

Test de vos connaissances
Sécurité des réseaux
Commandes réseaux
Sniffer réseaux Wireshark
Adressage IP

Nom et prénom : abdel-malik fofana 22218511

Exercice 1 - Commandes réseau

Pour les postes sous UNIC/LINUX : veuillez ajouter les répertoires /usr/bin, /sbin et /usr/sbin dans la variable d'environnement PATH.

Les commandes réseaux (unix et windows) de base sont:

- **Ifconfig (ipconfig)** affiche ou configure les interfaces réseaux de la machine, l'option -a permet de connaître toutes les interfaces;
 - -a (/all) plus d'infos sont affichées;
- **route** affiche ou configure la table de routage de la machine:
 - -F (PRINT): table de routage du noyau;
 - -n: affiche les adresse IP (pas de résolution DNS);
- **netstat** affiche de nombreuses informations sur la configuration réseau de la machine:
 - -i infos sur les interfaces;
 - -r infos sur la table de routage;
 - -t connexions tcp;
 - -u connexions udp;
 - -l ports en écoute;
 - -c affiche les infos en continu;
 - -n affiche les adresses IP (pas de résolution DNS).
- **arp** permet d'afficher le cache ARP de la machine. L'option -n indique de ne pas faire de résolution DNS;
 - -a infos sur la table arp;
- **ping** permet d'envoyer des ICMP ECHO_REQUEST vers une machine du réseau.
- **tracroute (tracert)** affiche la route suivie par les datagrammes IP entre la machine locale et une autre machine. L'option -n indique de ne pas faire de résolution DNS;
- **host (nslookup)** interroge un serveur DNS pour connaître l'adresse IP d'une machine à partir de son nom ou l'inverse;
- **dhclient -r eth0 (ipconfig /release) et dhclient eth0 (ipconfig /renew)** : met fin à votre bail DHCP courant et interroge le serveur DHCP pour renouveler votre bail

1. Tester chacune de ces commandes les unes après les autres et donner:

- la liste des interfaces sur votre machine ;

```
(maliki@Maliki-club)~$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    ether 02:42:3d:5d:bc:ef txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether c8:5a:cf:c1:e4:69 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Boucle locale)
    RX packets 1446 bytes 117880 (115.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1446 bytes 117880 (115.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.9.186 netmask 255.255.224.0 broadcast 10.10.31.255
    inet6 fe80::7399:737f:39ed:75d prefixlen 64 scopeid 0x20<link>
    ether f4:26:79:af:18:ba txqueuelen 1000 (Ethernet)
    RX packets 441727 bytes 504113833 (480.7 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 152878 bytes 32499842 (30.9 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

les interfaces sont : docker0 , eth0 , lo et wlan0

- l'adresse IP de votre machine ;

ip de la machine : 10.10.9.186

- le nom de la machine d'adresse IP **193.50.159.71**;

```
(root@Maliki-club)-[/home/maliki]
# nslookup 193.50.159.71
** server can't find 71.159.50.193.in-addr.arpa: NXDOMAIN
```

nslookup ne marchait pas donc j'ai utilisé whois

```
~$ whois 193.50.159.71
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See https://apps.db.ripe.net/docs/HTML-Terms-And-Conditions
%
% Note: this output has been filtered.
% To receive output for a database update, use the "-B" flag.
%
% Information related to '193.50.159.0 - 193.50.159.255'
% Abuse contact for '193.50.159.0 - 193.50.159.255' is 'certsvp@renater.fr'

inetnum:        193.50.159.0 - 193.50.159.255
netname:        FR-U-GUSTAVE-EIFFEL
descr:          Universite Gustave Eiffel
remarks:        **** BEGIN INFORMATION FROM OLD OBJECT ****
remarks:        netname:      FR-U-MARNE-NOISY
remarks:        descr:        Universite Paris-Est Marne-la-Vallee
remarks:        descr:        5 bld Descartes, Champs sur Marne
remarks:        descr:        77454 Marne La Vallee cedex 2
remarks:        **** END INFORMATION FROM OLD OBJECT ****
country:        FR
admin-c:        GPRT293-RIPE
tech-c:         GPRT293-RIPE
status:         ASSIGNED PA
mnt-by:         RENATER-MNT
remarks:        changed:      rensvp@renater.fr 20001030
remarks:        changed:      rensvp@renater.fr 20230822
created:        1970-01-01T00:00:00Z
last-modified:  2023-08-24T07:15:35Z
source:         RIPE

role:            U-GUSTAVE-EIFFEL
address:         FRANCE
nic-hdl:        GPRT293-RIPE
mnt-by:         RENATER-MNT
remarks:        changed:      rensvp@renater.fr 20230718
created:        2023-03-27T11:24:03Z
last-modified:  2023-08-24T06:27:07Z
```

nom de la machine 193.50.159.71 est FR-U-GUSTAVE-EIFFEL (Universite Gustave Eiffel)

- l'adresse IP de la machine de nom « www.yahoo.fr »

```
(root@Maliki-club)-[/home/maliki]
# nslookup www.yahoo.fr

Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
www.yahoo.fr canonical name = rc.yahoo.com.
rc.yahoo.com canonical name = src.g03.yahoodns.net.
Name:   src.g03.yahoodns.net
Address: 13.49.212.207
Name:   src.g03.yahoodns.net
Address: 13.50.184.192
```

l'adresse ip de www.yahoo.fr est 13.49.212.207 et 13.50.184.192

- l'adresse MAC de la carte réseau ;
Dans le ifconfig de tout à l'heure on a vu que l'adresse mac est : c8:5a:cf:c1:e4:69 pour ethernet
(et f4:26:79:af:18:ba pour le wifi)
- l'adresse et le masque de votre réseau ;
netmask 255.255.224.0
10.10.9.186/19
l'adresse est : 10.10.9.0
- la table de routage de votre machine.
Voici la table de routage de ma machine

```
(maliki@Maliki-club)-[~]
$ route -F

Table de routage IP du noyau

```

Destination	Passerelle	Genmask	Indic	Metric	Ref	Use	Iface
default	_gateway	0.0.0.0	UG	600	0	0	wlan0
10.10.0.0	0.0.0.0	255.255.224.0	U	600	0	0	wlan0
172.17.0.0	0.0.0.0	255.255.0.0	U	0	0	0	docker0

- La liste des adresses MAC des machines en communication avec vous.
Voici l'adresse mac en communication avec moi : 00:50:56:9f:38:3e

```
(maliki@Maliki-club)-[~]
$ arp -n

Adresse          TypeMap AdresseMat      Indicateurs      Iface
10.10.8.2         ether  00:50:56:9f:38:3e    C                wlan0
```

- L'adresse MAC de votre routeur (gateway) par défaut
l'adresse mac est : 00:50:56:9f:38:3e (voir screen du dessus)

2. Donner la liste des routeurs par lesquels passent des datagrammes entre vous et la machine www.google.com.

```
(maliki@Maliki-club)-[~]
$ traceroute www.google.com
traceroute to www.google.com (142.250.74.228), 30 hops max, 60 byte packets
 1 _gateway (10.10.8.2)  3.550 ms  3.478 ms  3.456 ms
 2 193.51.81.241 (193.51.81.241)  5.110 ms  5.087 ms  5.066 ms
 3 195.221.127.165 (195.221.127.165)  4.229 ms  5.012 ms  4.984 ms
 4 vl165-te0-1-0-8-ren-nr-jussieu-rtr-091.noc.renater.fr (193.51.181.102)  5.681 ms  6.144 ms  6.117 ms
 5 xe-0-0-13-paris2-rtr-131.noc.renater.fr (193.51.180.106)  5.576 ms  xe1-1-8-paris2-rtr-131.noc.renater.fr (193.51.177.114)  6.077 ms  xe-0-0-23-ren-nr-paris2-rtr-131.noc.renater.fr (193.55.204.215)  5.585 ms
 6 hu0-4-0-1-ren-nr-paris2-rtr-092.noc.renater.fr (193.51.177.83)  5.517 ms  2.583 ms  3.048 ms
 7 72.14.214.160 (72.14.214.160)  3.724 ms  4.559 ms *
 8 108.170.244.161 (108.170.244.161)  4.476 ms  108.170.244.225 (108.170.244.225)  5.254 ms  5.237 ms
 9 142.250.234.41 (142.250.234.41)  5.208 ms  5.187 ms  5.169 ms
10 paris40-in-f4.1e100.net (142.250.74.228)  5.161 ms  5.142 ms  5.124 ms
```

voici les routeur : [_gateway](#) , [193.51.81.241](#) , [195.221.127.165](#) ,
[vl165-te0-1-0-8-ren-nr-jussieu-rtr-091.noc.renater.fr](#) , [xe-0-0-13-paris2-rtr-131.noc.renater.fr](#) ,
[hu0-4-0-1-ren-nr-paris2-rtr-092.noc.renater.fr](#) , [72.14.214.160](#) , [108.170.244.161](#) , [142.250.234.41](#)
[,par10s40-in-f4.1e100.net](#)

3. En utilisant la commande **ping** déterminer la valeur du « **Round Trip Time** » moyen (en ms) entre votre machine et mailhost.math-info.univ-paris5.fr. Quelle est la signification du paramètre « RTT » ?

```
(maliki@Maliki-club)-[~]
$ ping mailhost.math-info.univ-paris5.fr.
PING mars.math-info.univ-paris5.fr (193.48.200.18) 56(84) bytes of data.
^C
--- mars.math-info.univ-paris5.fr ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1005ms

(maliki@Maliki-club)-[~]
$ ping mailhost.math-info.univ-paris5.fr
PING mars.math-info.univ-paris5.fr (193.48.200.18) 56(84) bytes of data.
^C
--- mars.math-info.univ-paris5.fr ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2047ms
```

Le ping ne marchait pas (comme beaucoup de mes camarades) j'ai donc fait avec google

```
(maliki@Maliki-club)-[~]
$ ping google.com
PING google.com(par21s23-in-x0e.1e100.net (2a00:1450:4007:81a::200e)) 56 data bytes
64 bytes from par21s23-in-x0e.1e100.net (2a00:1450:4007:81a::200e): icmp_seq=1 ttl=115 time=2.95 ms
64 bytes from par21s23-in-x0e.1e100.net (2a00:1450:4007:81a::200e): icmp_seq=2 ttl=115 time=4.70 ms
64 bytes from par21s23-in-x0e.1e100.net (2a00:1450:4007:81a::200e): icmp_seq=3 ttl=115 time=51.6 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 2.953/19.753/51.605/22.533 ms
```

le temp moyenne est 19.753 ms

Le paramètre « RTT » (Round Trip Time) représente le temps nécessaire pour qu'un paquet de données soit envoyé d'un hôte à un autre, et que la réponse soit reçue.

4. Demander l'adresse IP de votre voisin. À l'aide des commandes ci-dessus, trouver son adresse MAC.

[08:00:27:eb:59:61](#) est l'adresse mac de ma machine virtuelle

```
(root@Maliki-club)-[/home/maliki]
# arp -a
? (172.20.10.9) at 08:00:27:eb:59:61 [ether] on wlan0
_gateway (172.20.10.1) at 3e:7d:0a:06:fd:64 [ether] on wlan0
```

on peut le vérifier ici dans la machine virtuelle en faisant ifconfig :

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:eb:59:61 brd ff:ff:ff:ff:ff:ff
    inet 172.20.10.9/28 brd 172.20.10.15 scope global dynamic noprefixroute enp0s3
        valid_lft 86363sec preferred_lft 86363sec
```

5. Trouver l'adresse IP du serveur **www.yahoo.fr** ainsi que l'adresse IP de votre serveur DNS.

```
(root@Maliki-club)-[/home/maliki]
# nslookup www.yahoo.fr

Server:          172.20.10.1
Address:         172.20.10.1#53

Non-authoritative answer:
www.yahoo.fr     canonical name = rc.yahoo.com.
rc.yahoo.com     canonical name = src.g03.yahoodns.net.
Name:   src.g03.yahoodns.net
Address: 13.49.212.207
Name:   src.g03.yahoodns.net
Address: 13.50.184.192
```

l'adresse ip de www.yahoo.fr est 13.49.212.207
et l'adresse ip de mon serveur dns est : 172.20.10.1

```
(root@Maliki-club)-[/home/maliki]
# netstat -nr

Table de routage IP du noyau
Destination  Passerelle  Genmask      Indic  MSS  Fenêtre  irtt  Iface
0.0.0.0      172.20.10.1 0.0.0.0      UG     0 0      0 0    wlan0
172.17.0.0   0.0.0.0     255.255.0.0  U      0 0      0 0    docker0
172.20.10.0  0.0.0.0     255.255.255.240 U      0 0      0 0    wlan0
```

6. éditer le fichier /etc/hosts (windows/system32/drivers/etc/hosts) et décrire son contenu.

```
Ouvrir  hosts
/etc

1 127.0.0.1    localhost
2 127.0.1.1    Maliki-club.rev.sfr.net Maliki-club
3
4 # The following lines are desirable for IPv6 capable hosts
5 ::1         localhost ip6-localhost ip6-loopback
6 ff02::1     ip6-allnodes
7 ff02::2     ip6-allrouters
8
9
```

Le fichier /etc/hosts est une configuration système sur Linux utilisée pour mapper des adresses IP à des noms d'hôte locaux. Voici un résumé des lignes dans ce fichier particulier :

- 127.0.0.1 localhost : Adresse IP de bouclage local associée à localhost.
- 127.0.1.1 Maliki-club.rev.sfr.net Maliki-club : Spécifique à certaines distributions Linux, définissant le nom d'hôte de la machine.
- Lignes IPv6 : Configuration pour IPv6, associant des adresses IPv6 à des noms d'hôte.
- ::1 localhost ip6-localhost ip6-loopback : Adresse IPv6 de bouclage local associée à plusieurs noms d'hôte IPv6.
- ff02::1 ip6-allnodes : Adresse multicast pour tous les nœuds IPv6.
- ff02::2 ip6-allrouters : Adresse multicast pour tous les routeurs IPv6.

7. éditer le fichier /etc/services (windows/system32/drivers/etc/services) et décrire son contenu.

```
Ouvrir services [Lecture seule]
/etc
1 # Network services, Internet style
2 #
3 # Updated from https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml .
4 #
5 # New ports will be added on request if they have been officially assigned
6 # by IANA and used in the real-world or are needed by a debian package.
7 # If you need a huge list of used numbers please install the nmap package.
8
9 tcpmux      1/tcp          # TCP port service multiplexer
10 echo       7/tcp
11 echo       7/udp
12 discard    9/tcp          sink null
13 discard    9/udp          sink null
14 systat     11/tcp         users
15 daytime    13/tcp
16 daytime    13/udp
17 netstat    15/tcp
18 qotd       17/tcp          quote
19 chargen    19/tcp         ttytst source
20 chargen    19/udp         ttytst source
21 ftp-data   20/tcp
22 ftp        21/tcp
23 fsp        21/udp         fspd
```

Le fichier `/etc/services` répertorie les services réseau associés à des numéros de port spécifiques. Il fournit une correspondance entre les noms de service et les numéros de port, facilitant la configuration des services réseau sur un système.

8. Modifier vos fichiers systèmes pour pouvoir utiliser la commande « ping » vers la machine de votre voisin en remplaçant son adresse IP par le nom « `voisin.univ-paris1.fr` » et l'alias « `voisin` ».

```
(root@Maliki-club)-[/home/maliki]
# ping voisin.univ-paris1.fr
PING voisin.univ-paris1.fr (172.20.10.9) 56(84) bytes of data.
64 bytes from voisin.univ-paris1.fr (172.20.10.9): icmp_seq=1 ttl=64 time=0.250 ms
64 bytes from voisin.univ-paris1.fr (172.20.10.9): icmp_seq=2 ttl=64 time=0.625 ms
^C
--- voisin.univ-paris1.fr ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1032ms
rtt min/avg/max/mdev = 0.250/0.437/0.625/0.187 ms

(root@Maliki-club)-[/home/maliki]
# ping voisin
PING voisin (172.20.10.9) 56(84) bytes of data.
64 bytes from voisin.univ-paris1.fr (172.20.10.9): icmp_seq=1 ttl=64 time=0.534 ms
64 bytes from voisin.univ-paris1.fr (172.20.10.9): icmp_seq=2 ttl=64 time=0.690 ms
^C
--- voisin ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1010ms
rtt min/avg/max/mdev = 0.534/0.612/0.690/0.078 ms

(root@Maliki-club)-[/home/maliki]
```

j'ai ajouter au fichier `/etc/hosts` : ```\n172.20.10.9 voisin.univ-paris1.fr\n172.20.10.9 voisin\n```\n

9. en renouvelant votre bail, indiquer l'adresse IP de votre serveur DHCP et la durée de votre bail.

```
maliki@maliki-VirtualBox:~$ sudo dhclient -v
[sudo] Mot de passe de maliki :
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/enp0s3/08:00:27:eb:59:61
Sending on   LPF/enp0s3/08:00:27:eb:59:61
Sending on   Socket/fallback
DHCPDISCOVER on enp0s3 to 255.255.255.255 port 67 interval 3 (xid=0xddecf826)
DHCPOFFER of 172.20.10.9 from 172.20.10.1
DHCPREQUEST for 172.20.10.9 on enp0s3 to 255.255.255.255 port 67 (xid=0x26f8ecdd)
DHCPREQUEST for 172.20.10.9 on enp0s3 to 255.255.255.255 port 67 (xid=0x26f8ecdd)
DHCPACK of 172.20.10.9 from 172.20.10.1 (xid=0xddecf826)
RTNETLINK answers: File exists
bound to 172.20.10.9 -- renewal in 37493 seconds.
maliki@maliki-VirtualBox:~$
```

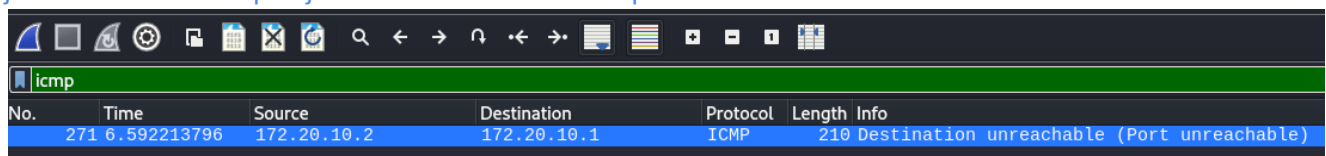
l'adresse IP du serveur DHCP est 172.20.10.1 et la durée du bail est indiquée comme 37493 seconds.

Exercice 2 – Travaux pratiques : Sniffer réseaux Wireshark

Le logiciel **Wireshark** permet de capturer l'ensemble des trames Ethernet reçues et envoyées à travers une interface. Pour des raisons de confidentialité, pour pouvoir réaliser une capture, vous devez avoir les droits root. Cependant vous pouvez charger une capture à partir d'un fichier et utiliser Wireshark pour l'analyser.

En utilisant les commandes réseaux ci-dessus ainsi que votre navigateur web, réaliser plusieurs captures avec wireshark et donner une description des différents échanges suivants :

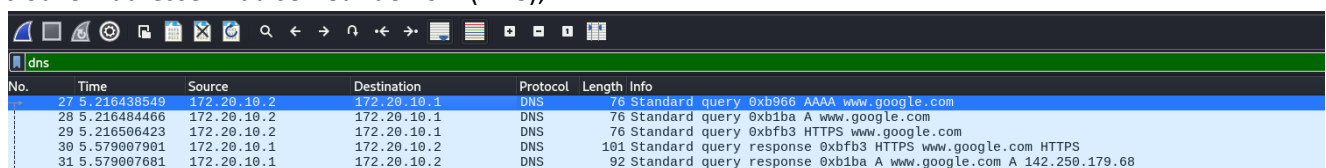
1. trouvez l'adresse IP de votre routeur de sortie ;
je sais que icmp est un protocole de la couche 3 comme le routeur
j'ai donc cherché icmp et je suis tombé sur l'adresse ip du routeur



No.	Time	Source	Destination	Protocol	Length	Info
271	6.592213796	172.20.10.2	172.20.10.1	ICMP	210	Destination unreachable (Port unreachable)

172.20.10.2 est mon adress ip du moment et 172.20.10.1 est mon routeur

2. trouver l'adresse IP du serveur de nom (DNS);

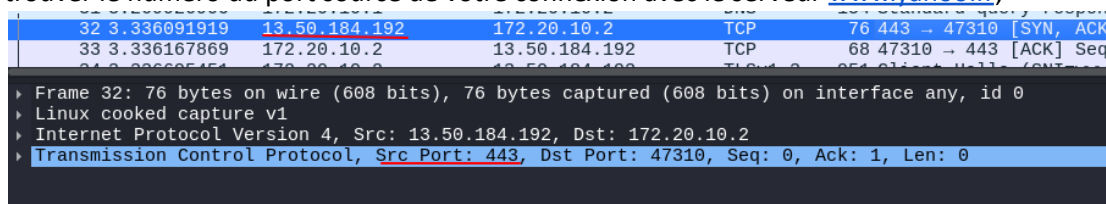


No.	Time	Source	Destination	Protocol	Length	Info
27	5.216438549	172.20.10.2	172.20.10.1	DNS	76	Standard query 0xb966 AAAA www.google.com
28	5.216484466	172.20.10.2	172.20.10.1	DNS	76	Standard query 0xb1ba A www.google.com
29	5.216506423	172.20.10.2	172.20.10.1	DNS	76	Standard query 0xbfb3 HTTPS www.google.com
30	5.579007901	172.20.10.1	172.20.10.2	DNS	101	Standard query response 0xbfb3 HTTPS www.google.com HTTPS
31	5.579007681	172.20.10.1	172.20.10.2	DNS	92	Standard query response 0xb1ba A www.google.com A 142.250.179.68

comme on peut voir quand on fait une requete on le fait au serveur destination 172.20.10.1
quand on recoit une reponse , on la recoit de 172.20.10.2 (mon ip)

l'ip du serveur est 172.20.10.1 car le routeur fait également dns

3. trouver le numéro du port source de votre connexion avec le serveur www.yahoo.fr;



No.	Time	Source	Destination	Protocol	Length	Info
32	3.336091919	13.50.184.192	172.20.10.2	TCP	76	443 → 47310 [SYN, ACK]
33	3.336167869	172.20.10.2	13.50.184.192	TCP	68	47310 → 443 [ACK] Seq=

Frame 32: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: 13.50.184.192, Dst: 172.20.10.2
Transmission Control Protocol, Src Port: 443, Dst Port: 47310, Seq: 0, Ack: 1, Len: 0

l'ip de www.yahoo.fr est 19.50.184.192 comme on a vu tout à l'heure
le port source est 443 (https)

4. détailler le format des trames ARP et présenter le diagramme des échanges ;
Voici un exemple de trame arp sur wireshark

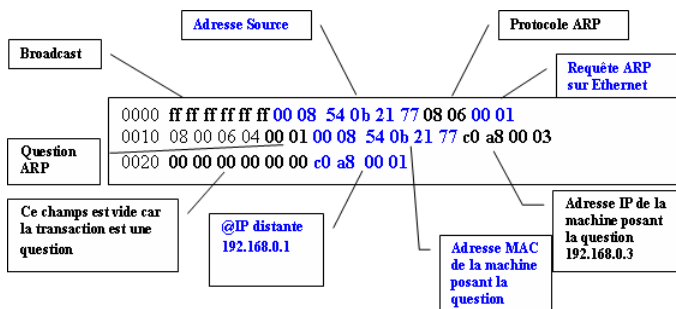
```

- Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: PCSSystemtec_eb:59:61 (08:00:27:eb:59:61)
  Sender IP address: 172.20.10.9
  Target MAC address: Xerox_00:00:00 (00:00:00:00:00:00)
  Target IP address: 172.20.10.1

0000  ff ff ff ff ff 08 00 27 eb 59 61 08 06 00 01 ..... 'Ya....
0010  08 00 06 04 00 01 08 00 27 eb 59 61 ac 14 0a 09 ..... 'Ya....
0020  00 00 00 00 00 00 ac 14 0a 01 00 00 00 00 00 .....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
  
```

L'en-tête ARP contient les informations de résolution d'adresse. Il contient les champs suivants :

- Type : indique le type de trame ARP.
- Protocole : indique le protocole de couche réseau auquel appartient l'adresse IP source.
- Adresse IP source : l'adresse IP de la machine source.
- Adresse MAC source : l'adresse MAC de la machine source.
- Adresse IP destination : l'adresse IP de la machine destination.
- Adresse MAC destination : l'adresse MAC de la machine destination.



L'échange ARP se déroule en deux étapes :

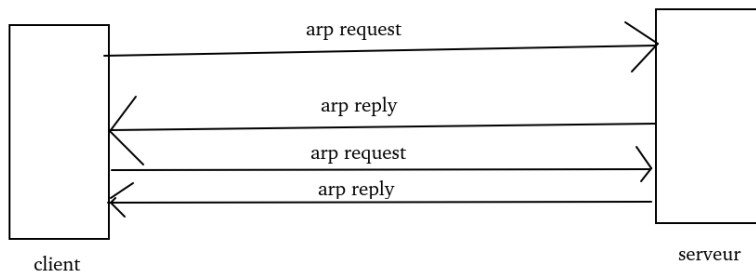
Requête ARP: Une machine qui souhaite communiquer avec une autre machine dont elle ne connaît pas l'adresse MAC émet une requête ARP. Cette requête contient l'adresse IP de la machine destinataire.

Réponse ARP: La machine dont l'adresse IP est indiquée dans la requête ARP répond par une réponse ARP. Cette réponse contient l'adresse MAC de la machine destinataire.

lorsque l'on fait un ping on a ça

16870	433.358290398	PCSSystemtec_eb:59:...	Broadcast	ARP	60 Who has 172.20.10.2? Tell 172.20.10.9
16871	433.358296177	Intel_af:18:ba	PCSSystemtec_eb:59:...	ARP	42 172.20.10.2 is at f4:26:79:af:18:ba

voici le datagramme:



5. détaillez le format des datagrammes ICMP;

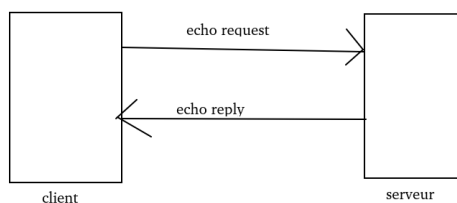
No.	Time	Source	Destination	Protocol	Length	Info
20	1.073218840	172.20.10.2	172.20.10.9	ICMP	98	Echo (ping) request id=0x1006, seq=1/256, ttl=64 (reply in 21)
21	1.073852176	172.20.10.9	172.20.10.2	ICMP	98	Echo (ping) reply id=0x1006, seq=1/256, ttl=64 (request in 20)

Voici ce que contient un paquet icmp:



En-tête ICMP

- L'en-tête ICMP est de 8 octets de long et contient les champs suivants :
- Type (8 bits): Ce champ indique le type de message ICMP. Il existe de nombreux types de messages ICMP, chacun ayant une signification différente. Certains types courants sont les requêtes d'écho, les réponses d'écho, les destinations inaccessibles, les délais dépassés et les problèmes de paramètres.
- Code (8 bits): Ce champ fournit des informations supplémentaires sur le type de message ICMP. Par exemple, la réponse d'écho a un type de 0 et un code de 0, tandis que la destination inaccessible a un type de 3 et un code qui spécifie la raison pour laquelle la destination est inaccessible.
- Checksum (16 bits): Ce champ est un checksum utilisé pour détecter les erreurs dans l'en-tête ICMP.
- Identificateur (16 bits): Ce champ est un identifiant unique pour le message ICMP. Il est utilisé pour faire correspondre les requêtes d'écho et les réponses d'écho.
- Numéro de séquence (16 bits): Ce champ est un numéro de séquence pour le message ICMP. Il est utilisé pour faire correspondre les requêtes d'écho et les réponses d'écho.



exemple de communication icmp

6. détaillez le format des datagrammes DNS:

deux parties : l'en-tête DNS et les données DNS.

L'en-tête DNS est de 12 octets de long et contient les champs suivants :

- ID (16 bits): Ce champ est un identifiant unique pour le datagramme DNS. Il est utilisé pour faire correspondre les requêtes DNS et les réponses DNS.
- QR (1 bit): Ce champ indique le type de message DNS. Une valeur de 0 indique une requête, tandis qu'une valeur de 1 indique une réponse.
- Opcode (4 bits): Ce champ indique le type de requête DNS. Les valeurs possibles sont les suivantes : 0 : Requête standard , 1 : Requête inverse , 2 : Statut du serveur , 3-15 : Réservé pour utilisation future
- AA (1 bit): Ce champ indique si la réponse est authentifiée. Une valeur de 1 indique que la réponse est authentifiée, tandis qu'une valeur de 0 indique qu'elle ne l'est pas.
- TC (1 bit): Ce champ indique si le datagramme DNS a été tronqué. Une valeur de 1 indique que le datagramme a été tronqué, tandis qu'une valeur de 0 indique qu'il ne l'a pas été.
- RD (1 bit): Ce champ indique si le client souhaite que le serveur retourne des enregistrements de ressources (RR) supplémentaires. Une valeur de 1 indique que le client souhaite que le serveur retourne des RR supplémentaires, tandis qu'une valeur de 0 indique qu'il ne le souhaite pas.
- RA (1 bit): Ce champ indique si le serveur est capable de retourner des RR supplémentaires. Une valeur de 1 indique que le serveur est capable de retourner des RR supplémentaires, tandis qu'une valeur de 0 indique qu'il ne l'est pas.
- Z (3 bits): Ce champ est réservé pour une utilisation future.
- RCode (4 bits): Ce champ indique le code d'erreur de la réponse. Les valeurs possibles sont les suivantes : 0 : Success , 1 : Format Error , 2 : Server Failure, 3 : Name Error, 4 : Not Implemented, 5 : Refused, 6-15 : Réservé pour utilisation future

Les requêtes DNS contiennent les informations suivantes :

- Le nom de domaine sur lequel la requête est effectuée.
- Le type d'enregistrement recherché.
- Les types d'enregistrements supplémentaires recherchés.

Les réponses DNS contiennent les informations suivantes :

- Le nom de domaine sur lequel la réponse est effectuée.
- Le type d'enregistrement retourné.
- La valeur de l'enregistrement.
- Les types d'enregistrements supplémentaires retournés.

Voici un exemple de communication dns sur wireshark

52298	861.209735604	172.20.10.2	172.20.10.1	DNS	75 Standard query 0x439b HTTPS www.youtube.com
52300	861.274672368	172.20.10.1	172.20.10.2	DNS	124 Standard query response 0x439b HTTPS www.youtube.com CNAME youtube-ui.l.google.com HTTPS

et

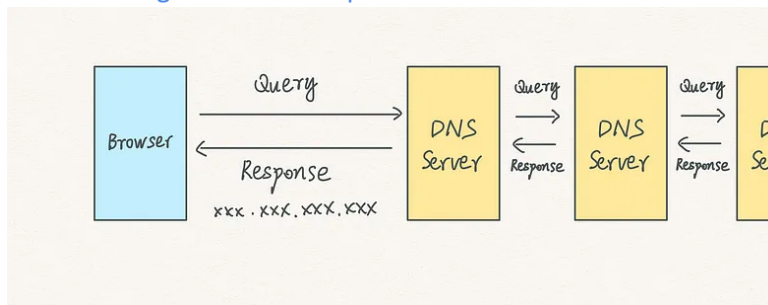
```

Wireshark - Paquet 52298 - wlan0
> Frame 52298: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface wlan0, id 0
> Ethernet II, Src: Intel_af:18:ba (f4:26:79:af:18:ba), Dst: 3e:7d:0a:06:fd:64 (3e:7d:0a:06:fd:64)
> Internet Protocol Version 4, Src: 172.20.10.2, Dst: 172.20.10.1
> User Datagram Protocol, Src Port: 27452, Dst Port: 53
> Domain Name System (query)
  Transaction ID: 0x439b
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    [Response In: 52300]

0000  3e 7d 0a 06 fd 64 f4 26 79 af 18 ba 00 00 45 00  >...d & y...E
0010  00 3d 7a 51 40 00 40 11 54 33 ac 14 0a 02 ac 14  =zQ000T3.....
0020  0a 01 6b 3c 00 35 00 29 6c 66 43 9b 01 00 00 01  .k<5) lfc.....
0030  00 00 00 00 00 00 03 77 77 77 07 79 6f 75 74 75  ....w ww.youtu
0040  62 65 03 63 6f 6d 00 00 41 00 01                be com..A..

```

Voici un datagramme d'exemple de communication dns :



- déterminez la procédure d'établissement d'une connexion TCP. Utiliser l'option « statistics -> Flow graph » pour représenter le diagramme des échanges de messages lors de cette ouverture de connexion.

la procédure se déroule ainsi :

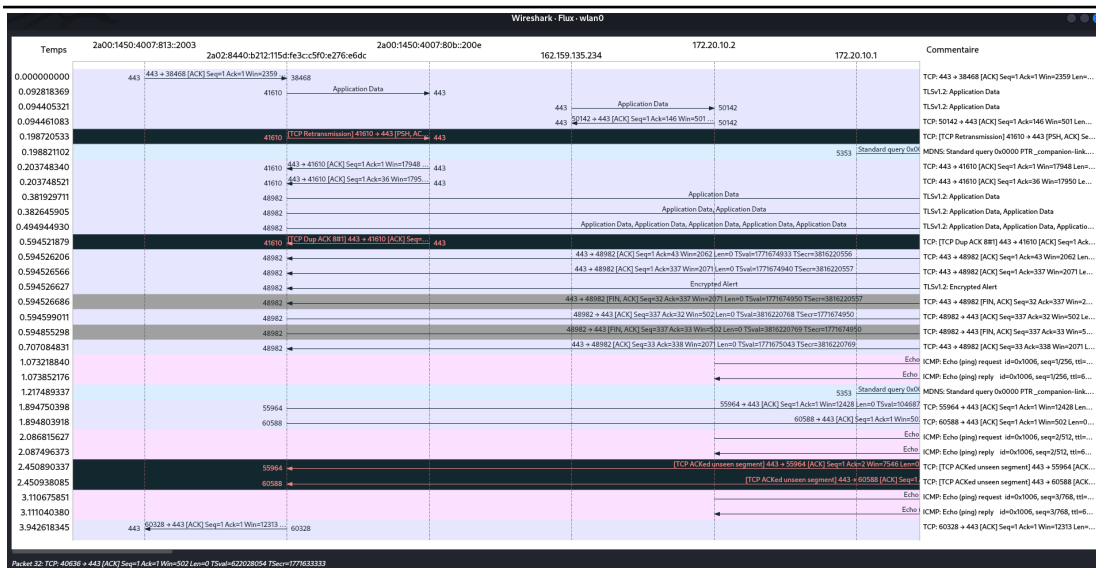
La connexion TCP se fait en trois étapes :

- SYN : L'initiateur demande la connexion.
- SYN-ACK : Le destinataire accepte et propose un numéro de séquence initial.
- ACK : L'initiateur confirme, et la connexion est établie.

comme ici :

164	15.010958922	2a02:8440:b212:115d...	2a00:1450:4007:80d...	TCP	94 48190 → 443 [SYN] Seq=0 Win=65536 Len=0 MSS=1396 SACK_PERM TSval=1456287924 TSecr=0 WS=128
165	15.011095188	2a02:8440:b212:115d...	2a00:1450:4007:818...	TCP	86 33898 → 443 [ACK] Seq=180 Ack=1121 Win=502 Len=0 TSval=1554271669 TSecr=1773663704
166	15.011872798	2a02:8440:b212:115d...	2a00:1450:4007:818...	TLSv1.2	121 Application Data
167	15.011899408	2a02:8440:b212:115d...	2a00:1450:4007:818...	TLSv1.2	125 Application Data
168	15.117743935	2a00:1450:4007:818...	2a02:8440:b212:115d...	TCP	86 443 → 33898 [ACK] Seq=1121 Ack=215 Win=1920 Len=0 TSval=1773663824 TSecr=1554271669
169	15.126677444	2a00:1450:4007:80d...	2a02:8440:b212:115d...	TCP	94 443 → 48190 [SYN, ACK] Seq=0 Ack=1 Win=58380 Len=0 MSS=1410 WS=32 SACK_PERM TSval=177366383
170	15.126745942	2a02:8440:b212:115d...	2a00:1450:4007:80d...	TCP	86 48190 → 443 [ACK] Seq=1 Ack=1 Win=65408 Len=0 TSval=1456288039 TSecr=1773663831

Voici le diagramme des échanges de messages:



Voici le diagramme des échanges de messages

- Pinger la machine de votre voisin et déterminer la valeur de l'adresse MAC destination de votre commande ICMP echo.

No.	Time	Source	Destination	Protocol	Length	Info
72	1.278573913	172.20.10.2	172.20.10.9	ICMP	98	Echo (ping) request id=0xa363, seq=1/256, ttl=64 (reply in 73)
73	1.278843599	172.20.10.9	172.20.10.2	ICMP	98	Echo (ping) reply id=0xa363, seq=1/256, ttl=64 (request in 72)
74	2.281292899	172.20.10.2	172.20.10.9	ICMP	98	Echo (ping) request id=0xa363, seq=2/512, ttl=64 (reply in 75)

Frame 72: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlan0, id 0
 Ethernet II, Src: Intel af:18:ba (f4:26:79:af:18:ba), Dst: PCSSystemtec_eb:59:61 (08:00:27:eb:59:61)
 Internet Protocol Version 4, Src: 172.20.10.2, Dst: 172.20.10.9
 Internet Control Message Protocol

l'adresse mac destination est 08:00:27:eb:59:61

- Pinger la machine « www.univ-paris1.fr » et déterminer la valeur de l'adresse MAC destination de votre commande ICMP echo. Comparer avec la question 8.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe80::f626:79ff:fea...	2a02:8440:b212:115d...	ICMPv6	86	Neighbor Solicitation for 2a02:8440:b212:115d:876:1c88:2d77:364
2	0.042233018	fe80::3c7d:aff:fe06...	fe80::f626:79ff:fea...	ICMPv6	78	Neighbor Advertisement 2a02:8440:b212:115d:876:1c88:2d77:364
11	1.136272896	2a02:8440:b212:115d...	2001:660:3305::23	ICMPv6	118	Echo (ping) request id=0x6c10, seq=1, hop limit=64 (reply in 12)
12	1.261906671	2001:660:3305::23	2a02:8440:b212:115d...	ICMPv6	118	Echo (ping) reply id=0x6c10, seq=1, hop limit=51 (request in 11)

Frame 11: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface wlan0, id 0
 Ethernet II, Src: Intel af:18:ba (f4:26:79:af:18:ba), Dst: 3e:7d:0a:06:fd:64 (3e:7d:0a:06:fd:64)
 Internet Protocol Version 6, Src: 2a02:8440:b212:115d:fe3c:c5f0:e276:e6dc, Dst: 2001:660:3305::23
 Internet Control Message Protocol v6

l'adresse mac destination est 3e:7d:0a:06:fd:64 et on a utilisé icmpv6 au lieu de icmp, on est en ipv6 ici contre ipv4 dans l'exo 8

Exercice 3 – Adressage IPv4 avancé

Vous êtes l'administrateur du réseau de votre entreprise, à qui l'on vient d'attribuer l'adresse IPv4 150.123.45.128/22 (en notation abrégée). Vous devez créer 3 sous-réseaux distincts pour les 3 succursales de votre entreprise à partir de cette adresse de réseau IP fournie par votre opérateur, ainsi qu'une DMZ (Zone Démilitarisée). Répondez aux questions suivantes.

a– Quel est le masque (en décimale) de votre réseau principal (/22) ? Combien de machines peut-on avoir au maximum dans ce réseau principal (/22) ?

Masque du réseau principal (/22) : 255.255.252.0

Nombre maximal de machines dans le réseau principal (/22) : 1022 ($2^{(32-22)}-2$) car on prend en compte le du réseau et de la diffusion.

b- Qu'est-ce que CIDR

CIDR (Classless Inter-Domain Routing) est un système de notation flexible des adresses IP, remplaçant le modèle de classes. Il indique la longueur du préfixe d'un réseau en utilisant la notation "adresse IP/préfixe". Par exemple, dans 150.123.45.128/22, "/22" signifie que les 22 premiers bits sont dédiés au réseau. Cela permet une gestion plus efficace des adresses IP.

c- Qu'est-ce que VLSM ?

permet l'utilisation de masques de sous-réseau de longueurs variables. Contrairement à la méthode traditionnelle, VLSM autorise des sous-réseaux de tailles différentes au sein d'un réseau, optimisant ainsi l'utilisation des adresses IP, surtout dans des réseaux de grande envergure. on peut donc ajouter/diminuer des adresse ip au prix de sous reseau

d- Qu'est-ce qu'une DMZ ?

Une DMZ (Zone Démilitarisée) est une zone intermédiaire entre le réseau interne d'une organisation et Internet. Elle héberge des services accessibles depuis l'extérieur, tels que des serveurs web, tout en isolant ces services du réseau interne pour renforcer la sécurité.

e - Quel masque de sous-réseau devez-vous utiliser pour votre nouveau plan d'adressage ?

Bloc d'adresse réseau	Masque de sous-réseau	Nb. d'hôtes / de sous-réseaux	Nombre de sous-réseaux
150.123.45.128/22	255.255.255.0/24	256	4
Plage d'adresses des hôtes	Adresse de diffusion	Masque générique	Notation CIDR
150.123.45.1 - 150.123.45.254	150.123.45.255	0.0.0.255	150.123.45.0/24

nous avons besoin de 4 sous reseaux sachant que /22 nous permet que 1 sous reseau , /23 que 2 sous reseau et /24 nous permet 4 sous réseau , alors le prochain masque est 255.255.255.0/24 (22+2)

f– Combien d'adresses IP distinctes est-il possible d'utiliser avec un tel masque, tous sous-réseaux possibles confondus ?

on a 8 bits restant pour les ip donc 2^8-2 soit 254 ip disponible par sous réseau

g- quelles sont les adresses des 4 sous réseaux de votre entreprise ?

Voici comment j'ai calculer le subnetting

150.123.45.128/22

Network ID:	150	123	44	0
Broadcast ID:	150	123	47	255
Usable IPs:	150.123.44.1 - 150.123.47.254			

45= 00101101
x 11111100 (252)
=00101100 =44

Suffit de diviser par 4 les ip disponible

Voici les adresses IP des 4 sous-réseaux :

DMZ : 150.123.44.0/24

Adresse réseau : 150.123.44.0

Plage d'adresses utilisables : 150.123.44.1 à 150.123.44.254

Adresse de diffusion : 150.123.44.255

Sous-réseau 1 : 150.123.45.0/24

Adresse réseau : 150.123.45.0

Plage d'adresses utilisables : 150.123.45.1 à 150.123.45.254

Adresse de diffusion : 150.123.45.255

Sous-réseau 2 : 150.123.46.0/24

Adresse réseau : 150.123.46.0

Plage d'adresses utilisables : 150.123.46.1 à 150.123.46.254

Adresse de diffusion : 150.123.46.255

Sous-réseau 3 : 150.123.47.0/24

Adresse réseau : 150.123.47.0

Plage d'adresses utilisables : 150.123.47.1 à 150.123.47.254

Adresse de diffusion : 150.123.47.255

h– Combien d'adresses IP de hosts (terminaux et routeurs inclus) pourra recevoir chaque sous-réseau de votre entreprise ?

Chaque sous-réseau peut recevoir un total de 254 adresses IP de hosts (+2 si on compte l'adresse du réseau et l'ip de broadcast

i– Quelle est l'adresse de broadcast globale des 4 sous -réseaux ?

Les adresse sont :

Adresse de diffusion DMZ : 150.123.44.255

Adresse de diffusion RESEAU 1: 150.123.45.255

Adresse de diffusion RESEAU 2: 150.123.46.255

Adresse de diffusion RESEAU 3: 150.123.47.255

si on devait en choisir une ca serait donc : 150.123.45.255

j- Quelles sont les adresses de diffusion dirigée du 1er et du 3eme sous-réseau? Quelle est la différence avec l'adresse de diffusion globale de la question précédente ?

Adresse de diffusion DMZ : 150.123.44.255

Adresse de diffusion RESEAU 2: 150.123.46.255

La différence entre l'adresse de diffusion globale et l'adresse de diffusion dirigée est que l'adresse de diffusion globale est utilisée pour envoyer un message à tous les hôtes d'un sous-réseau, tandis que l'adresse de diffusion dirigée est utilisée pour envoyer un message à tous les hôtes d'un réseau particulier.

Exercice 4 – QCM

1. À quoi sert ARP ?

1. À trouver l'adresse MAC d'une station dont on connaît l'adresse IP
2. À trouver l'adresse IP d'une station dont on connaît l'adresse MAC
3. À trouver l'adresse MAC d'une station dont on connaît le nom de HOST

la reponse est 1 , Arp sert À trouver l'adresse MAC d'une station dont on connaît l'adresse IP

2. À quoi sert R-ARP (Reverse ARP) ?

1. À trouver l'adresse MAC d'une station dont on connaît l'adresse IP
2. À trouver l'adresse IP d'une station dont on connaît l'adresse MAC
3. À trouver l'adresse MAC d'une station dont on connaît le nom de HOST

la reponse est 2 , À trouver l'adresse IP d'une station dont on connaît l'adresse MAC

3. Quel est le protocole associé à la commande PING ?

1. DNS
2. DHCP
3. ICMP

la reponse est 3 , ICMP

4. Sur combien d'octets une adresse IPv4 est-elle codée ?

1. 6
2. 8
3. 4

la reponse est 4 octets

5. À quoi correspond l'adresse 192.168.1.210 en binaire ?

1. 11000000 10101000 00000000 11010010
2. 11000000 10101000 00000001 11010011
3. 11000000 10101000 00000001 11010010

la reponse est 3 , 11000000 10101000 00000001 11010010

6. Parmi les filtres **WIRESHARK** ci-dessous, quel est celui qui permet de filtrer les trames envoyées par la machine source d'adresse IP 192.168.0.2 :

1. ip.src == 192.168.0.2
2. ip.dst == 192.168.0.2
3. ip.addr.src == 192.168.0.2
4. ip.addr.dst == 192.168.0.2

la reponse 1 est la bonne reponse : ip.src == 192.168.0.2

7 Le **masque** de sous-réseau IPv4 sert :

1. A Identifier l'adresse du réseau auquel appartient une station
2. A identifier le serveur DHCP sur le réseau
3. A protéger l'adresse IP des stations

La réponse 1 est la bonne reponse : A Identifier l'adresse du réseau auquel appartient une station.

8. La taille de l'adresse MAC est de :

1. 4 octets (32 bits)
2. 6 octets (48 bits)
3. 8 octets (64 bits)

La réponse 2 est la bonne reponse : 6 octets (48 bits)

9. Soit un réseau d'entreprise possédant l'adresse de réseau IP : 145.34.64.0/18. Quel est le **masque de réseau** et le nombre maximum d'adresses de stations possibles :

1. a. 255.255.0.0
2. b. 255.255.128.0
3. c. 255.255.192.0

La réponse 3 est la bonne reponse : 255.255.192.0 soit 16384 adresse possible

10. 9. Soit un réseau d'entreprise possédant l'adresse de réseau IP : 145.34.64.0/18. Quel est le nombre maximum d'adresses de stations possibles :

1. 1020
2. 16 382
3. 65 543

La réponse 2 est la bonne reponse : 16384 adresse

11. Quel protocole permettrait de résoudre l'adresse 132.148.0.1 en 00-a0-00-12-26-1F?

1. DHCP
2. WINS
3. R-ARP
4. ARP

La réponse 4 est la bonne reponse : arp

12. Quel protocole permettrait de résoudre l'adresse 00-a0-00-12-26-1F en 132.148.0.1 ?

1. DHCP

2. WINS
3. R-ARP
4. ARP

La réponse 3 est la bonne réponse : r-arp

13. Une Station A a une adresse IP 10.20.30.40 et un masque de sous-réseau est 255.255.255.0. Une Station B a une adresse IP 10.20.30.50 et un masque de sous-réseau est 255.255.255.0. Que peut-on dire de la communication entre les stations A et B

1. La communication entre A et B est directe car les stations A et B sont dans le même sous-réseau
2. La communication entre A et B est indirecte car les stations A et B ne sont pas dans le même sous-réseau
3. La communication peut être directe ou indirecte en fonction du type de fichier envoyé

La réponse 1 est la bonne réponse : La communication entre A et B est directe car les stations A et B sont dans le même sous-réseau

14. Il y a deux sortes de filtres **WIRESHARK** lesquels :

1. Filtres à la capture
2. Filtres de sélection
3. Filtres à l'affichage
4. Filtres protocolaires

La réponse 1 et 3 sont les bonnes réponses : Filtres à la capture et Filtres à l'affichage

15. La couche réseau IPv4 est chargée de :

1. Le contrôle de flux de paquets
2. Le contrôle d'erreurs des données
3. L'Adressage des stations
4. Le Routage des paquets

La réponse 3 et 4 sont les bonnes réponses : Le contrôle d'erreurs des données et Le Routage des paquets

On rappelle la structure d'une trame Ethernet et d'un paquet ARP.

Trame Ethernet :

Destination (6)	Source(6)	Type(2)	Données(n)
-----------------	-----------	---------	------------

Type (0800 IP, 0806 ARP, 00c0 PPP)

Paquet ARP :

Type mat. (2)	Protocole (2)	T. mat (1)	T. prot (1)	OP (2)	Adr. Mac émetteur. (6)	Adr. IP émetteur (4)	Adr. Mac destinataire. (6)	Adr. IP Destinataire (4)
------------------	------------------	---------------	----------------	-----------	---------------------------	-------------------------	-------------------------------	-----------------------------

OP (0001 requête, 0002 réponse)

Soient les suites hexadécimales ci-dessous correspondant à la capture de deux trames de réseau local Ethernet par WIRESHARK. Les octets de préambules ne sont pas représentés.

Trame n°1 :

FF FF FF FF FF FF 08 00 20 02 45 9E 08 06 00 01 08 00 06 04 00
01 08 00 20 02 45 9E 81 68 FE 06 00 00 00 00 00 00 81 68 FE 05

Trame n°2 :

08 00 20 02 45 9E 08 00 20 07 0B 94 08 06 00 01 08 00 06 04 00
02 08 00 20 07 0B 94 81 68 FE 05 08 00 20 02 45 9E 81 68 FE 06

16. Wireshark : A quoi correspondent la trame 1 ?

1. Réponse ARP encapsulée dans une trame Ethernet
2. Requête ARP encapsulée dans une trame Ethernet
3. Acquiescement ARP encapsulée dans une trame Ethernet

Réponse 1 : ARP encapsulée dans une trame Ethernet

17. Wireshark : A quoi correspondent la trame 2 ?

1. Réponse ARP encapsulée dans une trame Ethernet
2. Requête ARP encapsulée dans une trame Ethernet
3. Acquiescement ARP encapsulée dans une trame Ethernet

Réponse 2 : Requête ARP encapsulée dans une trame Ethernet

18 Wireshark- Soit la structure de trame de la question 27, Ou se trouve le paquet ARP par rapport à la trame Ethernet ?

1. le paquet ARP est encapsulé dans la trame Ethernet et son contenu se trouve dans le champ de données de la trame Ethernet
- 2- Le paquet ARP est encapsulé dans la trame Ethernet et son contenu se trouve dans le champ de données de la trame Ethernet avec suppression des champs d'adresses source et destination
3. La trame Ethernet est encapsulée dans un paquet ARP

Réponse 1 : Le paquet ARP est encapsulé dans la trame Ethernet et son contenu se trouve dans le champ de données de la trame Ethernet :

19- Que représente la valeur « FF FF FF FF FF FF » dans un réseau local Ethernet ?

1. Adresse Ethernet de la station émettrice
2. Adresse Ethernet de diffusion à toutes les stations du même sous-réseau
- 3- Adresse Ethernet de la station destinataire

Réponse 2 : Adresse Ethernet de diffusion à toutes les stations du même sous-réseau

20- Quels sont les paramètres de configuration que le serveur DHCP (Dynamic Host Configuration Protocol) attribue à une station qui démarre dans un réseau d'entreprise ? :

1. Adresse IP du serveur DNS de l'entreprise
2. Adresse IP du serveur Web de l'entreprise
3. Masque du réseau d'entreprise

Réponse 2 et 3 : Adresse IP du serveur DNS de l'entreprise et Masque du réseau d'entreprise

21- Quels sont les paramètres de configuration que le serveur DHCP (Dynamic Host Configuration Protocol) attribue à une station qui démarre dans un réseau d'entreprise ? :

1. Adresse MAC de la station
2. Adresse IP de la station
3. Adresse IP de la passerelle par défaut

Réponse 2 et 3 : adresse IP de la station et Adresse IP de la passerelle par défaut

22- Le délai de propagation d'une trame d'information sur un réseau dépend de :

1. La longueur de la trame
2. La distance parcourue
3. Le débit du réseau
4. La vitesse du support

Réponse 2 et 4 : La distance parcourue et la vitesse du support.

23. Pour connaître la configuration IP sur une machine Windows, utiliser la commande :

1. Ipconfig /all
2. Ifconfig /all
3. Ipconfig -a

reponse 1 : ipconfig /all

24. La couche physique est chargée de :

1. La conversion entre bits et signaux électriques
2. La transmission de bits
3. Le contrôle de flux
4. Le contrôle d'erreurs

la reponse 1 et 2 : La conversion entre bits et signaux électriques et La transmission de bits :

25. Quel(s) intérêt(s) de réaliser un sous-adressage de son réseau IP d'entreprise :

1. Réduire les collisions de paquets
2. Réduire le coût d'installation du réseau
3. Accroître la confidentialité des échanges
4. Accroître le nombre d'adresses IP attribuables aux stations

reponse 1 et 4 : réduire les collisions de paquets et d'accroître le nombre d'adresses IP attribuables aux stations

26. Quel est l'organisme qui contrôle l'attribution des adresses IP et gère l'annuaire DNS mondial :

1. IETF
2. OSI
3. ICANN
4. ONU

reponse 3 : ICANN

27. Quel est l'organisme qui développe et contrôle les standards techniques de l'Internet :

1. IETF
2. OSI
3. ICANN
4. ONU

Reponse 1 : IETF

28. Qu'est qu'un RFC dans le réseau Internet ?

1. Un document technique qui décrit un protocole de communication de l'Internet
2. Un formulaire de demande d'adresses IP publiques à destination des entreprises
3. Un registre des noms des domaines déjà réservés et en cours d'utilisation

Reponse 1: Un document technique qui décrit un protocole de communication de l'Internet.