HAYE Marc S5

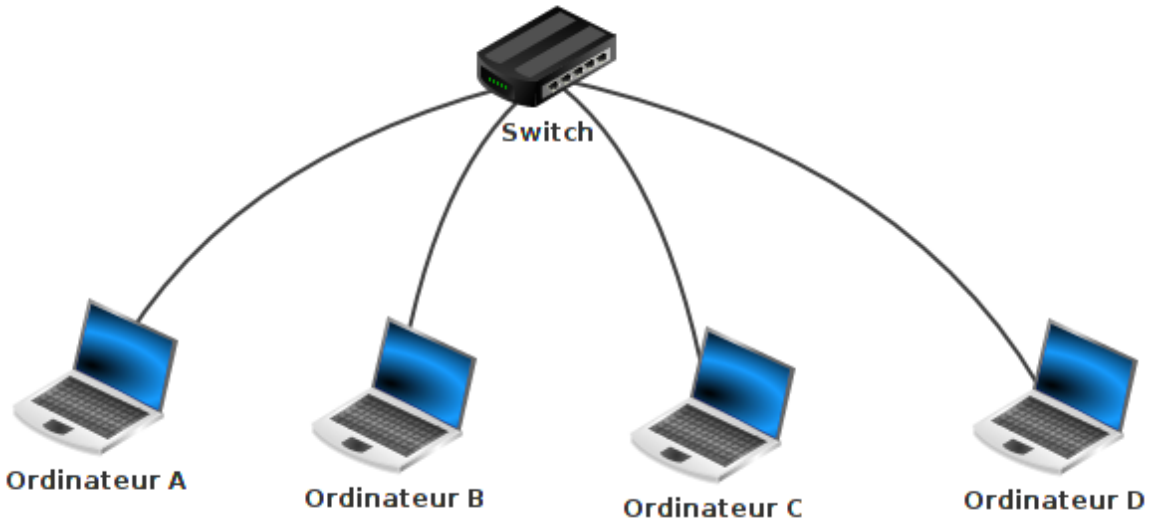
Rendu TDs - Découverte Réseau

Sommaire

TD 1

PARTIE 1

1) Switch et Routeur



Un switch est un dispositif réseau qui permet de connecter plusieurs appareils sur un même réseau local (LAN) en acheminant les données entre eux. Il sert essentiellement à créer un réseau local.

Un routeur, quant à lui, est un dispositif réseau qui relie différents réseaux ensemble en acheminant les données entre eux. Il permet notamment de connecter des réseaux locaux à Internet.

Le switch ne prend pas en compte les adresses IP alors que le routeur le fait, ce qui lui permet de déterminer la meilleure route pour acheminer les données d'un réseau à un autre.

Le prix des switches et des routeurs varie en fonction de leur niveau de performance, de leur capacité et des fonctionnalités qu'ils offrent.

En général, les switches sont moins chers que les routeurs car ils ont des fonctionnalités moins avancées et sont destinés à un usage local.

Un switch basique peut coûter entre 20 et 50 euros, tandis qu'un switch plus performant peut coûter entre 100 et 500 euros.

Les routeurs, en revanche, sont plus chers en raison de leur capacité à gérer des réseaux plus vastes et plus complexes.

Un routeur domestique basique peut coûter entre 50 et 100 euros, tandis qu'un routeur professionnel avec des fonctionnalités avancées peut coûter plusieurs milliers d'euros.

2) Les Switchs

Tableau représentant les principales caractéristiques des switchs utilisé au sein de l'IUT :

Marque / Modèle	Nombre de ports	Type de ports	Vitesse maximale	PoE (Power over Ethernet)	Gestion
HP ProCurve 2510-48	48	Ethernet 10/100Base-TX	100 Mbps	Oui (sur certains ports)	Gestionable
Netgear GS105	5	Ethernet 10/100 /1000Base-T	1 Gbps	Non	Non géré
Netgear GS724Tv4	24	Ethernet 10/100 /1000Base-T	1 Gbps	Oui (sur tous les ports)	Gestionable
3com Baseline Switch 2250-SFP Plus	50	Ethernet 10/100Base-TX, SFP	100 Mbps	Oui (sur certains ports)	Gestionable

3) Protocoles de communications

Les différents protocoles de communications sont :

1. Ethernet : c'est le protocole de couche liaison de données le plus couramment utilisé pour connecter des périphériques sur un réseau local. Il définit les règles de communication pour les paquets de données sur le câble.

2. TCP (Transmission Control Protocol) : c'est le protocole de couche transport qui fournit une communication fiable entre les applications en divisant les données en segments et en les rassemblant à la destination.

3. IP (Internet Protocol) : c'est le protocole de couche réseau qui permet l'acheminement des paquets de données à travers les réseaux en utilisant des adresses IP.

Ethernet est utilisé pour connecter les périphériques sur le réseau local, tandis que TCP et IP sont utilisés pour acheminer les paquets de données sur le réseau et garantir une communication fiable entre les applications.

Adresses IP

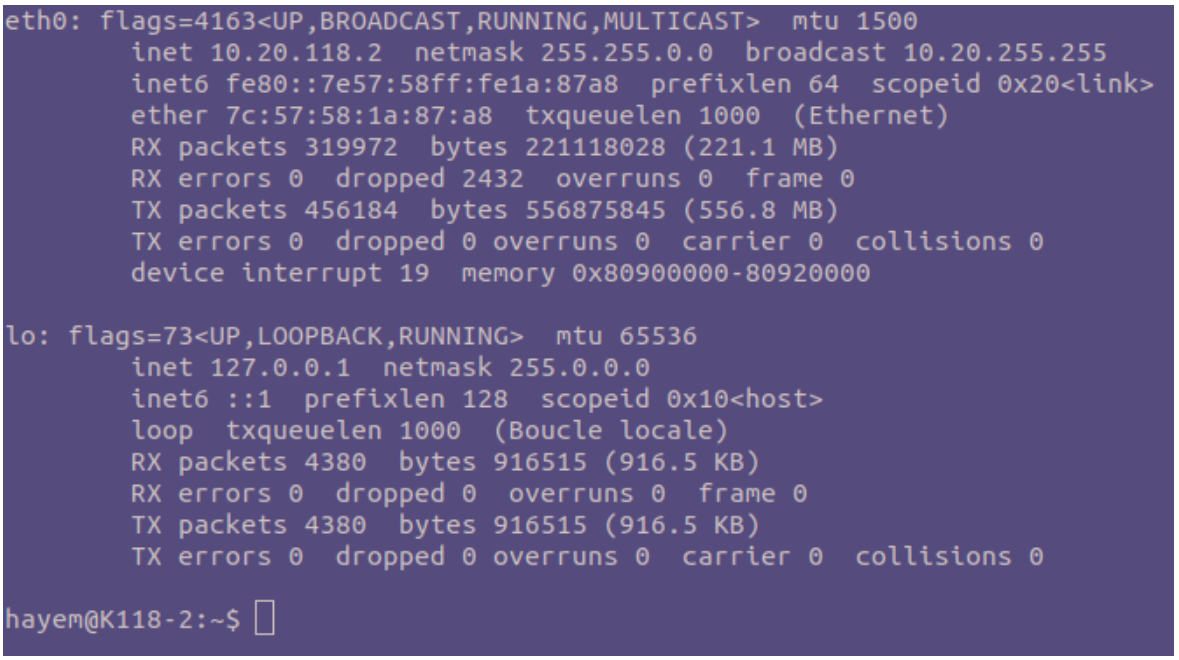
Ces valeurs sont des adresses IP.

Une adresse IP (Internet Protocol) est un numéro unique qui identifie un périphérique sur un réseau IP. Il s'agit d'une combinaison de nombres qui permettent aux périphériques de communiquer entre eux sur Internet ou sur un réseau local (LAN).

Il existe deux versions principales du protocole IP : IPv4 et IPv6. IPv4 est la version la plus courante et utilise des adresses IP de 32 bits, tandis qu'IPv6 utilise des adresses IP de 128 bits pour répondre à la demande croissante d'adresses IP dans le monde.

Les adresses IP sont essentielles pour permettre aux ordinateurs et aux autres périphériques de communiquer entre eux sur les réseaux.

Informations relatives au réseau des sessions étudiants disponibles à partir du terminale :



Des exemples

Adresse IP : 192.168.1.100
Masque de sous-réseau : 255.255.255.0
Passerelle par défaut : 192.168.1.1

Adresse IP : 10.0.0.50
Masque de sous-réseau : 255.0.0.0
Passerelle par défaut : 10.0.0.1

Adresse IP : 172.16.0.10
Masque de sous-réseau : 255.255.0.0
Passerelle par défaut : 172.16.0.1

10.10.0.1
Classe : *Privé A*
Masque : *255.0.0.0*

162.38.222.170
Classe : *Public B*
Masque : *255.255.0.0*

PARTIE 2

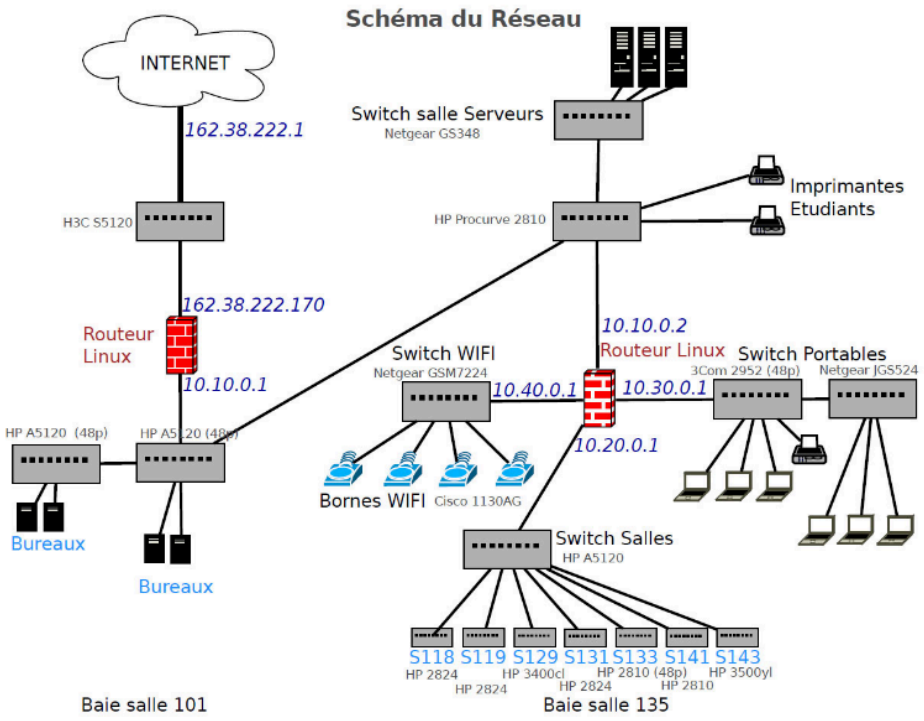


Schéma du Réseau
INTERNET
162.38.222.1
Switch salle Serveurs
Netgear GS348
H3C S5120
HP Procurve 2810
Imprimantes
Etudiants
162.38.222.170
Routeur
Linux
10.10.0.1
10.10.0.2
Routeur Linux
Switch WIFI
Netgear GSM7224
10.40.0.1
10.30.0.1
Switch Portables
3Com 2952 (48p)
Netgear JGS524
10.20.0.1
HP A5120 (48p)
HP A5120 (48p)
Bornes WIFI
Cisco 1130AG
Switch Salles
HP A5120
Bureaux
Bureaux
S118 S119 S129 S131 S133 S141 S143
HP 2824
HP 2824
HP 3400cl
HP 2824
HP 2810 (48p)
HP 2810
HP 3500yl
Baie salle 101
Baie salle 135

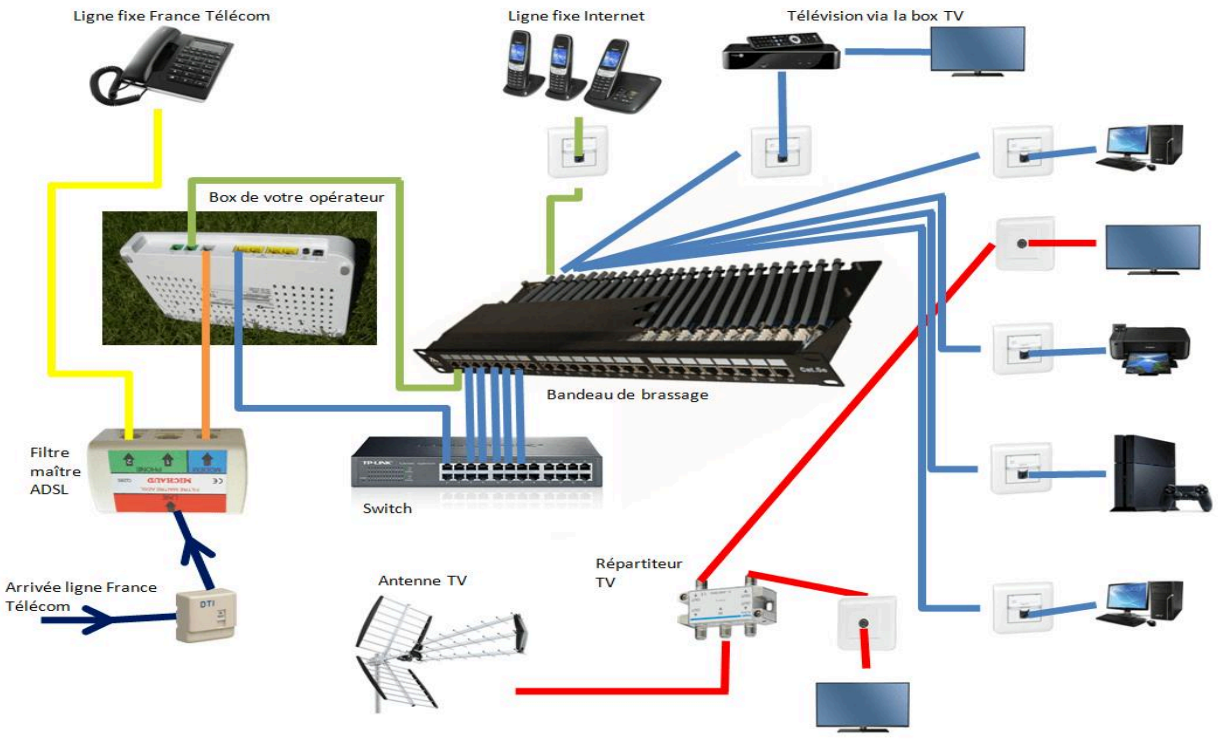

T.P. Info.
k119
Bibliothèque
Bur.
Salle
Réunion
k101
Repro.
Salle T.D.
k123
Rgt
Dét.
W.C.
T.P. Info.
k114
Salle T.D.
k125
Salle T.D.
k127
Salle T.D.
k116
T.D. Info.
k129
T.P. Info.
k118
T.P. Info.
k131
Réserve
Info.
T.P. Info.
Salle
T.P.
T.P.
Info.
T.P. Info.
k133
Repro.
Salle
Serveur
k137
T.P. Info.
k141
T.P. Info.
k143
T.P. Info.
T.D. Info.
k155

TD 2

1 - Introduction

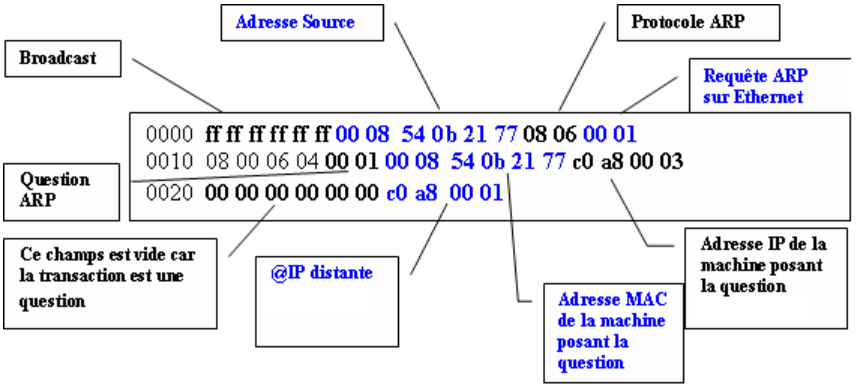
Les normes IEEE 802.1 / 802.2 et 802.3 correspondent respectivement aux normes pour les réseaux locaux (LAN), aux protocoles de liaison de données et à Ethernet.
Dans le cadre d'un réseau local, Ethernet couvre principalement la partie matérielle, telle que les cartes réseau, les câbles et les switches, ainsi que la partie logicielle avec le protocole de communication Ethernet.

2 - Découverte de l'Ethernet



Une adresse Ethernet, également connue sous le nom d'adresse MAC (Media Access Control), est une adresse physique unique de 48 bits attribuée à chaque carte réseau. L'adresse MAC est généralement représentée sous forme hexadécimale.

L'adresse MAC est construite en deux parties : les 24 premiers bits représentent l'identifiant de l'entreprise qui a fabriqué la carte réseau, et les 24 derniers bits sont un identifiant unique attribué par l'entreprise.
Il existe également des adresses multicast et broadcast (communique à tous) qui permettent la communication de groupe et la diffusion à tous les périphériques sur le réseau.



Le format de la trame Ethernet compose ses données en différentes parties :

- Le préambule: composé de 7 octets de données utilisés pour synchroniser les horloges des émetteurs et des récepteurs.
- L'adresse de destination correspond à l'adresse MAC du destinataire.
- Adresse source correspond à adresse MAC de l'émetteur.
- Type de protocole: indique le type de protocole de couche supérieure utilisé dans les données.

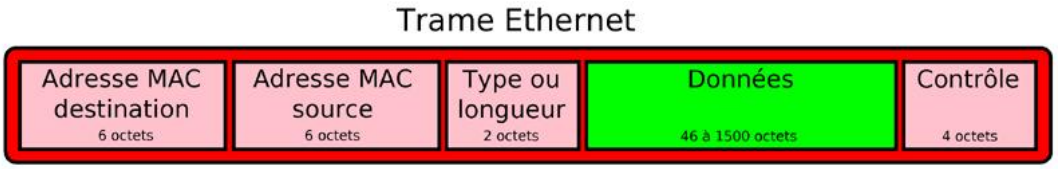
Les normes Ethernet actuelles prennent en charge des débits allant jusqu'à 400 Gbit/s, avec des normes telles que
Ethernet 10,100,1000,4G,5G…

Les raisons qui ont permis cette élévation du débit sont principalement liées aux avancées technologiques dans la fabrication de cartes réseau, de câbles et de switches, ainsi que des améliorations du protocole Ethernet.

Ethernet peut être utilisé sur une variété de supports de transmission, tels que les câbles coaxiaux, les câbles en paire torsadée, les fibres optiques et les connexions sans fil.
Les normes Ethernet spécifient les exigences pour chaque type de support de transmission. Par exemple, les normes Ethernet sur câble en paire torsadée comprennent 10Base-T, 100Base-TX, 1000Base-T, etc.

3 - Ethernet et les protocoles CSMA

Application 1



1.
Le protocole CSMA/CD (Carrier Sense Multiple Access with Collision Detection) est utilisé pour gérer les collisions sur un réseau Ethernet. Avant d'envoyer des données, chaque nœud vérifie si le canal est libre. Si le canal est occupé, le nœud attend un temps aléatoire avant de tenter de renvoyer les données.

Cependant, si deux nœuds émettent simultanément sur le même canal, une collision se produit et les données sont corrompues. Dans ce cas, chaque nœud arrête immédiatement la transmission, envoie un signal de brouillage pour alerter les autres nœuds de la collision, puis attend un

temps aléatoire avant de tenter de renvoyer les données. Le temps d'attente aléatoire est nécessaire pour éviter que les nœuds essaient de transmettre simultanément, ce qui pourrait entraîner une nouvelle collision.
Ce processus permet de gérer efficacement les collisions sur le réseau Ethernet et d'assurer une transmission fiable des données.

2. Le temps de traversée du signal sur un câble de 1 km de longueur avec une vitesse de propagation de 200 000 km/s est de :

temps = distance / vitesse de propagation = 1 km / 200 000 km/s = 5 µs

3. Pour détecter une collision, il faut que la durée de transmission soit au moins égale à 2 fois le temps de traversée du câble. Donc :

durée de transmission = 2 x temps de traversée = 2 x 5 µs = 10 µs
La quantité d'information qui doit être émise pour détecter une collision dépend de la taille minimale de la trame Ethernet, qui est de 64 octets (512 bits).

4. Si on envoie des trames avec une longueur inférieure à la taille minimale de la trame Ethernet (64 octets), on risque de ne pas détecter les collisions. En effet, si la trame est trop courte, elle peut être transmise avant que le détecteur de collision n'ait le temps de détecter la collision. Dans ce cas, les nœuds émetteurs ne détectent pas la collision et continuent d'envoyer des données, ce qui peut provoquer des erreurs de transmission.

Application 2

5. Pour un débit de 100 Mb/s sur une longueur de segment de 500 m, le temps de traversée du signal est :
   temps = distance / vitesse de propagation = 500 m / (200 000 km/s) = 2,5 µs

6. La longueur minimale d'une trame Ethernet est de 64 octets (512 bits), quel que soit le débit ou la longueur du segment. Cette

longueur minimale est imposée pour permettre la détection des collisions. Si une trame est plus courte que 64 octets, des bits de bourrage sont ajoutés pour atteindre cette longueur minimale.

Application 3

1. Le temps de traversée du signal sur un câble de 1 km de longueur à une vitesse de propagation de 200 000 km/s est donné par la formule suivante :
   Temps de traversée = Longueur du câble / Vitesse de propagation
   Donc, le temps de traversée dans ce cas serait de 5 microsecondes (0,001 km / 200 000 km/s).

2. Pour pouvoir détecter une collision, il faut que deux trames soient en cours de transmission en même temps. Dans ce cas, la quantité d'information qui doit être émise pour détecter une collision est au moins égale à la taille minimale d'une trame Ethernet, qui est de 64 octets, soit 512 bits.

3. Si on envoie des trames avec une longueur inférieure à la longueur minimale, cela peut entraîner une perte de performance et une augmentation du nombre de collisions sur le réseau.

4. Pour un réseau Ethernet de 100 Mb/s sur une longueur de segment de 500m, le temps de traversée du signal serait de 2,5 microsecondes (0,5 km / 200 000 km/s).

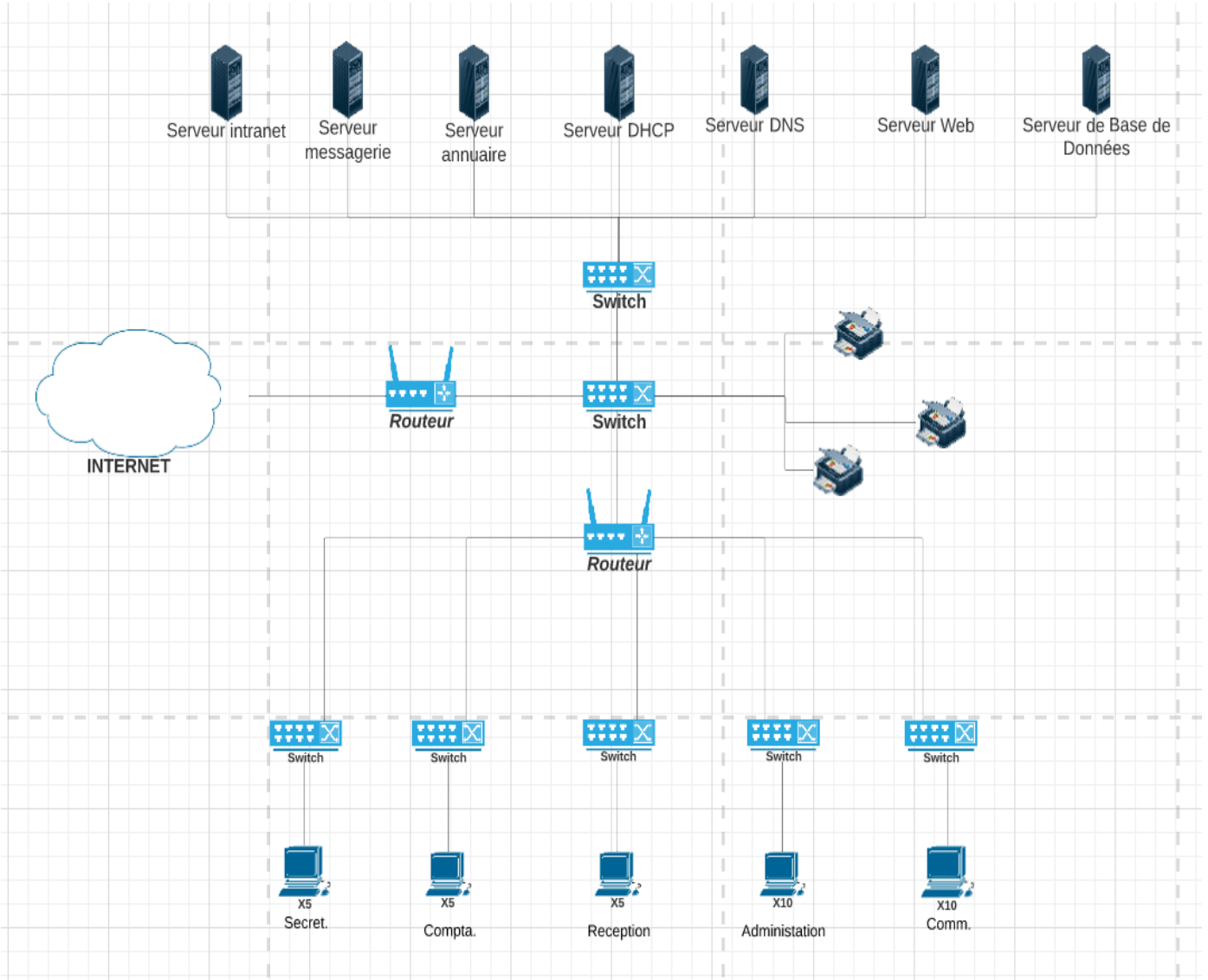
5. La longueur minimale d'une trame Ethernet est de 64 octets, soit 512 bits.

6. L'algorithme de Backoff est utilisé par le protocole CSMA/CD pour éviter les collisions. Lorsqu'une collision se produit, chaque nœud impliqué attend un temps aléatoire avant de renvoyer la trame. Si une nouvelle collision se produit, le temps d'attente est doublé (c'est-à-dire que le nœud attend 2 fois plus longtemps qu'avant). Ce processus est répété jusqu'à ce que le temps d'attente maximum soit atteint, après quoi le nœud abandonne la tentative d'envoi de la trame.

4 - Exercices supplémentaires

TD 3

Exercice 1



Exercice 2

La suite hexadécimale ci-dessous représente le contenu d'une trame ETHERNET (sans le CRC).

f4ca e55f 2df7 0023 dfff 90c3 0800 4500
0033 5bc5 4000 8006
e2d4 0a0a 9f02 d41b 3f03 0a7b 0015 cb8a
8fb1 9636 dd2f 5018
fe20 a778 0000 436f 7563 6f75 212e 200d
0a

En vous aidant de l'annexe 2 qui décrit les formats des principales trames circulant sur un réseau et de la table ascii,
on vous demande d'interpréter le contenu de cette trame.

Question 1)

f4ca e55f 2df7 0023 dfff 90c3 0800 4500
0033 5bc5 4000 8006
e2d4 0a0a 9f02 0a7b 0015 cb8a 8fb1 9636
dd2f 5018
fe20 a778 0000 436f 7563 6f75 212e 200d
0a

- **Légende :**
  - Entête
  - Paquet IP
  - Message TCP
  - Texte Transmis

f4ca e55f 2df7 - Adresse Destination
0023 dfff 90c3 - Adresse Source
0800 - Type

0a7b - Port Source
0015 - Port Destination

436f 7563 6f75 212e 200d 0a - Message correspondant : “Coucou!”

Les différents protocoles mis en oeuvre sont

- Ethernet
- IPv4
- TCP

Question 2)

Ces protocoles se situent dans les couches OSI 2, 3 et 4.

Question 3)

Question 4)

Question 5)

TD 4

I - Configuration IP d’une machine

A - La commande ipconfig (ou ifconfig)

M

```
Z:\>ipconfig /all

Configuration IP de Windows

   Nom de l’hôte . . . . . . . . . . . . : K114-1-6
   Suffixe DNS principal . . . . . . . . : INFO
   Type de noeud. . . . . . . . . . . . . : Hybride
   Routage IP activé . . . . . . . . . . : Non
   Proxy WINS activé . . . . . . . . . . : Non
   Liste de recherche du suffixe DNS.: INFO
                                       dep-info.iutmontp.univ-montp2.fr

Carte Ethernet Ethernet 3 :

   Suffixe DNS propre à la connexion. . . : dep-info.iutmontp.univ-montp2.fr
   Description. . . . . . . . . . . . . . : Intel(R) Ethernet Connection (11) I219-LM
   Adresse physique . . . . . . . . . . . : A4-BB-6D-DB-18-E0
   DHCP activé. . . . . . . . . . . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::15dd:450:51fd:7039%3(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 10.20.114.6(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.0.0
   Bail obtenu. . . . . . . . . . . . . . : jeudi 25 mai 2023 12:35:29
   Bail expirant. . . . . . . . . . . . . : vendredi 26 mai 2023 13:35:28
   Passerelle par défaut. . . . . . . . . : 10.20.0.1
   Serveur DHCP . . . . . . . . . . . . . : 10.20.0.1
   IAID DHCPv6 . . . . . . . . . . . : 379894637
   DUID de client DHCPv6. . . . . . . . : 00-01-00-01-26-54-67-0F-E4-54-E8-6A-3A-88
   Serveurs DNS. . .  . . . . . . . . . . : 10.10.1.1
                                       162.38.221.50
                                       193.51.152.152
   Serveur WINS principal . . . . . . . . : 10.10.1.40
   NetBIOS sur Tcpip. . . . . . . . . . . : Activé

Z:\>
```

B - Découverte d'une table de routage

```
Microsoft Windows [version 10.0.18363.1556]
(c) 2019 Microsoft Corporation. Tous droits réservés.

Z:\>route PRINT
===========================================================================
Liste d'Interfaces
  3...a4 bb 6d db 18 e0 ......Intel(R) Ethernet Connection (11) I219-LM
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Table de routage
===========================================================================
Itinéraires actifs :
Destination réseau    Masque réseau  Adr. passerelle   Adr. interface Métrique
          0.0.0.0          0.0.0.0        10.20.0.1      10.20.114.6     25
        10.20.0.0      255.255.0.0         On-link       10.20.114.6    281
      10.20.114.6  255.255.255.255         On-link       10.20.114.6    281
    10.20.255.255  255.255.255.255         On-link       10.20.114.6    281
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link       10.20.114.6    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link       10.20.114.6    281
===========================================================================
Itinéraires persistants :
  Aucun

IPv6 Table de routage
===========================================================================
Itinéraires actifs :
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
  3    281 fe80::/64                On-link
  3    281 fe80::15dd:450:51fd:7039/128
                                    On-link
  1    331 ff00::/8                 On-link
  3    281 ff00::/8                 On-link
===========================================================================
Itinéraires persistants :
  Aucun

Z:\>
```

1. L'adresse 0.0.0.0 correspond à la destination par défaut.
   L'adresse 127.0.0.0 correspond à la destination hôte, ou "localhost".
   224.0.0.0 correspond à la plage d'adresses multicast.
   L'adresse 255.255.255.255 correspond à l'adresse de destination, ou le "broadcast".

2.

3. Pour le masque 255.255.255.255, toutes les adresses sont prises et aucune ne peut être adressée.

C- La commande tracert (ou traceroute - Linux)

```
Z:\>tracert

Utilisation : tracert [-d] [-h SautsMaxi] [-j ListeHôtes] [-w délai]
              [-R] [-S srcaddr] [-4] [-6] nom_cible

Options :
   -d                 Ne pas convertir les adresses en noms d'hôtes.
   -h SautsMaxi       Nombre maximum de sauts pour rechercher la cible.
   -j ListeHôtes      Itinéraire source libre parmi la liste des hôtes
                      (IPv4 uniquement).
   -w délai           Attente d'un délai en millisecondes pour chaque réponse.
   -R                 Chemin de suivi (IPv6 uniquement).
   -S srcaddr         Adresse source à utiliser (IPv6 uniquement).
   -4                 Force utilisant IPv4.
   -6                 Force utilisant IPv6.

Z:\>
```

WWW.UMONTPELLIER.FR

```
hayem@K114-1-6:~$ traceroute www.umontpellier.fr
traceroute to www.umontpellier.fr (193.51.152.74), 30 hops max, 60 byte packets
 1  _gateway (10.20.0.1)  0.232 ms  0.192 ms  0.172 ms
 2  10.10.0.1 (10.10.0.1)  0.330 ms  0.309 ms  0.290 ms
 3  * * *
 4  192.168.1.2 (192.168.1.2)  0.384 ms  0.365 ms *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
hayem@K114-1-6:~$
```

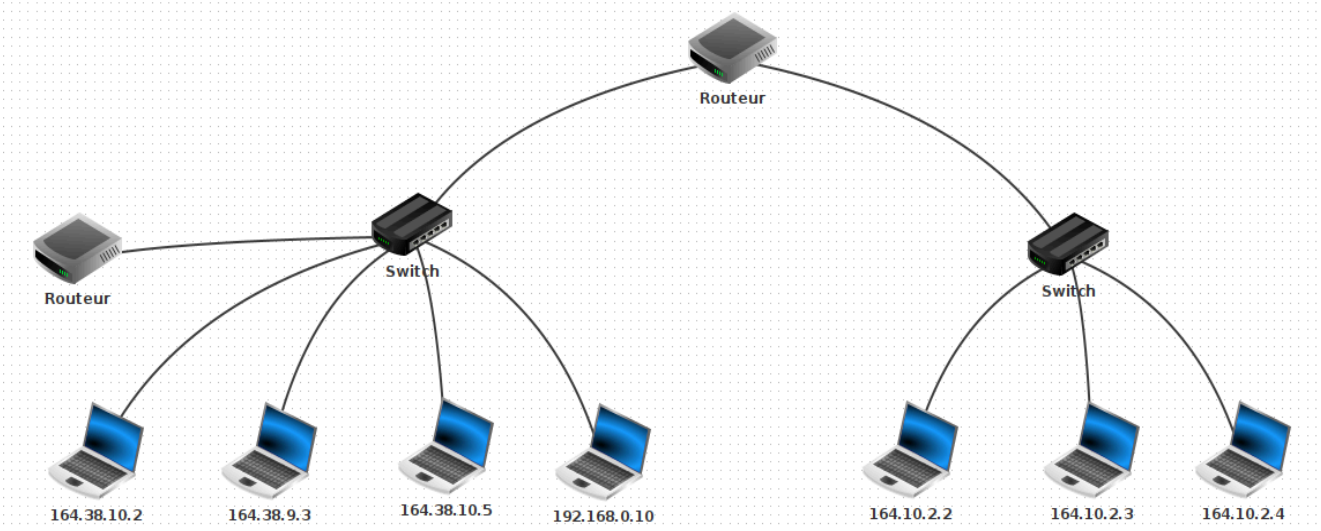
```
hayem@K114-1-6:~$ traceroute www.parisdescartes.fr
traceroute to www.parisdescartes.fr (193.51.86.27), 30 hops max, 60 byte packets
 1  _gateway (10.20.0.1)  0.201 ms  0.223 ms  0.185 ms
 2  10.10.0.1 (10.10.0.1)  0.284 ms  0.256 ms  0.225 ms
 3  * * *
 4  192.168.1.2 (192.168.1.2)  0.315 ms  0.288 ms  0.265 ms
 5  sortie-triolet5-vlan0102.univ-montp2.fr (162.38.102.100)  0.391 ms  0.367 ms  0.394 ms
 6  195.83.174.146 (195.83.174.146)  0.736 ms  0.970 ms *
 7  * vl1759-be6-ren-nr-montpellier-rtr-091.noc.renater.fr (193.55.203.145)  2.207 ms *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * 195.221.127.6 (195.221.127.6)  18.199 ms *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
hayem@K114-1-6:~$
```

```
hayem@K114-1-6:~$ traceroute www.yahoo.com
traceroute to www.yahoo.com (87.248.100.215), 30 hops max, 60 byte packets
 1  _gateway (10.20.0.1)  0.233 ms  0.195 ms  0.174 ms
 2  10.10.0.1 (10.10.0.1)  0.430 ms  0.404 ms  0.384 ms
 3  * * *
 4  192.168.1.2 (192.168.1.2)  0.491 ms * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * reserve-ip8-ren-nr-lyon2-rtr-091.noc.renater.fr (193.51.177.104)  13.788 ms
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * usw1-1-lbc.ir2.yahoo.com (77.238.190.106)  31.799 ms  31.832 ms
17  media-router-fp73.prod.media.vip.ir2.yahoo.com (87.248.100.215)  33.083 ms  33.158 ms  33.138 ms
hayem@K114-1-6:~$
```

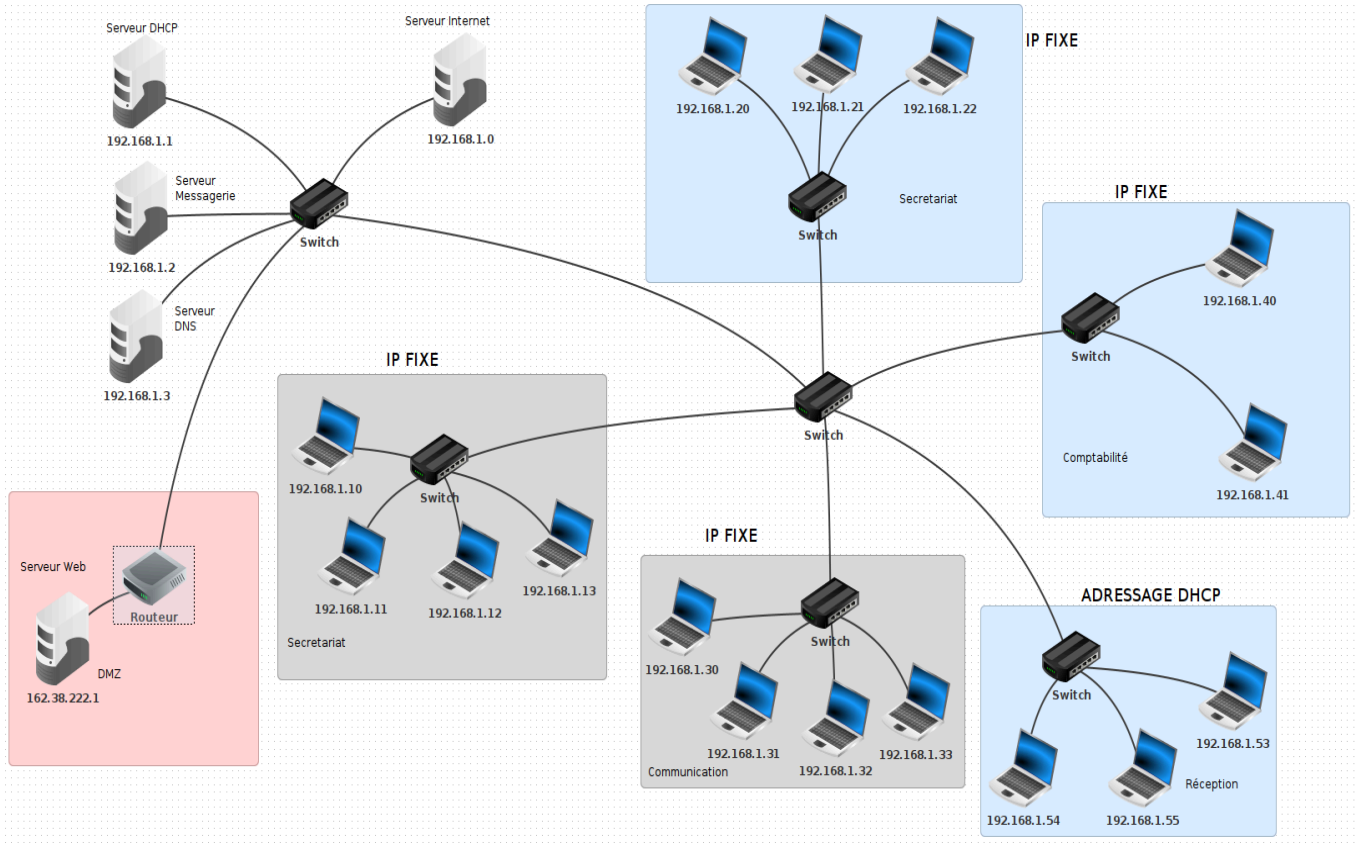
```
hayem@K114-1-6:~$ traceroute -4 216.239.53.101 www.yahoo.com
Cannot handle "packetlen" cmdline arg `www.yahoo.com' on position 2 (argc 3)
hayem@K114-1-6:~$ traceroute -4 www.yahoo.com
traceroute to www.yahoo.com (87.248.100.216), 30 hops max, 60 byte packets
 1  _gateway (10.20.0.1)  0.198 ms  0.190 ms  0.185 ms
 2  10.10.0.1 (10.10.0.1)  0.337 ms  0.332 ms  0.328 ms
 3  * * *
 4  192.168.1.2 (192.168.1.2)  0.483 ms  0.480 ms  0.475 ms
 5  sortie-triolet5-vlan0102.univ-montp2.fr (162.38.102.100)  0.607 ms * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * xe-0-0-9-paris2-rtr-131.noc.renater.fr (193.51.177.9)  18.159 ms xe0-1-9-paris2-rtr-131.noc.renater.fr (193.51.177.144)  18.116 ms
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * media-router-fp74.prod.media.vip.ir2.yahoo.com (87.248.100.216)  31.629 ms  31.586 ms
hayem@K114-1-6:~$
```

II - Adressage IP

A - Recherche d’anomalies



B1 - Configuration d'un réseau



Questions techniques

1) Les adresses qui commencent par 192 sont des adresses privées. Les adresses commençant par 168 sont des adresses publiques.

2) Ce sont des adresses de classe C. Le masque associé est 255.255.255.0.

3) Le serveur web n'a pas la même adresse IP car elle est publique, ce qui est nécessaire pour accéder au réseau web.

4) Un serveur DMZ peut filtrer les accès, renforcer la sécurité, isoler le réseau interne et fournir des fonctionnalités de surveillance pour maintenir la sécurité et la disponibilité des ressources internes.

5) Le rôle d'un serveur DHCP est d'attribuer automatiquement aux différents éléments d'un réseau une adresse IP comprise dans une plage d'adressage donnée au préalable selon le masque de sous-réseau.

6) (Visible sur le schéma ci-dessus)

7)

Table de routage

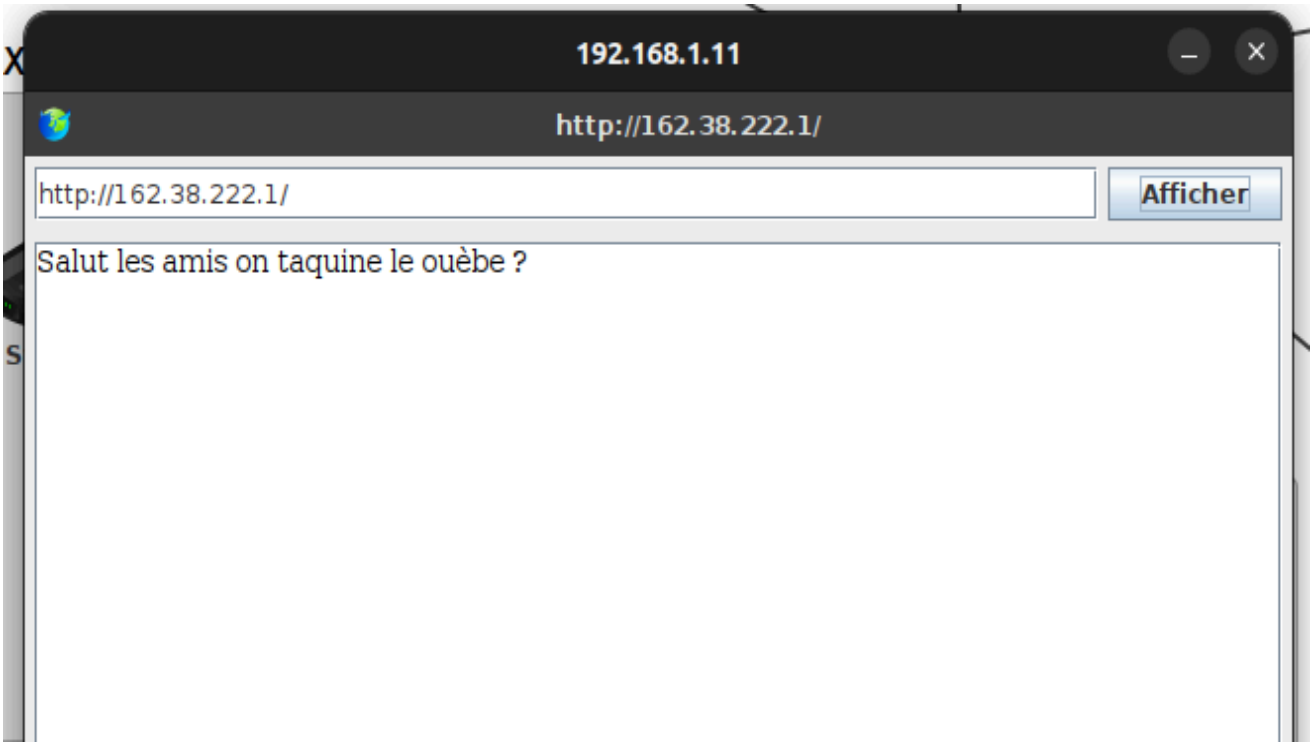
IP de destination	Masque	Passerelle suivante	Via l'interface
162.38.222.254	255.255.255.255	127.0.0.1	127.0.0.1
192.168.1.254	255.255.255.255	127.0.0.1	127.0.0.1
162.38.222.0	255.255.255.0	162.38.222.254	162.38.222.254
192.168.1.0	255.255.255.0	192.168.1.254	192.168.1.254
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1

x

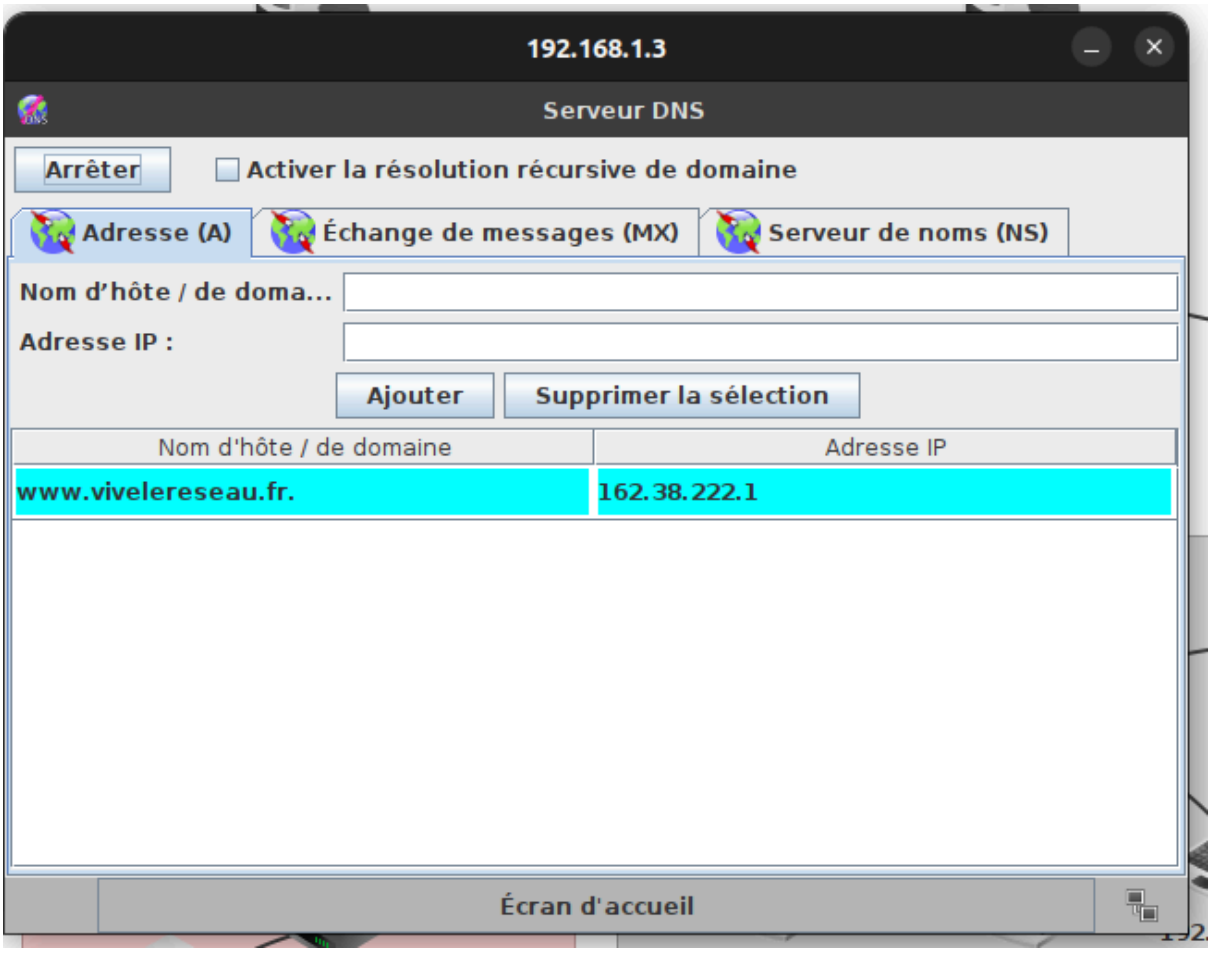
B2 - Application pratique DHCP / Serveur Web / DNS

1) ADRESSAGE POSTES CLIENTS

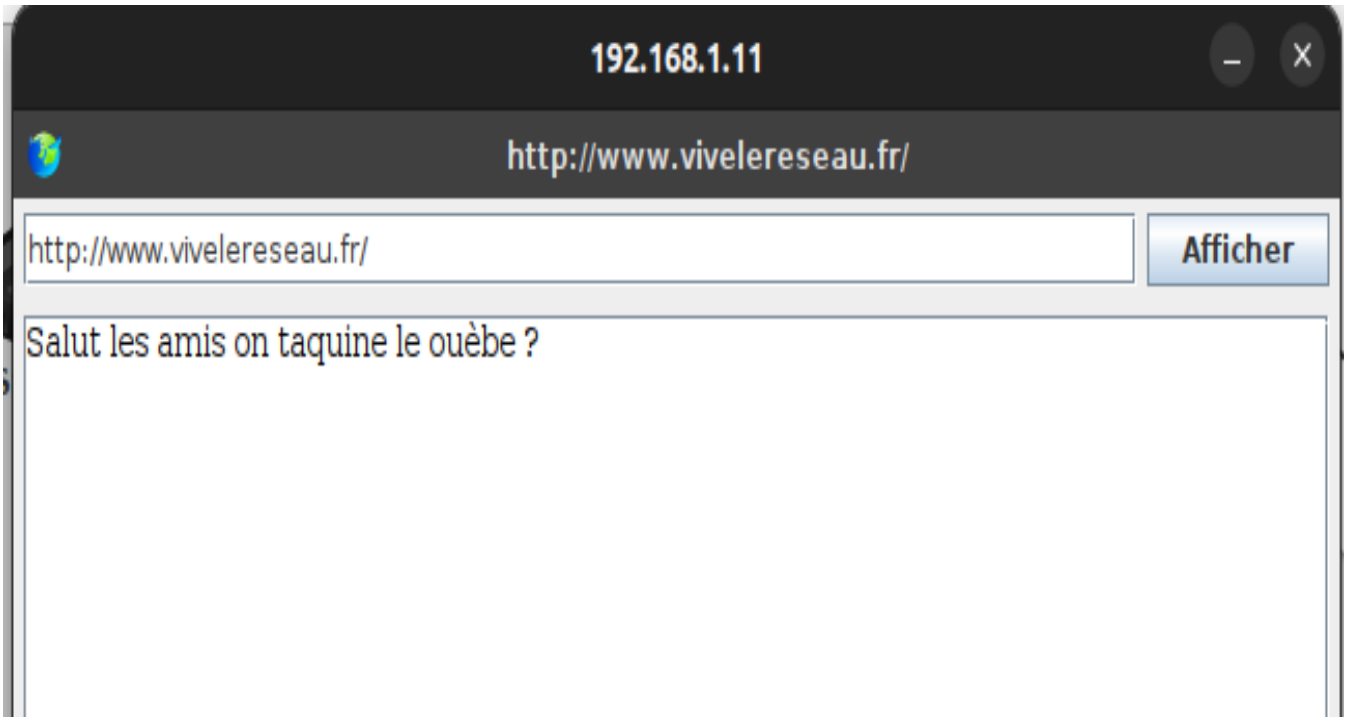
2) APPLICATION Serveur Web sur le poste 162.38.222.1



6) APPLICATION UTILISATION DU DNS



6) RESULTAT APPLICATION UTILISATION DU DNS



III - Etudes de cas (Optionnel)

Questions techniques