TD1

1 Classes d'adresses IPv4

Au début d'internet, les adresses IPv4 étaient découpées en 5 classes :

Classe A: les adresses commençant par 0, le premier octet identifiant le réseau ;

Classe B: les adresses commençant par 10, les deux premiers octets identifiant le réseau ;

Classe C: les adresses commençant par 110, les trois premiers octets identifiant le réseau ;

Classe D: les adresses commençant par 1110, réservées pour le multicast ;

Classe E: les adresses commençant par 1111, réservées par l'IANA.

La notation CIDR introduite en 1993 a rendu les classes A, B et C obsolètes. La contrepartie est de devoir indiquer pour chaque adresse la taille de son masque de sous-réseau.

1. Pour chaque classe, préciser la plage d'adresses concernée et le masque de sous-réseau associé.
2. Rappeler les plages d'adresses réservées pour les réseaux privées. Quelles sont leurs classes ?
3. Donner le nombre d'adresses IP disponibles avec le système de classes. Comparer avec la notation CIDR et l'agrégation des sous-réseaux.

2 Autour du protocole ICMP

Le protocole ICMP (Internet Control Message Protocol)[1] est un protocole de couche 3 qui permet de diagnostiquer les erreurs de transmission. On décrit ici le protocole ICMP pour IPv4, dont l'en-tête fait 32 bits, répartis selon la façon suivante :

- le premier octet code le type du message, allant de 0 à 18 ;
- le deuxième octet correspond au code d'erreur, allant de 0 à 15 ;
- le reste est une somme de contrôle.

Bien que ce protocole agisse à la même couche qu'IP, le paquet ICMP est encapsulé dans un datagramme IP. La commande *ping <IP>* envoie par exemple une série de paquets ICMP à l'adresse IP fournie en argument avec le type 8 (demande d'ECHO). Le destinataire répond avec des paquets ICMP de type 0 (réponse à un ECHO). L'intérêt de cette commande est notamment d'afficher à l'écran l'ensemble des messages d'erreurs envoyés via ICMP par les routeurs rencontrés sur le chemin.

1. Représenter comment un paquet ICMP est encapsulé dans une trame Ethernet. Quelles sont les différences avec l'encapsulation d'un message de couche 4 tel qu'un datagramme UDP ?
2. Afin d'éviter qu'un paquet ne reste indéfiniment sur le réseau, le protocole IP contient un champ TTL (Time To Live) qui se décrémente à chaque routeur rencontré (voir en Figure 5). Lorsqu'un routeur voit un message avec un champ TTL à 0, il jette ce message et envoie à la place un paquet ICMP à la source avec le type 11 (Temps de vie dépassé). Utiliser ce principe pour proposer un algorithme pour la commande *traceroute <IP>* dont le but est d'afficher la liste des routeurs rencontrés sur le chemin vers la machine avec l'adresse IP fournie.
3. Le serveur derrière www.epita.fr est indisponible. La commande *traceroute www.epita.fr* montre deux routeurs qui se répètent indéfiniment. Qu'est-ce qui se passe et comment y remédier ?
4. La commande *traceroute www.moodle.com* montre que les routeurs 6 et 7 sont en fait le même routeur. Qu'est-ce qui se passe ? Est-ce une erreur ?

[1] décrit dans la RFC 792 : https://tools.ietf.org/html/rfc792

3 Exemple de réseau

On considère un réseau dont le schéma est représenté avec le logiciel de simulation GNS3[2] en Figure 1. Les spécifications des composants sont donnés en Figure 2. Seul le routeur 2 a accès au reste d'Internet, et ce via l'interface eth1.

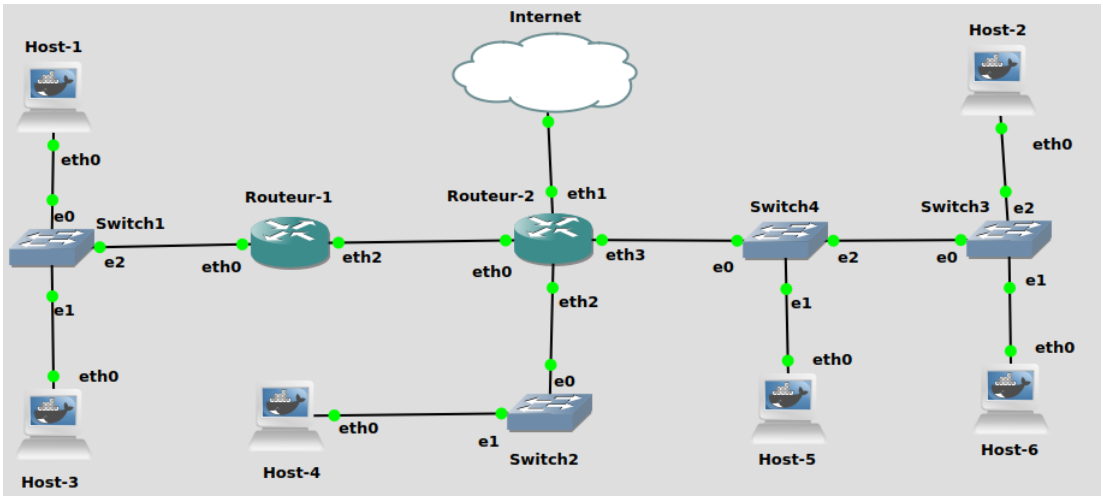

Figure 1: Schéma GNS3 du réseau.

Machine	Interface	Adresse MAC	Adresse IP
Host 1	eth0	ce:b1:3b:31:a5:24	192.168.10.2/24
Host 3	eth0	ce:b1:3b:31:a5:25	192.168.10.3/24
Routeur 1	eth0	96:a1:64:e7:96:84	192.168.10.1/24
Routeur 1	eth2	96:a1:64:e7:96:85	42.42.42.42/31
Routeur 2	eth0	00:06:5b:10:6c:82	42.42.42.43/31
Host 4	eth0	00:68:eb:10:a2:04	192.168.20.2/24
Routeur 2	eth2	00:06:5b:10:6c:84	192.168.20.1/24
Host 2	eth0	00:68:eb:10:a2:02	192.168.30.2/24
Host 4	eth0	00:68:eb:10:a2:04	192.168.30.3/24
Host 6	eth0	00:68:eb:10:a2:06	192.168.30.4/24
Routeur 2	eth3	00:06:5b:10:6c:85	192.168.30.1/24

Figure 2: Spécifications des différentes machines du réseau.

1. Rappeler le rôle et la couche de chacune des machines.
2. Lister les différents sous-réseaux qui apparaissent.
3. Donner les tables de routage (statique) des deux routeurs et des Hosts 2, 3 et 4.
4. La plage d'adresse 42.32.0.0 à 42.47.255.255 est possédée par une entreprise sud-coréenne. Leur site est-il accessible depuis un des Hosts ? Si oui, lesquels ?
5. On fait l'hypothèse que le réseau est correctement configuré et que chaque machine vient de lancer une requête ARP gratuite. Décrire l'ensemble des messages envoyés dans le réseau et les adresses qu'ils contiennent lorsque Host 1 exécute la commande *ping 192.168.30.2*.
6. Même question, mais on suppose que tous les caches ARP sont vides.

[2] https://www.gns3.com/

7. On tente les commandes suivantes. Exécuter la commande *ping 192.168.30.2* depuis Host 1 n'affiche aucune réponse. L'exécution de la commande *ping 192.168.10.1* depuis Host 2 affiche un paquet ICMP de la part de 192.168.30.1 avec un type 3 (Destinataire inaccessible) et un code 0 (Le réseau n'est pas accessible). Quelle est l'erreur de configuration ? Comment la corriger ?

8. Un sniffeur écoute le réseau et lit sur Wireshark la trame Ethernet présenté en Figure 3. À quel niveau du réseau se trouve le sniffeur ? Utiliser les en-têtes présentés en annexe pour décoder la trame et le message contenu.

```
0000  96 a1 64 e7 96 84 ce b1  3b 31 a5 24 08 00 45 00   ··d····· ;1·$··E·
0010  00 54 c3 62 40 00 40 01  cd f1 c0 a8 0a 02 c0 a8   ·T·b@·@· ········
0020  1e 02 08 00 9e 64 00 63  00 03 73 d6 ac 61 00 00   ·····d·c ··s··a··
0030  00 00 79 2a 01 00 00 00  00 00 10 11 12 13 14 15   ··y*···· ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                             67
```

Figure 3: Capture Wireshark du réseau.

Annexe

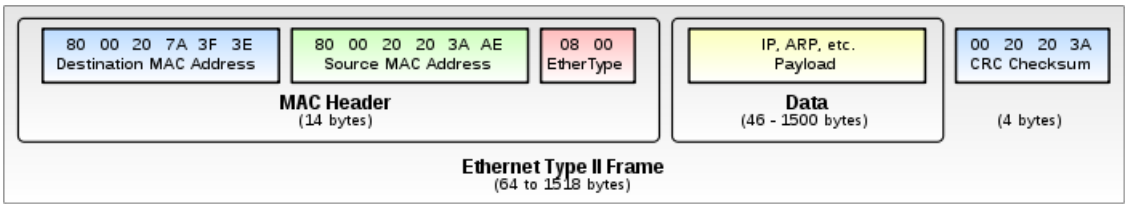

Figure 4: En-tête Ethernet type II (sans le préambule).

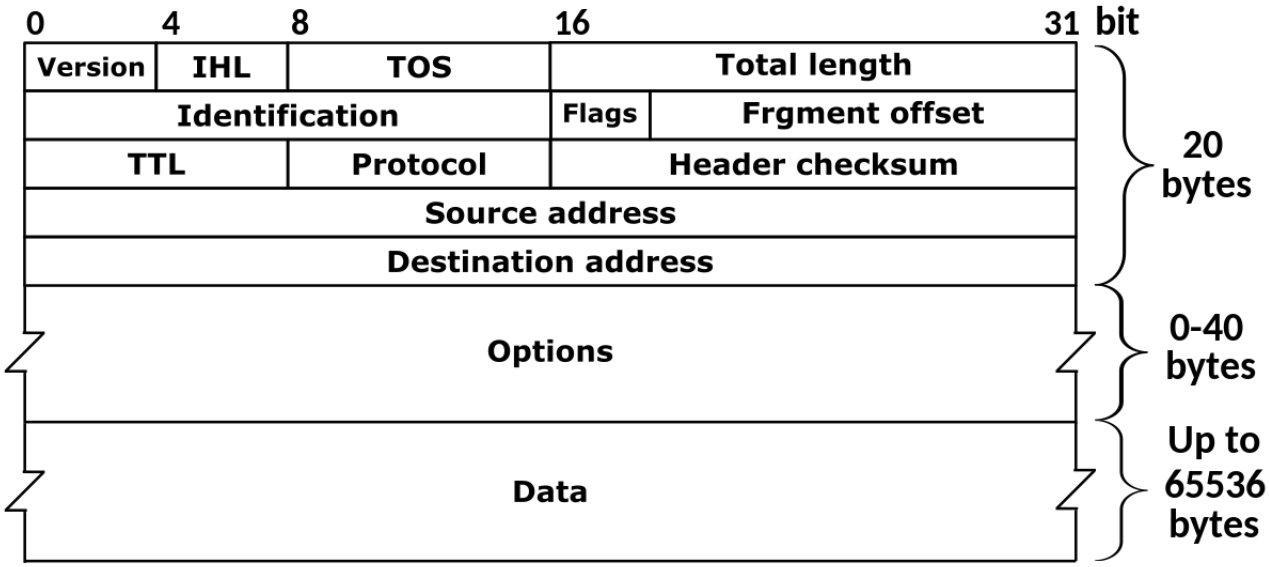

Figure 5: En-tête IPv4.