TD 6

ACHEMINEMENT IP & ICMP

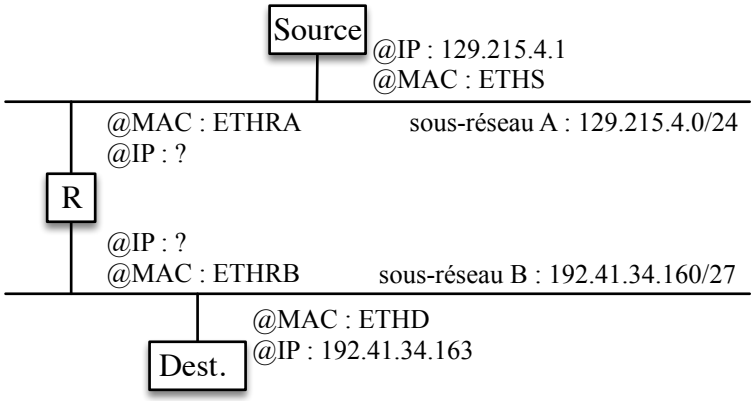
1. ACHEMINEMENT DIRECT / INDIRECT

Il existe deux façons d'acheminer un paquet IP :

- L'**acheminement direct** concerne la transmission d'un paquet IP entre deux machines connectées au même réseau physique. La source encapsule le paquet dans une trame dont l'adresse de destination est l'adresse MAC (Ethernet) de la destination.
- L'**acheminement indirect** intervient lorsque la destination n'est pas connectée au même réseau physique que la source. La transmission du paquet est alors effectuée de proche en proche (*hop by hop*) ; les tables d'acheminement fournissent l'adresse du prochain routeur (*gateway*) sur le chemin vers la destination. Chaque paquet est alors encapsulé dans une trame dont l'adresse MAC de destination est celle du prochain routeur (*next hop*).

Exercice 1.1 | Acheminement & ARP

On considère deux sous-réseaux A et B interconnectés par un routeur IP comme décrit dans la figure suivante (les adresses MAC étant représentées de façon symbolique) :



1. Combien d'adresses IP sont disponibles pour le routeur R sur chacun des sous-réseaux A et B ? Quelle est, sur chacun, la première adresse (contenant le plus possible de bits à 0) et la dernière adresse (contenant le plus possible de bits à 1) utilisables par le routeur ?

Dans la suite, on choisira pour le routeur R, la dernière adresse IP possible (celle contenant le plus de bits à 1) sur chaque sous-réseau.

La machine source doit envoyer un paquet IP à la machine destination. S'agissant d'un acheminement indirect, la source doit, dans un premier temps, envoyer le paquet au routeur R qui est le prochain saut vers la destination. Pour cela la source doit tout d'abord connaître l'adresse MAC du routeur R sur le sous-réseau A. Elle utilise pour cela le protocole ARP.

2. Remplir le tableau suivant avec les valeurs de l'entête des trames Ethernet encapsulant les deux messages ARP (la requête et la réponse) circulant sur le sous-réseau A.

	Adresse MAC source	**Adresse MAC destination**
Requête ARP		
Réponse ARP		

3. Compléter le tableau suivant en indiquant les adresses telles qu'elles apparaissent dans ces deux messages ARP.

	Source		**Cible**	
	Adresse MAC	**Adresse IP**	**Adresse MAC**	**Adresse IP**
Requête ARP				
Réponse ARP				

4. A l'issue de cet échange ARP, la source peut envoyer son paquet au routeur R. Compléter les entêtes Ethernet et IP de ce paquet transmis sur le sous-réseau A.

Adresse MAC		**Adresse IP**	
Source	**Destination**	**Source**	**Destination**

Le routeur R doit alors retransmettre le paquet à la destination. Pour cela il doit tout d'abord connaître l'adresse MAC de la machine de destination située sur le sous-réseau B. Il utilise à son tour le protocole ARP.

5. Remplir le tableau suivant avec les valeurs de l'entête des trames Ethernet encapsulant les deux messages ARP (la requête et la réponse) circulant sur le sous-réseau B.

	Adresse MAC source	**Adresse MAC destination**
Requête ARP		
Réponse ARP		

6. Compléter le tableau suivant en indiquant les adresses telles qu'elles apparaissent dans ces deux messages ARP.

	Source		**Cible**	
	Adresse MAC	**Adresse IP**	**Adresse MAC**	**Adresse IP**
Requête ARP				
Réponse ARP				

7. A l'issue de cet échange ARP, la source peut envoyer son paquet au routeur R. Compléter les entêtes Ethernet et IP de ce paquet transmis sur le sous-réseau B.

Adresse MAC		**Adresse IP**	
Source	**Destination**	**Source**	**Destination**

2. TABLE DE ROUTAGE IP & ACHEMINEMENT (*FORWARDING*)

Une table de routage IP (ou table d'acheminement IP ou FIB pour *Forwarding Information Base*) est constituée d'au moins quatre colonnes :

`Destination`	`Mask`	`Gateway`	`Interface`

- La colonne `Destination` indique la destination que permet de joindre cette entrée ;
- La colonne `Mask` spécifie le masque associé à cette destination ;
- La colonne `Gateway` indique l'adresse du prochain routeur (en cas d'acheminent indirect) ;
- La colonne `Interface` indique l'interface sur laquelle le paquet doit être transmis pour suivre la route considérée.

Exercice 2.1

On considère un routeur R1 ayant la table de routage suivante :

`Destination`	`Mask`	`Gateway`	`Interface`
192.4.153.1	255.255.255.255	R2	eth0
192.4.153.128	255.255.255.192	R3	eth0
128.96.33.0	255.255.255.128	*	eth0
128.96.34.0	255.255.255.128	*	eth1
128.96.40.0	255.255.255.0	R2	eth0
0.0.0.0	0.0.0.0	R4	eth1

Le routeur R1 peut donc délivrer directement des paquets sur ses interfaces eth0 et eth1, ou faire suivre des paquets aux routeurs R2, R3 et R4.

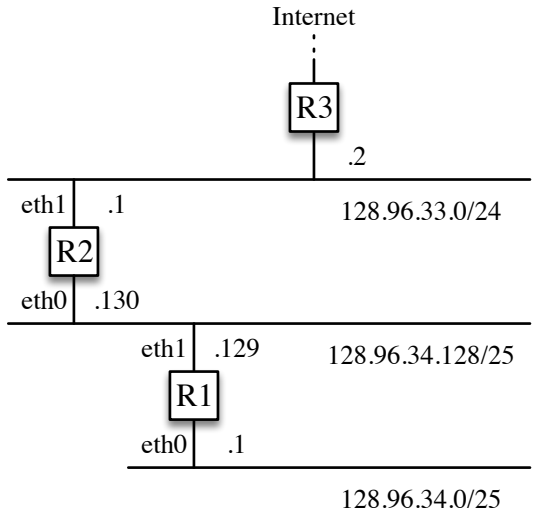
1. Indiquer ce que fait R1 sur réception d'un paquet adressé aux destinations suivantes :

Adresse de destination	Prochaine étape
M1 : 128.96.33.10	
M2 : 128.96.34.12	
M3 : 128.96.40.151	
M4 : 192.4.153.133	
M5 : 192.4.153.1	
M6 : 192.4.153.90	

2. Faire un schéma du réseau sur lequel apparaissent les routeurs (R1 à R4), ainsi que toutes les destinations de la table précédente (M1 à M6).

Exercice 2.2

On considère un réseau décomposé en trois sous-réseaux et représenté sur la figure suivante :



1. Donner les lignes des tables de routage des routeurs R1 et R2 que l'on peut déduire du schéma.

   Table de routage de R1 :

Destination	Mask	Gateway	Interface

Table de routage de R2 :

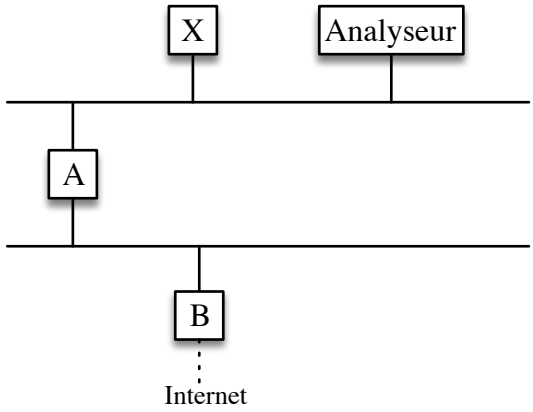
Destination	Mask	Gateway	Interface

3. PROTOCOLE ICMP

ICMP (*Internet Control Message Protocol*) est utilisé pour véhiculer des messages de contrôle et des rapports d'erreurs, par exemple à des fins de tests ou lorsqu'un service ou un hôte est inaccessible. ICMP peut être vu comme la partie contrôle de IP, et à ce titre, les deux protocoles sont indissociables.

Exercice 3.1

Un analyseur de réseau (de type Wireshark) est disposé sur un réseau local Ethernet afin de permettre l'observation des trames circulant sur le support. La structure du dispositif de mesure est la suivante :



On y voit deux réseaux Ethernet appartenant à la même organisation, interconnectés via un routeur A, ainsi qu'une connexion vers l'extérieur réalisée via le routeur B.

Une trace a été obtenue par l'analyseur (les deux trames sont données sans préambule ni CRC) :

```
08 00 20 0a ac 96 08 00 20 0a 70 66 08 00 4f 00
00 7c cb c9 00 00 ff 01 b9 7f 84 e3 3d 05 c0 21
9f 06 07 27 04 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 08 00 a2 56 2f 00
00 00 29 36 8c 41 00 03 86 2b 08 09 0a 0b 0c 0d
0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d
1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d
2e 2f 30 31 32 33 34 35 36 37
```

```
08 00 20 0a 70 66 08 00 20 0a ac 96 08 00 4f 00
00 7c 3f 86 00 00 fb 01 49 af c0 21 9f 06 84 e3
3d 05 07 27 28 84 e3 3c 20 c0 2c 41 12 c0 46 47
05 c0 21 9f 02 c0 21 9f 06 c0 46 47 06 c0 2c 41
1a 84 e3 3c 1e 84 e3 3d 87 00 00 00 aa 56 2f 00
00 00 29 36 8c 41 00 03 86 2b 08 09 0a 0b 0c 0d
0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d
1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d
2e 2f 30 31 32 33 34 35 36 37
```

On s'intéresse tout d'abord à la première trame.

1. A l'aide d'un décodage manuel de la première trame, identifier les différentes unités de données encapsulées (trame, paquet, message). Pour chacune, donner leur taille, la taille de leur en-tête et la taille des éventuelles options.
2. Quelles sont les adresses MAC et IP contenues dans la première trame (et le datagramme encapsulé) ? A quelles machines correspondent-elles ?
3. Le datagramme encapsulé est-il fragmentable ? Est-il fragmenté ?
4. Qu'est-ce qui prouve qu'il vient tout juste d'être émis ?
5. Combien d'options comporte l'en-tête du datagramme ? A quel(s) type(s) correspond(ent)-elle(s) ?
6. Combien y-a-t-il d'octets de bourrage (cadrage) dans l'en-tête du premier datagramme et à quoi servent-ils ?
7. Quel est le type du message encapsulé par le datagramme ?
8. Quel est le but de cet échange ?

On considère maintenant la seconde trame.

9. Vérifier que la deuxième trame possède la même structure que la première.
10. Comparer les adresses MAC et IP contenues dans cette trame avec celle de la première trame, et vérifier qu'il s'agit bien de la « réponse » à la trame précédente.
11. Combien de routeurs le datagramme encapsulé a-t-il traversé ?
12. Combien d'adresses ont été enregistrées dans les options de ce deuxième datagramme ? A quoi correspondent-elles ? L'enregistrement de route peut-il être incomplet ?
13. Faire un schéma symbolique des différents réseaux et passerelles empruntés par les datagrammes. Représenter sur ce schéma les différentes adresses Ethernet et IP utilisées.