque aussi une nouvelle entrée (IP : 224.0.0.251).

Question 10.5

Packet	Source	Destination	Flags	Size	Relative Time	Protocol	Summary
1	Intelorate:2A:D...	Ethernet Broadcast		64	0.000000	ARP Request	192.168.20.198 = ?
4	Intelorate:2A:D...	Ethernet Broadcast		64	1.000110	ARP Request	192.168.20.198 = ?
6	Intelorate:2A:D...	Ethernet Broadcast		64	2.000060	ARP Request	192.168.20.198 = ?
41	Intelorate:2A:D...	Ethernet Broadcast		64	20.005069	ARP Request	192.168.20.198 = ?
44	Intelorate:2A:D...	Ethernet Broadcast		64	21.004960	ARP Request	192.168.20.198 = ?
45	Intelorate:2A:D...	Ethernet Broadcast		64	22.004950	ARP Request	192.168.20.198 = ?
443	Intelorate:2A:D...	Ethernet Broadcast		64	40.008520	ARP Request	192.168.20.198 = ?
446	Intelorate:2A:D...	Ethernet Broadcast		64	41.008477	ARP Request	192.168.20.198 = ?
453	Intelorate:2A:D...	Ethernet Broadcast		64	42.008521	ARP Request	192.168.20.198 = ?

La taille de chaque trame ARP est de 64 octets.

Question 10.6

Ethernet Header	
Destination:	FF:FF:FF:FF:FF:FF Ethernet Broadcast [0-5]
Source:	00:1C:C0:2A:D5:75 Intelorate:2A:D5:75 [6-11]
Protocol Type:	0x0806 IP ARP [12-13]

La valeur de ce champ est 0x0806 signifiant qu'il s'agit du protocole IP ARP.

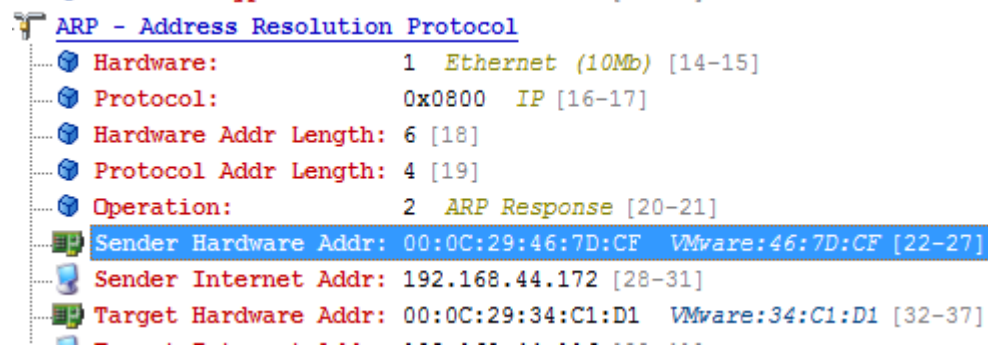
Question 10.7

Hardware Addr Length:	6 [18]
Protocol Addr Length:	4 [19]
Operation:	2 ARP Response [20-21]
Sender Hardware Addr:	00:0C:29:46:7D:CF VMware
Sender Internet Addr:	192.168.44.172 [28-31]
Target Hardware Addr:	00:0C:29:34:C1:D1 VMware

Hardware Addr Length:	6 [18]
Protocol Addr Length:	4 [19]
Operation:	1 ARP Request [20-21]
Sender Hardware Addr:	00:1C:C0:2A:D5:75 Intelorate:2A:D5:75
Sender Internet Addr:	192.168.20.199 [28-31]
Target Hardware Addr:	00:00:00:00:00:00 Xerox:00:00:00 (ig)
Target Internet Addr:	192.168.20.198 [38-41]

Il s'agit de la valeur de « Operation ». Elle est de 2 dans le cas d'une réponse et de 1 dans le cas d'une requête.

Question 10.8



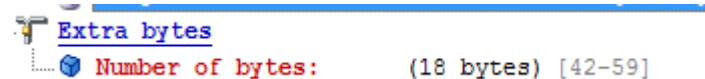
L'adresse physique de l'expéditeur de la réponse à « ping » est 00:0C:29:46:7D:CF. C'est l'adresse physique du serveur.

Question 10.9



La séquence d'encapsulation est 0xE33766EF.

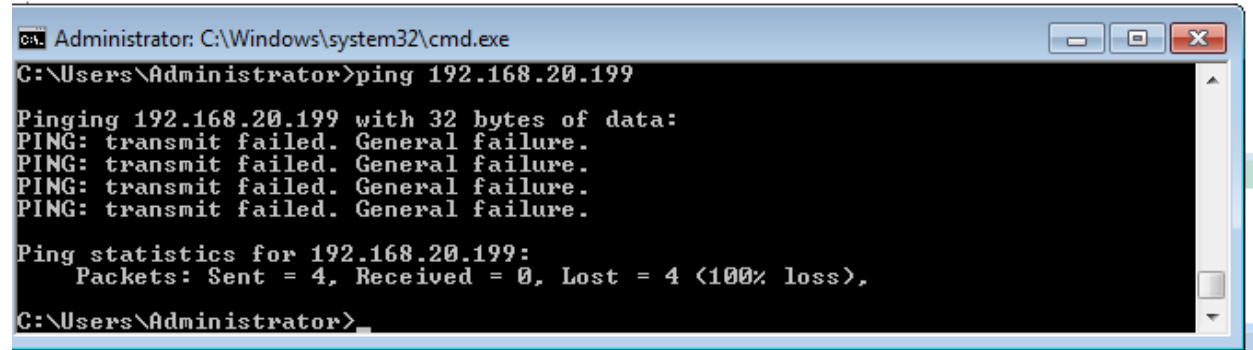
Question 10.10



C'est un nombre additionnel d'octets ajoutés (valeur 00) afin que la taille de la trame soit d'exactement 64 octets. Dans ce cas il s'agit de 28% (18/64).

Question 10.11

```
Operation: 1 ARP Request [20-21]
Sender Hardware Addr: 00:1C:C0:2A:D5:75 Intelorator:2A:D5:75 [22-27]
Sender Internet Addr: 192.168.20.199 [28-31]
```



The screenshot shows a Windows command prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The user has entered the command "ping 192.168.20.199". The output shows four failed ping attempts, each with the message "PING: transmit failed. General failure." followed by "Ping statistics for 192.168.20.199: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),".

La valeur de l'adresse MAC de l'expéditeur est 00:1C:C0:2A:D5:75. Ce nœud ne fait pas parti du réseau.

Question 10.12

```
Target Hardware Addr: 00:00:00:00:00:00 Xerox:00:00:00 (ignored) [32-37]
Target Internet Addr: 192.168.20.198 [38-41]
```

La valeur de l'adresse MAC de la destination est 00:00:00:00:00:00. Cette adresse ne correspond à aucun nœud car la requête ARP connaît seulement l'adresse logique de la cible et non son adresse physique.

Question 10.13

```
Sender Hardware Addr: 00:0C:29:46:7D:CF VMware:46:7D:CF [22-27]
Sender Internet Addr: 192.168.44.172 [28-31]
Target Hardware Addr: 00:0C:29:34:C1:D1 VMware:34:C1:D1 [32-37]
Target Internet Addr: 192.168.44.116 [38-41]
```

La réponse à la requête se trouve dans le champ « Sender Hardware Addr ». Elle contient l'adresse de la destination de la requête « ping » soit celle du serveur.