

Examen 3I014 « Réseaux »

Jeudi 10 Janvier 2019 – Durée : 2 heures

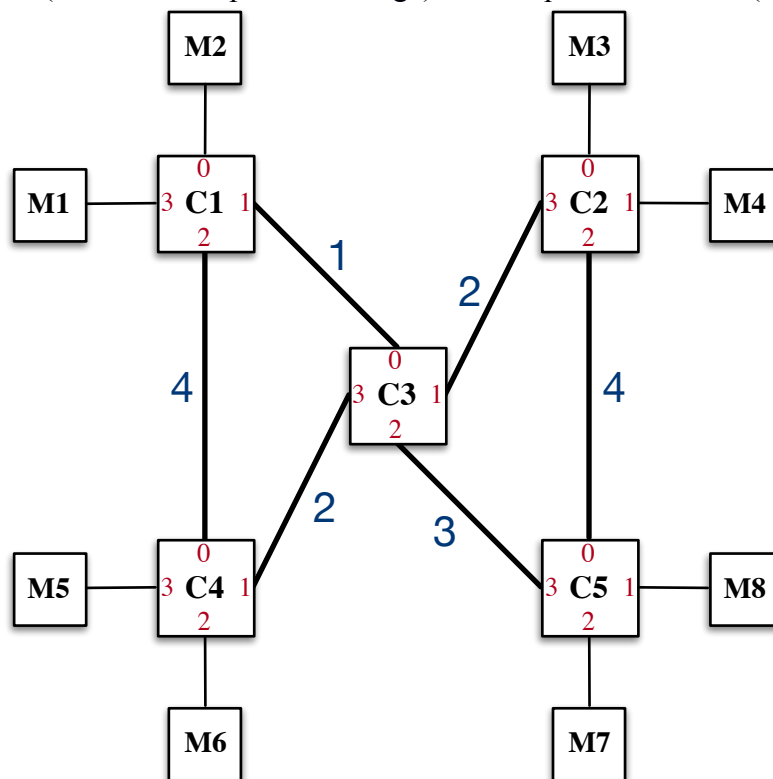
Sont autorisées : 1 feuille A4 manuscrite recto/verso, 1 calculatrice (téléphone interdit)

Voici :

- 4 feuilles contenant les énoncés et les zones de réponse à compléter (sans déborder). **Vous devez reporter votre numéro d'anonymat sur chacune des feuilles.**
- 3 feuilles d'annexe que vous pouvez détacher.

Exercice 1 : Routage et commutation (5 points)

On considère le réseau suivant constitué de 5 commutateurs (C1 à C5) et de 8 machines (M1 à M8). Chaque commutateur possède 4 ports (numérotés de 0 à 3). Chaque machine est connectée directement et de façon unique sur un des ports d'un commutateur. Les commutateurs sont reliés par 6 liaisons bidirectionnelles dont le « poids » (critère utilisé pour le routage) est indiqué sur chacune (entre 1 et 4).



1. Donner les tables de routage des 5 commutateurs (après convergence des algorithmes).

C1			C2			C3			C4			C5		
dest	next	dist	dest	next	dist	dest	next	dist	dest	next	dist	dest	next	dist
C2	C3	3	C1	C3	3	C1	C1	1	C1	C3	3	C1	C3	4
C3	C3	1	C3	C3	2	C2	C2	2	C2	C3	4	C2	C2	4
C4	C3	3	C4	C3	4	C4	C4	2	C3	C3	2	C3	C3	3
C5	C3	4	C5	C5	4	C5	C5	3	C5	C3	5	C4	C3	5

On suppose que le réseau fonctionne en mode connecté. Chaque commutateur possède donc, en plus de sa table de routage, une table de commutation mémorisant les différents circuits virtuels le traversant. On supposera qu'initialement aucun circuit virtuel n'est ouvert et que toutes les tables de commutation sont vides. On supposera par ailleurs que dès qu'un commutateur (ou qu'une machine) doit choisir un numéro de voie logique (VL) il (elle) utilisera le plus petit entier disponible supérieur ou égal à 1.

- Remplir les tables de commutation des différents commutateurs à l'issue de chacun des événements suivants (chaque événement se terminant avant que le suivant commence). Pour une ouverture de circuit virtuel, indiquer les entrées à ajouter des tables ; pour une fermeture de circuit virtuel, indiquer les entrées à retirer des tables.

Ev1 : ouverture d'un circuit virtuel entre M1 et M3 ;

Ev2 : ouverture d'un circuit virtuel entre M2 et M5 ;

Ev3 : ouverture d'un circuit virtuel entre M3 et M7 ;

Ev4 : ouverture d'un circuit virtuel entre M3 et M2 ;

Ev5 : fermeture du circuit virtuel entre M2 et M5 ;

Ev6 : ouverture d'un circuit virtuel entre M1 et M4.

	C1				C2				C3				C4				C5			
	port	VL	port	VL	port	VL	port	VL	port	VL	port	VL	port	VL	port	VL	port	VL	port	VL
Ev1	3	1	1	1	3	1	0	1	0	1	1	1								
Ev2	0	1	1	2					0	2	3	1	1	1	3	1				
Ev3					0	2	2	1									0	1	2	1
Ev4	1	3	0	2	0	3	3	2	1	2	0	3								
Ev5	0	1	1	1					0	2	3	1	1	1	3	1				
Ev6	3	2	1	2	3	3	1	1	0	2	1	3								

- Que se passe-t-il si la liaison entre C2 et C3 tombe en panne ? Développer la réponse.

Tous les circuits virtuels empruntant cette liaison tombent. Il s'agit ici des circuits virtuels entre M1 et M3, entre M3 et M2, et entre M1 et M4. Les algorithmes de routage sont censés réagir « vite » afin de découvrir de nouvelles routes. Ainsi, toutes les routes passant par la liaison C2-C3 devront emprunter successivement les deux liaisons C2-C5 puis C5-C3.

Exercice 2 : Plan d'adressage (5 points)

Un administrateur doit configurer 4 sous-réseaux : les sous-réseaux A et B doivent disposer de 300 adresses IP chacun, tandis que les sous-réseaux C et D en contiendront au plus 100 chacun.

- Sur combien de bits les NetId (préfixe réseau) et HostId de chaque sous-réseau devront-ils être codés ?

	Net ID	Host ID
Sous-réseaux A et B	23	9
Sous-réseaux C et D	25	7

L'administrateur s'adresse alors à un organisme capable d'attribuer des préfixes réseaux. Cet organisme peut mettre en place deux politiques : la première consiste à attribuer une seule adresse dont le masque est suffisant pour pouvoir répondre au cahier des charges de l'administrateur, la deuxième solution consiste à attribuer plusieurs préfixes d'adresses de classe C contigus. Cet organisme doit définir quelle solution présentera le meilleur taux d'utilisation des adresses.

- Le premier choix envisagé consiste donc à attribuer l'adresse réseau suivante : 195.139.48.0 / 21.

- Indiquez la valeur de cette adresse au format binaire :

11000011 . 10001011 . 00110000 . 00000000 195.139.48.0/21
octet 1 octet 2 octet 3 octet 4

- Proposez un plan d'adressage cohérent avec les informations données à la question 1. Pour chaque sous-réseau, indiquez l'adresse IP du sous-réseau, celle de la première et de la dernière adresse disponible.

L'affectation se fait dans l'ordre : le sous-réseau A prend la première adresse IP disponible, ... Vous donnerez les adresses IP en notation décimale pointée, le masque et vous mettrez en correspondance la valeur binaire des 2 derniers octets des adresses IP.

	adresse au format binaire												adresse en décimal pointé	masque				
	octet 3					octet 4												
sous réseau A	0	0	1	1	0	0	0	0	.	0	0	0	0	0	0	0	195.139.48.0	/23
1er poste	0	0	1	1	0	0	0	0	.	0	0	0	0	0	0	1	195.139.48.1	/23
dernier poste	0	0	1	1	0	0	0	1	.	1	1	1	1	1	1	0	195.139.49.254	/23
<hr/>																		
sous réseau B	0	0	1	1	0	0	1	0	.	0	0	0	0	0	0	0	195.139.50.0	/23
1er poste	0	0	1	1	0	0	1	0	.	0	0	0	0	0	0	1	195.139.50.1	/23
dernier poste	0	0	1	1	0	0	1	1	.	1	1	1	1	1	1	0	195.139.51.254	/23
<hr/>																		
sous réseau C	0	0	1	1	0	1	0	0	.	0	0	0	0	0	0	0	195.139.52.0	/25
1er poste	0	0	1	1	0	1	0	0	.	0	0	0	0	0	0	1	195.139.52.1	/25
dernier poste	0	0	1	1	0	1	0	0	.	0	1	1	1	1	1	0	195.139.52.127	/25
<hr/>																		
sous réseau D	0	0	1	1	0	1	0	0	.	1	0	0	0	0	0	0	195.139.52.128	/25
1er poste	0	0	1	1	0	1	0	0	.	1	0	0	0	0	0	1	52.129	/25
dernier poste	0	0	1	1	0	1	0	0	.	1	1	1	1	1	1	0	52.254	/25

On définit le taux d'utilisation de l'adresse réseau comme le nombre d'adresses IP attribuées (@ des machines attribuées, @ réseau, @ de diffusion) sur le nombre total d'adresses IP disponibles dans un réseau.

c. Quel sera le taux d'utilisation de votre configuration ?

Sous réseau A : machines 300 + @sous réseau + @diffusion = 302
Sous réseau B : machines 300 + @sous réseau + @diffusion = 302
Sous réseau C : machines 100 + @sous réseau + @diffusion = 102
Sous réseau B : machines 100 + @sous réseau + @diffusion = 102
Nombre d'adresses requises = 808
Nombre total d'adresses IP disponibles en /21 = 2^{11}
 $U = 0,39$

L'organisme d'attribution d'adresses évalue ensuite le taux d'utilisation obtenu avec la deuxième approche consistant à attribuer des adresses de classe C contigües. Ainsi au lieu d'allouer une seule adresse 195.139.48.0/21, il attribue 195.139.48.0/24 puis 195.139.49.0/24, ...

3. Indiquez le nombre minimum d'adresses de classe C contigües qu'il faudrait pour gérer la configuration demandée. Vous préciserez quelle(s) adresse(s) réseau sera(ont) alors affectée(s) à chaque sous-réseau en partant de 195.139.48.0/24 pour le sous-réseau A. (Attention : n'oubliez pas d'indiquer le masque pour chaque adresse de réseau.)

Nombre minimum d'adresses de classe C requis :
Sous réseau A : 195.139.48.0/24 et 195.139.49.0/24
Sous réseau B : 195.139.50.0/24 et 195.139.51.0/24
Sous réseau C : 195.139.52.0/25
Sous réseau D : 195.139.52.128/25

4. En déduire le taux d'utilisation de la deuxième solution avant de conclure sur l'approche qui sera retenue par l'organisme d'attribution d'adresses

Nombre total d'adresses IP disponibles en = $5 * 256 = 1280$
 $U = 808 / 1280 = 0,63$
La deuxième politique est donc la meilleure.

Exercice 3 : Codage/décodage (5 points)

Vous trouverez dans l'annexe A1, 5 trames consécutives extraites d'une trace Wireshark. En vous aidant de l'annexe A2, répondez aux questions suivantes.

1. Quelle application a généré cet échange ? Justifiez.

Web. On a en N° port la valeur 80, qui est associée à HTTP.

2. Quelle est l'adresse IP (en décimal pointé) du client ? Justifiez que c'est bien celle du client.

192.168.0.48

La trame 1 encapsule un paquet IP dont l'@ src est 192.168.0.48 et ce paquet encapsule un segment TCP SYN dont le N° port src est égal à 0 et donc supérieur à 1024.

3. Quelle est l'adresse IP (en décimal pointé) du serveur ? Justifiez que c'est bien celle du serveur.

132.227.118.100

La trame 1 encapsule un paquet IP dont l'@ dst est 132.227.118.100 et ce paquet encapsule un segment TCP SYN dont le N° port dst est égal à 80 et indiquant que le destinataire est un serveur Web.

4. Combien de routeurs séparent le client du serveur ? Justifiez.

Dans la trame 2, on a un $TTL = 0x\ 31 = 49$. En supposant que TTL avait été initialisé à 64 par le serveur, il y a donc 15 routeurs entre le client et le serveur.

5. A qui appartient l'adresse MAC f4 : ca : e5 : 4f : b8 : 98 ? Justifiez.

C'est l'@ dest de la trame émise par le client. Sachant qu'il y a des routeurs entre le client et le serveur, c'est l'@ MAC de la passerelle du client (i.e. du 1^{er} routeur).

6. A qui appartient l'adresse MAC 8c : 85 : 90 : 7a : 33 : c8 ? Justifiez.

C'est l'@ src de la trame émise par le client. C'est donc l'@ du client.

7. Quel est le numéro initial de séquence (en hexadécimal) du client ?

6c 44 a0 28

8. Quel est le numéro initial de séquence (en hexadécimal) du serveur ?

d4 76 0c 1d

9. Donnez le codage hexadécimal de la 3^{ème} trame (vous mettrez XX comme valeur d'octet pour les champs dont la valeur ne peut pas être déduite).

f4 ca e5 4f b8 98 8c 85 90 7a 33 c8 08 00 45 00
00 28 XX XX X0 00 40 06 XX XX c0 a8 00 30 84 e3
76 64 c0 0e 00 50 6c 44 a0 29 d4 76 0c 1e **50** 10
XX XX XX XX 00 00 00 00 00 00 -- -- -- -- --

XX pour : identificateur IP, flag DF, checksum IP, fenêtre TCP, checksum TCP.

Il faut rajouter 4 octets à 0 pour le bourrage Ethernet (taille min data = 46 octets)

10. La 4^{ème} trame a été tronquée. Le message applicatif est-il une requête ou une réponse ? Justifiez.

C'est une requête HTTP GET : on le lit directement dans la colonne de droite de la trace (celle qui donne les caractères ASCII affichables).

11. Quelle est la longueur de ce message applicatif ? Justifiez.

La requête fait 484 octets.

Dans la trame 4, le client envoie un NumSeq de TCP = 6c 44 a0 29

Dans la trame 5, le serveur envoie un Acknum de TCP = 6c 44 a2 0d. Il a donc reçu :
 $0x a2 0d - 0x a0 29 = 0x 01 e4 = 484$ octets.

Exercice 4 : RIP et Web (5 points)

La figure 1 donnée dans l'annexe A3 représente un réseau local où :

- X et Y sont des machines hôtes ;
- S est un serveur Web et D le serveur DNS local ;
- R0 et R1 sont des routeurs internes au réseau local ;
- G joue le rôle de *gateway* pour les machines du réseau local ;
- Les liens sont des câbles Ethernet.

On suppose que les machines hôtes et les routeurs connaissent leur adresse IP respective qui correspond à celle indiquée sur la figure. Les adresses MAC de X et Y seront notées MX et MY. Pour les routeurs, les adresses MAC de leurs interfaces seront notées en fonction de la machine qu'elles connectent : les adresses MAC de R0 sont MR0X, MR0R1 et MR0G.

1. Donner la valeur du masque **le plus court** qu'il est autorisé de configurer pour X et G.

255.255.255.0

2. Les routeurs R0, R1 et G exécutent le protocole à vecteurs de distance RIP qui utilise l'algorithme de Bellman-Ford. Tous les liens du réseau local ont un coût égal à 1. A t_0 , la table de routage de R0 contient notamment les entrées suivantes :

Destination	Masque	Saut suivant	Distance
9.9.0.0	255.255.0.0	192.168.1.10	20
8.8.7.0	255.255.255.0	192.168.2.10	5
8.8.8.0	255.255.255.0	192.168.2.10	2

A $t_1 > t_0$, R0 reçoit de G le vecteur de distance suivant :

Destination = 9.9.0.0, masque = 255.255.0.0, distance = 14

Destination = 8.8.7.0, masque = 255.255.255.0, distance = 3

Destination = 8.8.8.0, masque = 255.255.255.0, distance = 3

Comment R0 met-il à jour sa table de routage après avoir traité ce vecteur de distance ? Compléter en conséquence la table ci-dessous en indiquant la valeur des cellules vides :

Destination	Masque	Saut suivant	Distance
9.9.0.0	255.255.0.0	192.168.1.10	15
8.8.7.0	255.255.255.0	192.168.2.10	4
8.8.8.0	255.255.255.0	192.168.2.10	4

3. La machine X exécute la commande suivante :

ping -c 1 192.168.15.10

Un analyseur de réseau observe le trafic traversant le lien R0-R1 (point d'observation noté '1' sur la figure 1). Compléter le tableau suivant en indiquant l'ensemble des trames observées nécessaires afin de réaliser cette opération. Préciser pour chaque trame, les informations pertinentes selon les données qu'elles encapsulent. On supposera qu'aucune trame n'est perdue, dupliquée ou reçue en erreur. Les caches de la machine X seront supposés vides. (Indication : certaines trames n'encapsulent pas de paquet IP.)

Trame Ethernet			Paquet IP			
Adresse MAC Source	Adresse MAC Destination	Type	Adresse IP Source	Adresse IP Destination	Protocole	TTL
MR0R1	FF:FF:....:FF	0x0806	--	--	--	--
MR1R0	MR0R1	0x0806	--	--	--	--
MR0R1	MR1R0	0x0800	192.168.3.10	192.168.15.10	0x01	63
MR1R0	MR0R1	0x0800	192.168.15.10	192.168.3.10	0x01	63

4. Par la suite, la machine X souhaite télécharger une page html hébergée par S. Un analyseur de réseau observe le trafic traversant le lien R0-G (point d'observation noté '2' sur la figure 1). Compléter le tableau ci-dessous en donnant la séquence des trames observées avant que le navigateur web de X puisse afficher la page html. Vous indiquerez uniquement les trames qui diffèrent entre elles en raison d'au moins un des champs listés dans le tableau. On suppose que X connaît déjà l'adresse IP de S. La table de routage de G n'a pas changée depuis l'envoi du vecteur de distance donné dans la question 2).

Trame Ethernet			Paquet IP			
Adresse MAC Source	Adresse MAC Destination	Type	Adresse IP Source	Adresse IP Destination	Protocole	TTL
MR0G	FF:FF:....:FF	0x0806	--	--	--	--
MGR0	MR0G	0x0806	--	--	--	--
MR0G	MGR0	0x0800	192.168.3.10	9.9.9.99	0x06	64
MGR0	MR0G	0x0800	9.9.9.99	192.168.3.10	0x06	49

5. Certaines entrées du tableau précédent contiennent des informations présentes dans plusieurs trames. Indiquer quelles sont ces entrées et pour chacune d'elles, donner le nombre de trames qui partagent les mêmes informations telles que listées par cette entrée. Expliquer la raison de chaque trame. On supposera qu'aucun des paquets IP n'est fragmenté, dupliqué, déséquenté, perdu ou reçu en erreur. La page html complète tient dans un seul paquet IP.

192.168.3.10 > 9.9.9.99 : 4 (+2) TCP SYN, TCP ACK, TCP data (HTTP GET) (TCP FIN, TCP ACK), TCP ACK
 192.168.3.10 < 9.9.9.99 : 3 (+2) TCP SYN ACK, TCP ACK, TCP data (HTTP 200 OK) (TCP ACK, TCP FIN)

Supposons à présent le réseau présenté dans la figure 2 donnée dans l'annexe A3 : X, R1 et G sont connectés au même réseau Ethernet.

6. Donner le masque **le plus long** qu'il est autorisé de configurer pour X et G.

255.255.252.0

7. La machine X exécute à nouveau la commande suivante :

```
ping -c 1 192.168.15.10
```

Un analyseur de réseau observe le trafic qui traverse le point d'observation noté '1' dans la figure 2 de l'annexe A3. Compléter le tableau suivant en indiquant l'ensemble des trames observées nécessaires afin de réaliser cette opération. Préciser pour chaque trame les informations pertinentes selon le type des données qu'elle encapsule. Les caches de la machine X seront supposés vides avant l'exécution du *ping*. (Indication : certaines trames n'encapsulent pas de paquet IP.)

Trame Ethernet			Paquet IP			
Adresse MAC Source	Adresse MAC Destination	Type	Adresse IP Source	Adresse IP Destination	Protocole	TTL
MX	FF:FF:....:FF	0x0806	--	--	--	--
MR1X	MX	0x0806	--	--	--	--
MX	MR1X	0x0800	192.168.3.10	192.168.15.10	0x01	64
MR1X	MX	0x0800	192.168.15.10	192.168.3.10	0x01	63

8. Supposons à présent que X est configuré par erreur avec le masque 255.255.0.0.

```
ping -c 1 192.168.15.10
```

Quelle(s) trame(s) voit passer l'analyseur de réseau positionné au niveau du point d'observation noté '1' dans la figure 2 de l'annexe. Si une trame est dupliquée, remplissez une seule entrée pour cette trame.

Trame Ethernet			Paquet IP			
Adresse MAC Source	Adresse MAC Destination	Type	Adresse IP Source	Adresse IP Destination	Protocole	TTL
MX	FF:FF:....:FF	0x0806	--	--	--	--

Si une ou plusieurs des entrées du tableau précédent contiennent des informations présentes dans plusieurs trames, indiquer quelle(s) entrée(s) et pour chacune, combien de trames contiennent les mêmes informations telles que listées par cette entrée. Expliquer pourquoi.

Un seul ICMP ECHO REQUEST donc une seule requête ARP après laquelle ARP abandonne.

Annexe A1

Trame 1

0000	f4 ca e5 4f b8 98 8c 85 90 7a 33 c8 08 00 45 00	...O.....z3...E.
0010	00 40 0a 0b 40 00 40 06 7e 98 c0 a8 00 30 84 e3	.@...@.@.~....0..
0020	76 64 c0 0e 00 50 6c 44 a0 28 00 00 00 00 b0 02	vd...PlD.(.....
0030	ff ff e8 fa 00 00 02 04 05 b4 01 03 03 06 01 01
0040	08 0a 09 d5 ba 80 00 00 00 00 04 02 00 00

Trame 2

0000	8c 85 90 7a 33 c8 f4 ca e5 4f b8 98 08 00 45 00	...z3....O....E.
0010	00 34 12 00 40 00 31 06 8d a4 84 e3 76 64 c0 a8	.4..@.1.....vd..
0020	00 30 00 50 c0 0e d4 76 0c 1d 6c 44 a0 29 80 12	.0.P...v..lD.)..
0030	16 d0 ee 70 00 00 02 04 05 b4 01 01 04 02 01 03	...p.....
0040	03 07	..

Trame 3

0000	-- -- -- -- -- -- -- -- -- -- -- -- -- -- --	-----
0010	-- -- -- -- -- -- -- -- -- -- -- -- -- -- --	-----
0020	-- -- -- -- -- -- -- -- -- -- -- -- -- -- 5 --	-----
0030	-- -- -- -- -- -- -- -- -- -- -- -- -- -- --	-----

Trame 4

0000	f4 ca e5 4f b8 98 8c 85 90 7a 33 c8 08 00 45 02	...O.....z3...E.
0010	02 0c 0a 0d 40 00 40 06 7c ca c0 a8 00 30 84 e3@.@.0..
0020	76 64 c0 0e 00 50 6c 44 a0 29 d4 76 0c 1e 50 18	vd...PlD.) .v..P.
0030	10 00 ef bf 00 00 47 45 54 20 2f 6c 6d 64 2f 6cGET /lmd/l
0040	69 63 65 6e 63 65 2f 2f 70 75 62 6c 69 63 2f 69	icence//public/i
0050	6e 64 65 78 2e 70 68 70 20 48 54 54 50 2f 31 2e	ndex.php HTTP/1.
0060	31 0d 0a 48 6f 73 74 3a 20 77 77 77 2d 6c 69 63	1..Host: www-lic
0070	65 6e 63 65 2e 75 66 72 2d 69 6e 66 6f 2d 70 36	ence.ufr-info-p6
0080	2e 6a 75 73 73 69 65 75 2e 66 72 0d 0a 43 6f 6e	.jussieu.fr..Con
0090	6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c	nection: keep-al

.....

Trame 5

0000	8c 85 90 7a 33 c8 f4 ca e5 4f b8 98 08 00 45 00	...z3....O....E.
0010	00 28 ba 7c 40 00 31 06 d3 33 84 e3 76 64 c0 a8	.(. @.1..3..vd..
0020	00 30 00 50 c0 0e d4 76 0c 1e 6c 44 a2 0d 50 10	.0.P...v..lD..P.
0030	00 36 44 39 00 00 00 00 00 00	.6D9.....

Annexe A2

Structure d'une trame Ethernet

```
.64bits--+48bits--+48bits--+16b--+ - - - +32b--.
.(Préam)| adresse | adresse |type| données |(CRC)|.
.      | dest.   | source  |   |   |   |   |
.-----+-----+-----+-----+ - - - +-----.
```

Quelques types : 0x0800 = DoD Internet (IP)
0x0806 = ARP
0x8035 = RARP

Structure d'un paquet ARP

```
<-----32bits----->
<--8bits--><--8bits--><-----16bits----->
+-----+-----+-----+-----+
| Hardware | Protocol |
+-----+-----+-----+-----+
| Hlen     | Plen     | Operation |
+-----+-----+-----+-----+
| Sender HA (bytes 0-3) |
+-----+-----+-----+-----+
| Sender HA (bytes 4-5) | Sender IA (bytes 0-1) |
+-----+-----+-----+-----+
| Sender IA (bytes 2-3) | Sender HA (bytes 0-1) |
+-----+-----+-----+-----+
| Target HA (bytes 2-5) |
+-----+-----+-----+-----+
| Target IA (bytes 0-3) |
+-----+-----+-----+-----+
```

Hardware = type d'interface physique

ex : 0x0001 pour Ethernet

Protocol = type de protocole pour lequel une requête a été émise

ex : 0x0800 pour IP

Hlen = lg de l'adresse physique (en octets)

Plen = lg de l'adresse protocolaire (en octets)

Operation = type d'opération à effectuer par le récepteur

ex : 0x0001 pour une requête ARP

0x0002 pour une réponse ARP

Sender HA = adresse physique (Ethernet) de l'émetteur

Sender IA = adresse protocolaire (IP) de l'émetteur

Target HA = adresse physique (Ethernet) du récepteur

Target IA = adresse protocolaire (IP) du récepteur

Structure d'un paquet IP

```
<-----32bits----->
<4b--><4b--><--8bits--><-----16bits----->
+-----+-----+-----+-----+
| Ver | IHL | TOS |Lg. totale (en octets)|
+-----+-----+-----+-----+
| Identificateur |Fl| FO |
+-----+-----+-----+-----+
| TTL | Protocole | Checksum(en-tête) |
+-----+-----+-----+-----+
| Adresse Source |
+-----+-----+-----+-----+
| Adresse Destination |
+-----+-----+-----+-----+
... Options ...
+-----+-----+-----+-----+
... Données ...
+-----+-----+-----+-----+
```

Ver = Version d'IP

IHL = Longueur de l'en-tête IP (en mots de 4 octets)

TOS = Type de service (zéro généralement)

Fl (3 premiers bits) = Bits pour la fragmentation

* 1er = réservé

* 2ème = DF (Ne pas fragmenter)

* 3ème = MF (Fragment suivant existe)

FO (13 bits suivants) = Position relative du fragment

dans le datagramme initial (déplacement exprimé en

mots de 8 octets (seuls un datagramme complet ou un

premier fragment peuvent avoir ce champ à 0)

TTL = Durée de vie restante

Protocole = protocole transporté

ex : 1 = ICMP

2 = IGMP

6 = TCP

8 = EGP

11 = GLOUPS

17 = UDP

89 = OSPF

Structure d'un message UDP

```
<-----32bits----->
+-----+-----+-----+-----+
| Port Source | Port Destination |
+-----+-----+-----+-----+
| Longueur | Checksum (msg) |
+-----+-----+-----+-----+
... Données ...
+-----+-----+-----+-----+
```

Structure d'un segment TCP

```
<-----32bits----->
<4b--> <-6bits--><-----16bits----->
+-----+-----+-----+-----+
| Port Source | Port Destination |
+-----+-----+-----+-----+
| Numéro de Séquence |
+-----+-----+-----+-----+
| Numéro d'Acquittement |
+-----+-----+-----+-----+
| THL | | Flags | Taille Fenêtre |
+-----+-----+-----+-----+
| Checksum (msg) | Pointeur d'urgence |
+-----+-----+-----+-----+
... Options ...
+-----+-----+-----+-----+
... Données ...
+-----+-----+-----+-----+
```

THL = Longueur de l'entête TCP sur 4 bits (en mots de 4 octets)

Flags = indicateur codé sur 6 bits, de gauche à droite

- * 1er = URG (Données urgentes)
- * 2ème = ACK (Acquittement)
- * 3ème = PSH (Données immédiates)
- * 4ème = RST (Réinitialisation)
- * 5ème = SYN (Synchronisation)
- * 6ème = FIN

Options = suite d'options codées sur

* un seul octet :

00 = Fin des options

01 = NOP (pas d'opération)

* plusieurs octets, avec un codage TLV

T = un octet pour le type de l'option

2 Négociation de la taille max. du segment

3 Adaptation de la taille de la fenêtre

4 Autorisation des acquittements sélectifs

8 Estampilles temporelles

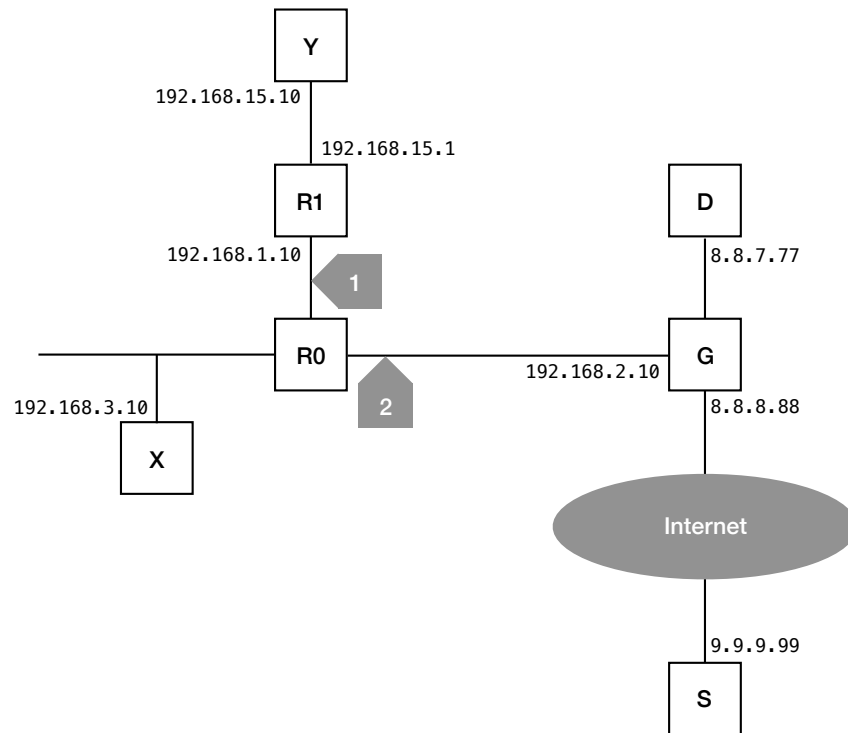
L = un octet pour la taille totale de l'option

V = valeur de l'option (sur L-2 octets)

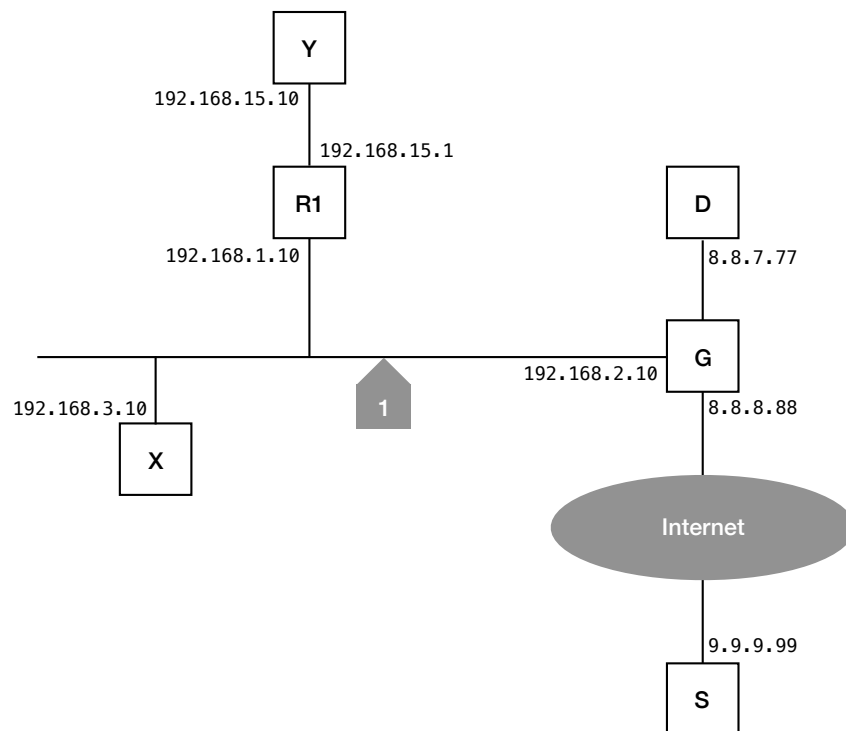
Services associés aux ports

ftp-data	20/tcp
ftp	21/tcp
ssh	22/tcp
telnet	23/tcp
smtp	25/tcp
dns	53/udp
www	80/tcp
pop-3	110/tcp
imap	143/tcp
bgp	179/tcp
snmp	161/udp
...	

Annexe A3



- Figure 1 (exercice 4) -



- Figure 2 (exercice 4) -