

Exercices dirigés

UTC505/USRS4D

-IP-

E. Gressier-Soudan

2021-2022

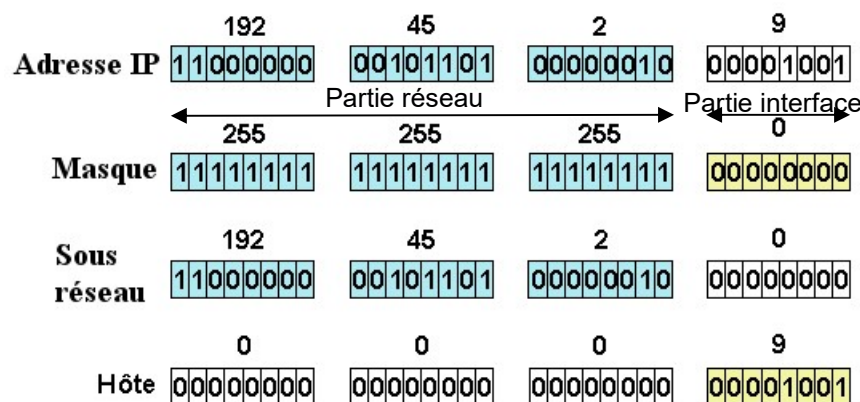
Ce polycopié a été élaboré par l'équipe enseignante "Réseaux et protocoles" à partir d'exercices rédigés par MM. Florin, Gressier-Soudan qu'ils en soient ici remerciés.

ED•Adressage IP & Forwarding Adresses, réseau et sous-réseau, tables de routage

L'objectif de ce chapitre d'exercices est de faire manipuler les adresses IP, les masques, en binaire, en hexadécimal, et en décimal pour pouvoir passer de l'un à l'autre aisément.

Son deuxième objectif est de comprendre le processus de traversée d'un routeur.

Les concepts à comprendre sont l'adresse IP (ici IPv4 mais c'est extensible à IPv6) et le masque. Le masque délimite la partie adresse de réseau¹ de la partie numéro d'interface. C'est très clair quand on manipule les bits d'une adresse et les bits d'un masque. Le tout est résumé dans la figure ci-dessous avec un masque de longueur 24 bits :



source https://sti2d.ecolelamache.org/v_le_masque_de_sous_rseau.html (21/05/2021)

L'adresse IP désigne un coupleur de communication au niveau de la couche de communication réseau (3 dans les modèles OSI et Internet) IP, et l'adresse de réseau désigne un ensemble d'interfaces. L'adresse IP d'interface est utilisée pour désigner une destination à atteindre particulière. L'adresse de réseau est utilisée dans les routeurs pour qu'un datagramme IP envoyé vers une destination puisse atteindre cette destination.

¹ Ici réseau est à prendre au sens large. La partie réseau peut parfois être découpée ou redécoupée en réseau puis sous-réseau(x).

L'opération "masque" sur les adresses correspond à un ET logique appliqué donc bit par bit suivant la longueur du masque sur une adresse de réseaux IPv4 ou IPv6.

Rappels sur l'univers binaires :

Puissance de 2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Valeur décimale	128	64	32	16	8	4	2	1
Somme des colonnes de gauche à droite	128	192	224	240	248	252	254	255

Table des valeurs des groupements de chiffres binaires

Binaire	Décimal	Octal	Hexadécimal	Binaire	Décimal	Octal	Hexadécimal
0000	0	0	0	1000	8	10	8
0001	1	1	1	1001	9	11	9
0010	2	2	2	1010	10	12	A
0011	3	3	3	1011	11	13	B
0100	4	4	4	1100	12	14	C
0101	5	5	5	1101	13	15	D
0110	6	6	6	1110	14	16	E
0111	7	7	7	1111	15	17	F

source : https://fr.wikipedia.org/wiki/Syst%C3%A8me_binaire (24/04/2021)

Here is the bitwise equivalent operations of two bits P and Q:

p	q	F^0	NOR^1	Xq^2	$\neg p^3$	\rightarrow^4	$\neg q^5$	XOR^6	$NAND^7$	AND^8	$XNOR^9$	q^{10}	If/then ¹¹	p^{12}	Then/if ¹³	OR^{14}	T^{15}
1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
1	0	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
0	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
0	0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
Bitwise equivalents		0	NOT (p OR q)	(NOT p) AND q	NOT p	p AND (NOT q)	NOT q	p XOR q	NOT (p AND q)	p AND q	NOT (p XOR q)	q	(NOT p) OR q	p	p OR (NOT q)	p OR q	1

source : https://en.wikipedia.org/wiki/Bitwise_operation (24/04/2021)

Exemple :

```

00001010
ET (logique)
11111111
=
00001010

```

Plus si cela vous intéresse [ici](#) (origine Masque de réseau et sous-réseaux par le LYCEE CFA-CFC JEANNE D'ARC, consulté le 15/03/2020).

Cours et exercices sur les conversions en binaire, hexadécimal et décimal (consultés le 13/10/2019) :

<https://www.apprendre-en-ligne.net/info/codage/codage.pdf>

http://www.scientillula.net/MPI/fex6_conversions/fex6_conversions.html

<https://lipn.univ-paris13.fr/~manzonetto/~M1101/M1101-td-01-correction.pdf>

Mise en perspective du Masque, de l'adresse IPv4 (de longueur 32 bits), et de l'adresse de réseau:

Soit une adresse IPv4 : 10.168.0.0, en fonction de la valeur du masque, essayons de déterminer sa nature.

1. Hypothèse : le masque du réseau auquel 10.168.0.0 appartient vaut /18

Effectuons "10.168.0.0" ETlogique "/18".

Le masque /18 est la notation compacte de 11111111.11111111.11 000000.00000000 et exprimé en décimal c'est : 255.255.192.0.

"10.168.0.0" ETlogique "/18" = 10.168.0.0 ETlogique 11111111.11111111.11 000000.00000000

Un octet tout à 1 appliqué à un nombre sur un octet, ne change rien au nombre (ET équivalent à la multiplication et 1 est neutre pour la multiplication).

Un octet tout à 0 appliqué à un nombre sur un octet, le transforme en 0 (ET équivalent à la multiplication et 0 est absorbant pour la multiplication)

Donc on peut calculer partiellement rapidement : "10.168.0.0" ETlogique "/18" = 10.168.qqch.0 ! Il reste à trouver ce qqch. En fait c'est simple car dans l'adresse l'octet correspondant au 3^{ème} octet du masque vaut 0. On a donc ce qqch qui vaut 0.

D'où "10.168.0.0" ETlogique "/18" = 10.168.0.0

Par la suite, on notera "10.168.0.0" ETlogique "/18" par 10.168.0.0/18

Définition : Une adresse IP est une adresse de réseau (et pas d'interface ou d'host) si la partie qui correspond au numéro d'interface est à 0.

Des calculs ci-dessus, peut-on déduire que 10.168.0.0 est une adresse de réseau ou de host ?

Comme 10.168.0.0/18 = 10.168.0.0, on en conclut que 10.168.0.0 est une adresse de réseau. En effet :

10.168.0.0/18 => 10.10101000.00000000.0/18 => 10.10101000.00 000000.0 = 10.168.0.0

2. Hypothèse : le masque auquel 10.168.0.0 appartient vaut maintenant /10, est-ce que 10.168.0.0 est une adresse de réseau ou de host ?

10.168.0.0/10 => 10.10101000.00000000.0/10 => 10.10 000000.00000000.0 = 10.128.0.0 est différent de 10.168.0.0 donc 10.168.0.0 n'est pas une adresse de réseau quand le masque est /10

Le concept à maîtriser ensuite correspond à l'adresse de diffusion associée à un réseau, adresse IPv4 bien sûr dans notre contexte. Là encore, il faut se servir du masque du réseau. On détecte la partie réservée à numéroté les interfaces dans l'adresse IP d'un réseau, grâce au masque, puis on met que des 1 dans cette zone.

3. On cherche l'adresse de diffusion limitée au réseau, ou encore appelée broadcast, de 10.128.0.0/10 ?

10.128.0.0 s'écrit 10.10 000000.00000000.00000000 sachant que le masque est 11111111.11 000000.00000000.00000000

adresse de réseau : 10 .10 000000.00000000.00000000

masque : 11111111.11 000000.00000000.00000000

broadcast : 10 .10 111111.11111111.11111111

broadcast décimal : 10 . 191 . 255 . 255 (128+63=191)



Exercice 1 : Calcul d'adresses IPv4.

Question 1 :

Sur Internet, on trouve des outils pour calculer des adresses, l'un de ceux-ci donne pour résultat si on lui fournit l'adresse d'interface 10.168.0.1 et le masque /20:

```
Address: 10.168.0.1          00001010.10100100.0000 0000.00000001
Netmask: 255.255.240.0 = 20  11111111.11111111.1101 0000.00000000
=>
Network: 10.168.0.0/20      00001010.10101000.0000 0000.00000000
Broadcast: 10.168.15.255    00001010.10101000.0000 1111.11111111
HostMin: 10.168.0.1         00001010.10101000.0000 0000.00000001
HostMax: 10.168.15.254      00001010.10101000.0000 1111.11111110
Hosts/Net: 4094              (Private Internet)
```

Est-ce que le résultat est correct ou contient-il une ou plusieurs erreurs ? Justifiez votre réponse.

Question 2 :

L'outil peut aussi proposer un calcul si on veut découper son réseau en sous réseaux. Si on indique un masque /21 voila les propositions qu'il fait pour 2 sous-réseaux :

```
Netmask: 255.255.248.0 = 21  11111111.11111111.11011 000.00000000

Network: 10.168.0.0/21      00001010.10101000.00000 000.00000000
Broadcast: 10.168.7.255    00001010.10101000.00000 111.11111111
HostMin: 10.168.0.1        00001010.10101000.00000 000.00000001
HostMax: 10.168.7.254      00001010.10101000.00000 111.11111110
Hosts/Net: 2046             (Private Internet)

Network: 10.168.8.0/21      00001010.10101000.00001 000.00000000
Broadcast: 10.168.15.255    00001010.10101000.00001 111.11111111
HostMin: 10.168.8.1         00001010.10101000.00001 000.00000001
HostMax: 10.168.15.254      00001010.10101000.00001 111.11111110
Hosts/Net: 2046             (Private Internet)

Subnets: 2, Hosts: 4092
```

Est-ce que le résultat est correct ou contient-il une ou plusieurs erreurs ? Pourquoi lorsqu'on passe à deux sous-réseaux on perd deux hosts ? Justifiez votre réponse.

Question 3 :

L'outil peut aussi fournir des réponses quand on propose de rechercher une adresse englobante, "supernet". Si on propose un masque /18 on obtient la réponse suivante :

```
Netmask: 255.255.192.0 = 18  11111111.11111111.11 000000.00000000

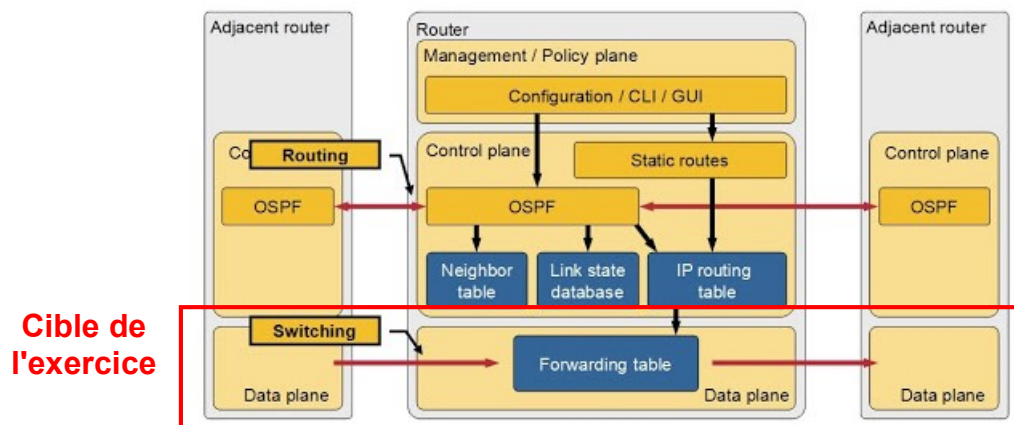
Network: 10.168.0.0/18      00001010.10101000.00 000000.00000000
Broadcast: 10.168.63.255    00001010.10101000.00 111111.11111111
HostMin: 10.168.0.1         00001010.10101000.00 000000.00000001
HostMax: 10.168.63.254      00001010.10101000.00 111111.11111110
Hosts/Net: 16382            (Private Internet)
```


Pourquoi peut-on disposer de 16382 hosts maintenant ? Justifiez votre réponse.

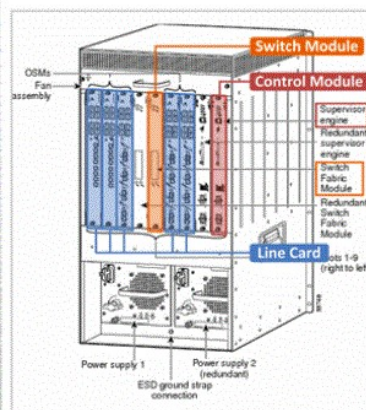
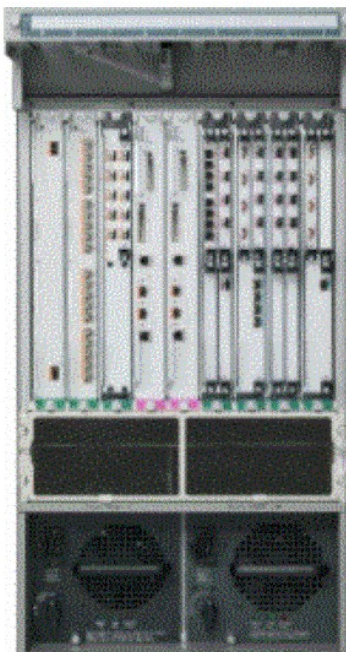
Exercice 2 : Principe du "forwarding" dans un routeur IP

Pour introduire l'exercice, il faut s'imaginer l'organisation d'un routeur. La figure ci-après aide à se représenter les fonctions mise en œuvre dans cet équipement.

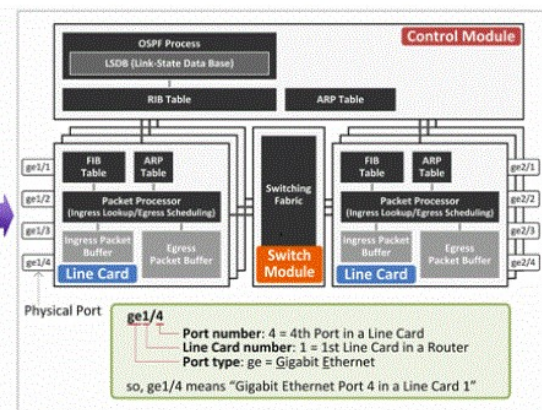
Management, Control and Data Planes



source : <https://blog.ipspace.net/2013/08/management-control-and-data-planes-in.html> (consultée le 29/10/2020)



Cisco 7600 Router

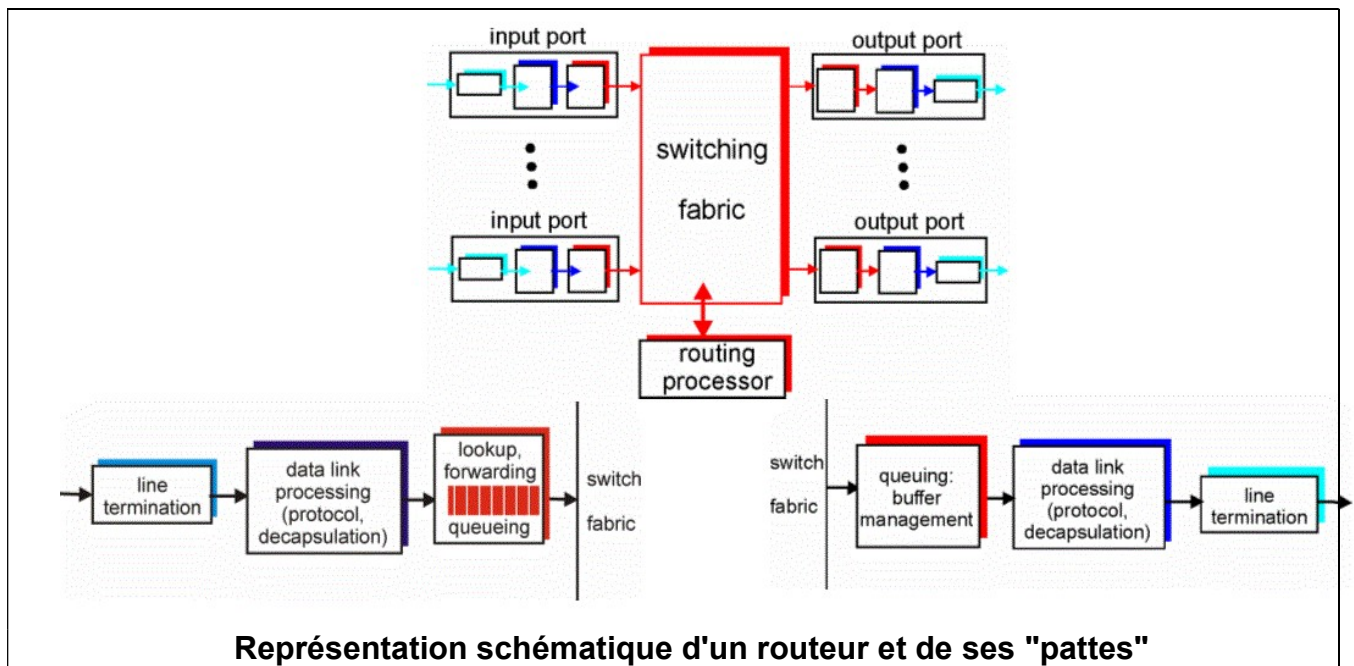


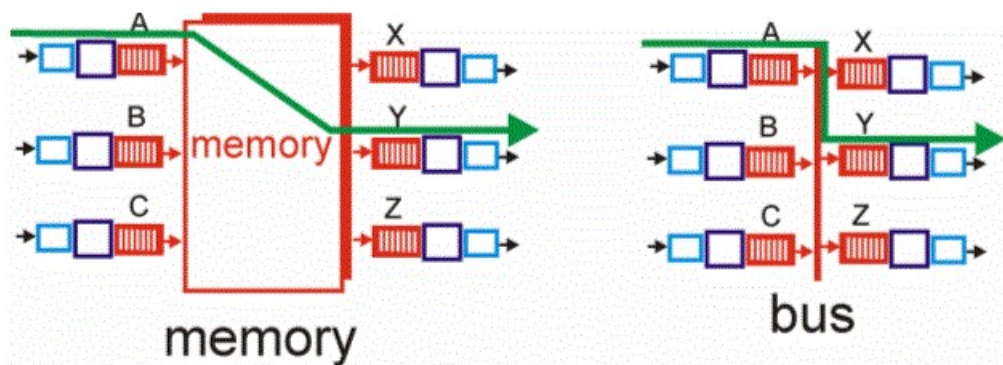
General Router Architecture

Source : <https://www.netmanias.com/en/post/blog/6338/ip-routing-network-protocol-switching/switching-and-routing-part-1-router-architecture> (29/04/2021)

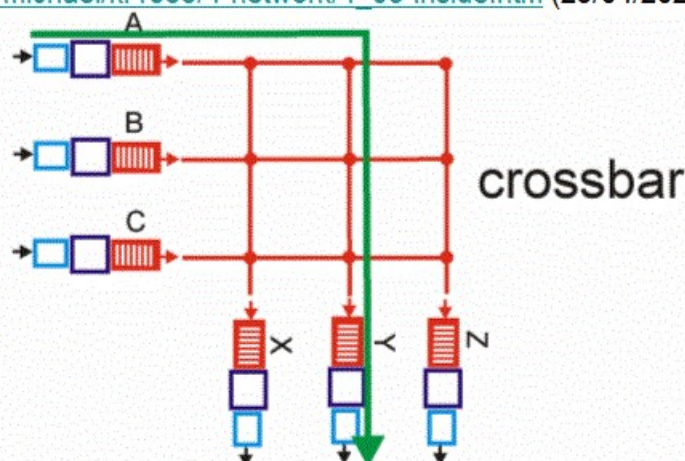
Source : https://www.cisco.com/c/fr_ca/support/routers/7600-series-routers/series.html (29/04/2021)

Mise en correspondance des vues logique et physique d'un routeur et de son organisation interne





Source : http://www2.ic.uff.br/~michael/kr1999/4-network/4_06-inside.htm (29/04/2021)



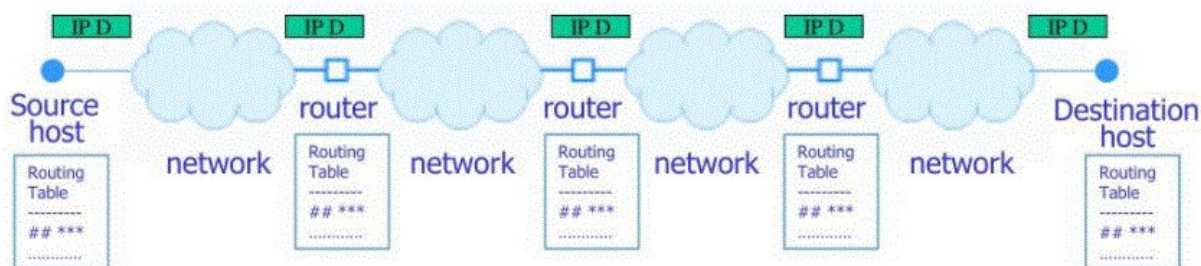
Différentes mises en œuvre de la partie commutation

Complément :

La nouvelle vision de l'architecture introduit 3 plans : Management Plane, Control Plane et Data Plane. Le management plane s'occupe essentiellement de configuration et des informations liées à l'administration à distance, c'est le dernier plan qui s'est formalisé. Le control plane est plus ancien et c'est là qu'on trouve toute l'intelligence du routeur : calcul des routes, génération des tables de routages, tables de gestion de la QoS, tables de gestion des groupes multicast... Le plan forwarding est aussi appelé plan de données ou Data Plane existe depuis toujours.

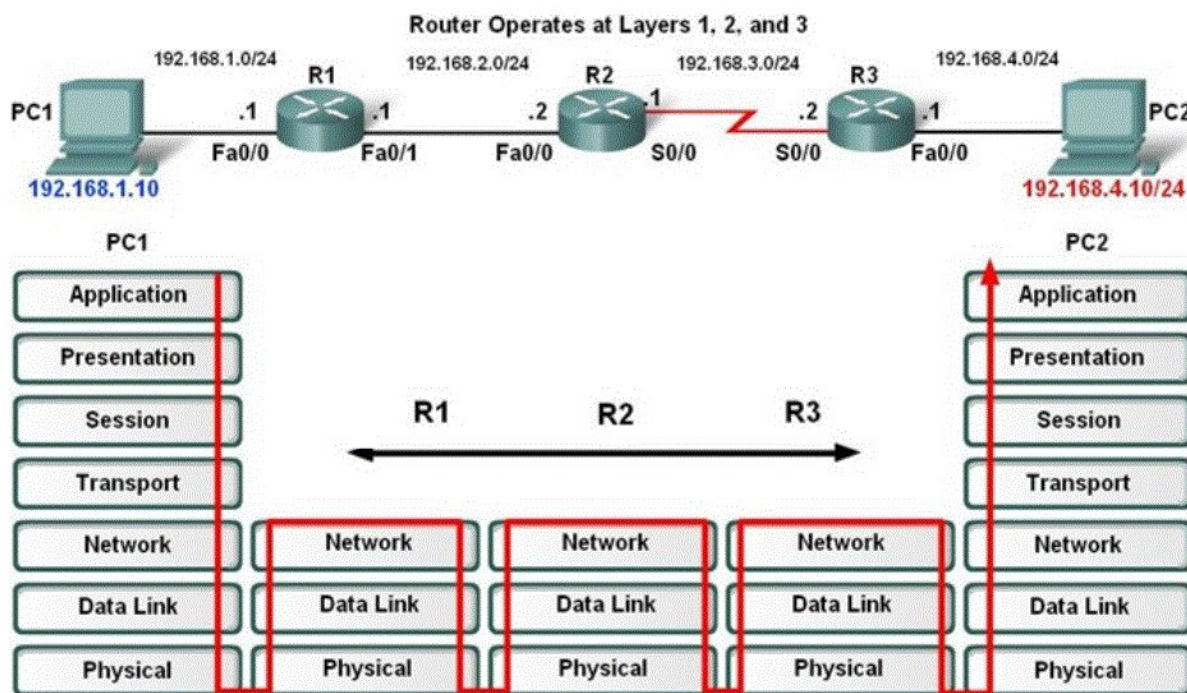
Cette nouvelle terminologie correspond à l'émergence de nouvelles technologies en relation avec l'approche SDN, Software Defined Network qui offre une vision logicielle des technologies réseaux et qui correspond à une démarche de virtualisation des équipements réseaux à l'instar de la virtualisation de l'exécution avec les machines virtuelles (VM pour Virtual Machine en anglais).

L'équipement routeur a pour rôle de diriger un datagramme (l'unité de message gérée par la couche IP) d'une voie d'entrée vers une voie de sortie qui le rapproche de sa destination. Au niveau macroscopique cela donne :



source : <https://line.17qq.com/articles/snqnnpnwwy.html> (22/04/2021)

Le schéma ci-après représente le chemin de traversée des couches en relation avec le modèle ISO d'une succession de routeurs :



source : <https://slideplayer.fr/slide/4259942/> (22/04/2021)

Et parcourir le chemin d'un point à un autre de l'Internet en traversant une succession de routeur se fait à l'aide des tables de routage.

Dans un routeur IP la table de routage comporte pour chaque entrée (ligne) une "route". On trouve dans l'exemple de la table suivante:

- un numéro d'entrée pour se repérer facilement,
- l'adresse IP d'un réseau de destination,
- le masque associé à cette adresse réseau de destination (en notation /n),
- l'adresse IP du prochain routeur ou du prochain hôte à visiter sur la route,
- le coût (la métrique),
- l'interface de sortie coupleur/carte réseau qui va donner la liaison à emprunter.

D'autres informations sont prévues dans les tables de routage IP mais n'apparaissent pas dans l'exemple de l'exercice, comme par exemple l'adresse du port à utiliser en sortie ou le type de la route pour définir si le datagramme IP doit atteindre une destination distante ou s'il est à délivrer à sa destination directement par le présent routeur. Ici, toutes

les destinations à atteindre sont distantes.

N°	Réseau Destination	Masque du réseau Dest	Prochain Routeur	Métrique	Interface associée
1	0.0.0.0	/0	10.1.3.65	1	eth1
2	10.1.0.0	/16	10.1.3.65	1	eth1
3	10.1.3.0	/24	10.1.3.1	0	eth1
4	10.1.3.64	/26	10.1.3.126	0	eth0
5	10.1.3.128	/26	10.1.3.190	0	eth0
6	10.1.3.192	/26	10.1.3.254	0	eth0
7	10.1.4.0	/24	10.1.3.4	11	eth1
8	10.1.4.64	/26	10.1.3.4	9	eth1
9	10.1.4.128	/26	10.1.3.4	10	eth1
10	10.1.16.64	/26	10.1.3.65	5	eth1
11	10.1.8.0	/24	10.1.3.65	6	eth1
12	10.1.8.0	/26	10.1.3.65	9	wlan0
13	10.1.8.64	/26	10.1.3.65	17	ppp2
14	10.1.8.64	/26	10.1.3.62	22	ppp0
15	10.1.8.128	/26	10.1.3.65	25	ppp1

Question 1

Une fois extraite l'adresse IP de destination du datagramme, on va chercher quel est le réseau de destination le plus approprié connu par le routeur. Chaque réseau de destination potentiel correspond à une ligne de la table de routage. Chaque ligne pour identifier un réseau de destination contient l'adresse de réseau et le masque associé.

Pour établir une correspondance entre le réseau mentionné sur une ligne de la table de routage et l'adresse IP de destination contenue dans le datagramme, on applique le masque à l'adresse de destination.

- Si le résultat de l'application du masque à l'adresse IP de destination correspond à l'adresse du réseau dans la ligne de la table de routage, on garde la ligne. On dit que la ligne est candidate à la propagation du datagramme. On dit aussi ligne candidate à l'acheminement du datagramme vers le prochain routeur
- Si le résultat ne correspond pas, la ligne est tout simplement éliminée.

On fait ce calcul de masque pour toutes les lignes dans la table de routage. A la fin de cette phase il reste, normalement une ou plusieurs lignes candidates. S'il n'y en a pas, on se trouve en présence d'une erreur de routage, le datagramme est éliminé et le routeur prévient la source (via l'@IP source contenue dans le datagramme) comme quoi la destination n'est pas atteignable (HOST UNREACHABLE).

On comprend la nécessité d'avoir une table de routage la moins longue possible car le temps pour déterminer une interface de sortie est proportionnel à son nombre d'entrées. Les routeurs peuvent bénéficier d'optimisations hardware qui permettent de traiter plusieurs entrées de la table de routage en même temps, par exemple avec



l'utilisation de mémoires associatives.

Application à la destination **10.1.8.66**. Quelles sont les routes qui passent positivement ce test ?

Question 2

Lorsque l'on a opéré ce premier élagage on réalise un second élagage conduisant à choisir les routes qui sont associées aux masques les plus longs.

Pourquoi les routeurs doivent-ils réaliser une recherche de "correspondance la plus longue" ('Longest Match based **forwarding** algorithm') ?

Donner le numéro des entrées qui passent ce second filtrage.

Question 3

Les routeurs peuvent ensuite arbitrer entre différentes routes selon un routage de la pomme de terre chaude. Dans le paquet IP il existe dans l'entête une zone dédiée à la qualité de service du paquet (TOS 'type of service'), qui contient deux informations.

Rappelez la signification de ces deux informations de qualité de service.

Que peut faire un routeur pour utiliser cette zone et filtrer entre les différentes routes encore jugées équivalentes?

Question 4

Un quatrième filtrage peut utiliser la métrique.

Rappeler la signification de cette valeur.

Comment utiliser cette entrée dans la table de routage pour filtrer entre les différentes routes qui seraient encore jugées équivalentes ?

Question 5

Un cinquième filtrage peut mettre en avant des techniques propres à chaque fabricant de routeur.

Quelle optimisation plus globale au réseau peut-on encore réaliser si l'on a encore plusieurs routes jugées équivalentes ?

Question 6

S'il n'existe plus lors de l'une des étapes précédentes de route possible pour atteindre le destinataire, que se passe t'il ?

Exercice 3 : Routage IP sur un hôte

On vous donne l'extrait du résultat de la commande `ipconfig` sur une machine quelconque.

```
Carte Ethernet Connexion au réseau local filaire eth0 :
  Suffixe DNS propre à la connexion. . . : cnam.fr
  Adresse IPv4. . . . . : 163.173.231.107
  Masque de sous-réseau. . . . . : 255.255.255.0
  Passerelle par défaut. . . . . : 163.173.231.2
```

```
Carte réseau sans fil Connexion réseau sans fil wif0 :
  Suffixe DNS propre à la connexion. . . : cnam.fr
  Adresse IPv4. . . . . : 163.173.112.23
  Masque de sous-réseau. . . . . : 255.255.255.0
  Passerelle par défaut. . . . . : 163.173.112.2
```

On en déduit que la machine possède 2 interfaces.

Question 1

Paramètres de configuration

- Donner la notation compacte pour le masque (/n)
- Donner l'adresse de réseau IP associée correspondant à chacune des interfaces
- Donner l'adresse IP du routeur associé pour chacun des réseaux IP auxquels ces interfaces appartiennent.
- Donner l'adresse de diffusion associée à chacun des réseaux IP apparaissant dans les résultats ci-dessus

Suite du problème. En fait, le réseau IP a été mal paramétré, on conçoit un nouveau plan d'adressage.

Sur la machine, on veut envoyer le datagramme IP d'adresse de destination 163.173.228.26.

Question 2

Quand elle met en fonctionnement que sa carte Ethernet on a la table de routage locale suivante active:

	Réseau/mask	Next hop	métrique	accessibilité	interface
L1	0.0.0.0/0	163.173.231.2	10	distant	eth0
L2	127.0.0.0/8	0.0.0.0	0	direct	lo0
L3	163.173.228.0/24	0.0.0.0	0	direct	eth0

Quelle ligne de la table de routage emprunte le datagramme d'adresse IP destination 163.173.228.26 pour sortir du routeur et atteindre cette destination ? Estimer combien de routeurs au minimum sont traversés et pourquoi ? Expliquez brièvement votre réponse.

Question 3

Quand la station E ne met en fonctionnement que sa carte Wifi, on a la table de routage locale suivante active :

	Réseau/mask	Next hop	métrique	accessibilité	Interface
L1	0.0.0.0/0	163.173.112.2	10	distant	wif0
L2	127.0.0.0/8	0.0.0.0	0	direct	lo0
L3	163.173.112.0/24	0.0.0.0	0	direct	wif0

Quelle ligne de la table de routage emprunte le datagramme d'adresse IP destination 163.173.228.26 pour sortir du routeur et atteindre cette destination ? Estimer combien de routeurs au minimum sont traversés et pourquoi ? Expliquez brièvement votre réponse.

Question 4

La station E active son interface Wifi. On effectue la commande tracer et on obtient le résultat suivant :

Détermination de l'itinéraire vers 163.173.228.26 avec un maximum de 30 sauts :

```

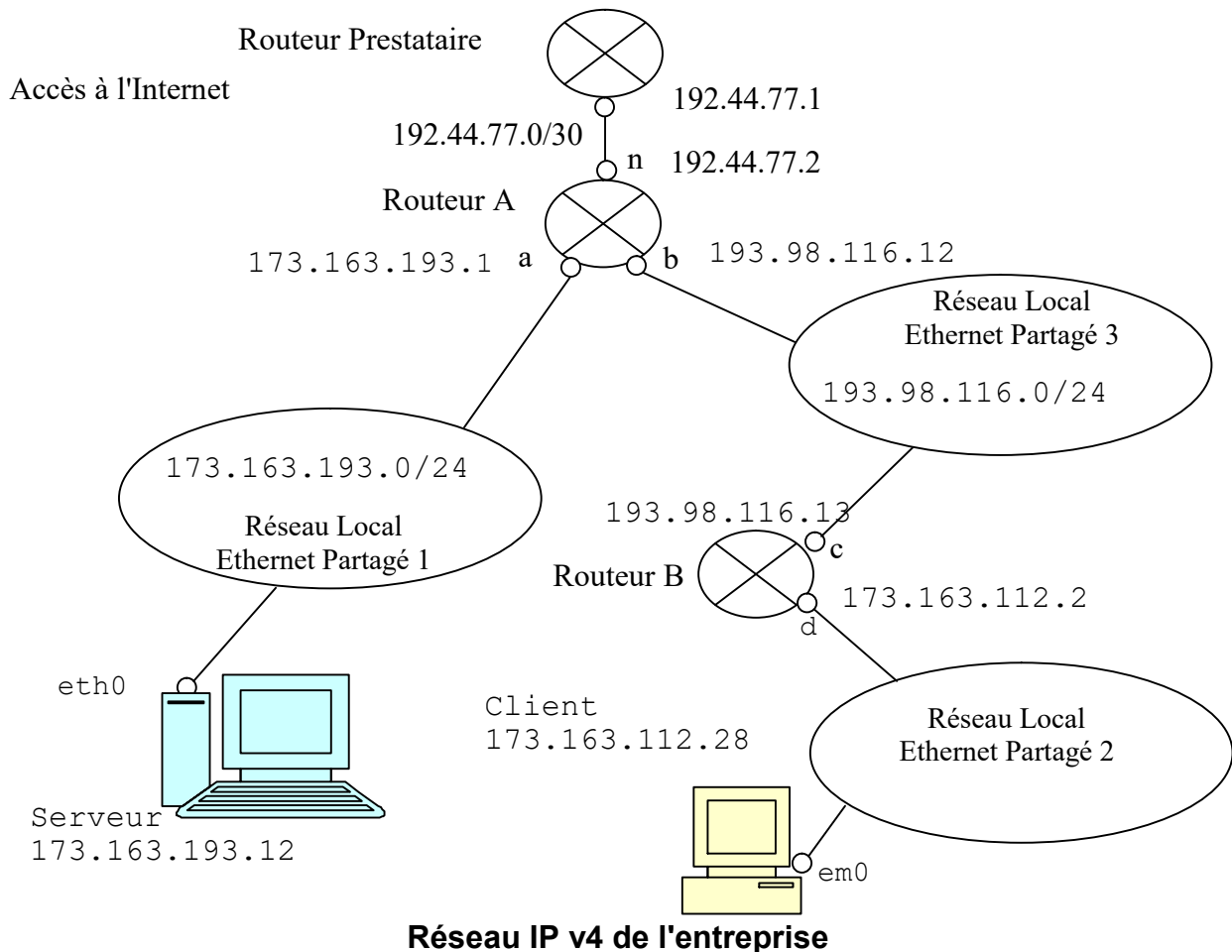
1      5 ms      2 ms      6 ms  163.173.112.2
2      3 ms      9 ms     47 ms  163.173.228.26

```

Ce choix est-il cohérent avec votre réponse à la question 3 ? Pourquoi ?

Exercice 4 : Fonctionnement du Routage IP V4 dans un trajet Client-Serveur, illustration de l'acheminement d'un datagramme à travers un ensemble de sous-réseaux

Dans le réseau de la figure ci-après on raisonne suivant un adressage de type CIDR (Classless Inter Domain Routing). On travaille sur le réseau suivant :



Vous observerez que certaines informations sont manquantes, par exemple pour le réseau local Ethernet partagé 2. Les questions de l'exercice vont vous permettre de compléter les informations manquantes.

On s'intéresse à tout ce qui peut être lié à l'acheminement d'une source vers une destination IP. Les routeurs sont configurés manuellement (routage statique).

Soit une station qu'on désignera par Client. Son système d'exploitation est de type Windows. On applique la commande `ipconfig/all`, et on obtient l'affichage suivant :

```
Suffixe DNS propre ... la connexion. : manc.fr
Description. . . . . : Ethernet LAN 802.3 NIC
Adresse physique . . . . . : 4C-ED-DE-E5-A8-3A
Adresse IPv4 . . . . . : 173.163.112.28
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 173.163.112.2
Serveurs DNS. . . . . : 173.163.128.6
```

Question 1

Donner le masque de sous-réseau auquel appartient Client en notation compacte à partir des résultats de la commande `ipconfig` ci-dessus.

Question 2

Quelle est l'adresse IPv4 correspondant à l'interface Ethernet d'adresse MAC :

4C-ED-DE-E5-A8-3A ?

Question 3

Quelle est l'adresse IP du réseau auquel appartient cette interface ? Expliquez très brièvement comment vous la trouvez.

Question 4

Quelle est l'adresse de broadcast IP associée à ce réseau IP ? Expliquez très brièvement comment vous la trouvez.

Question 5

Combien d'adresses IPv4 sont disponibles pour être affectées à des interfaces dans ce sous-réseau ? On supposera que chaque machine n'a qu'une seule interface réseau. Expliquez brièvement votre résultat. Observez bien le réseau local Ethernet partagé 2 avant de répondre.

Question 6

L'adresse IP de l'interface du routeur associée à ce réseau IP V4 est 173.163.112.2. Complétez les cases vides de la table de routage de la machine `Client` ci-après.

On indique que le nom de l'interface réseau de la machine `Client` est `em0`.

Réseau IP/mask	Next-Hop	Commentaire	Inter-face	Accessibilité
0.0.0.0/0		Route par défaut	em0	distant
127.0.0.0/8	0.0.0.0	Loopback, on ne passe par la carte NIC	lo0	direct
	0.0.0.0	Le réseau IP où je suis connecté, on passe par la carte NIC	em0	direct

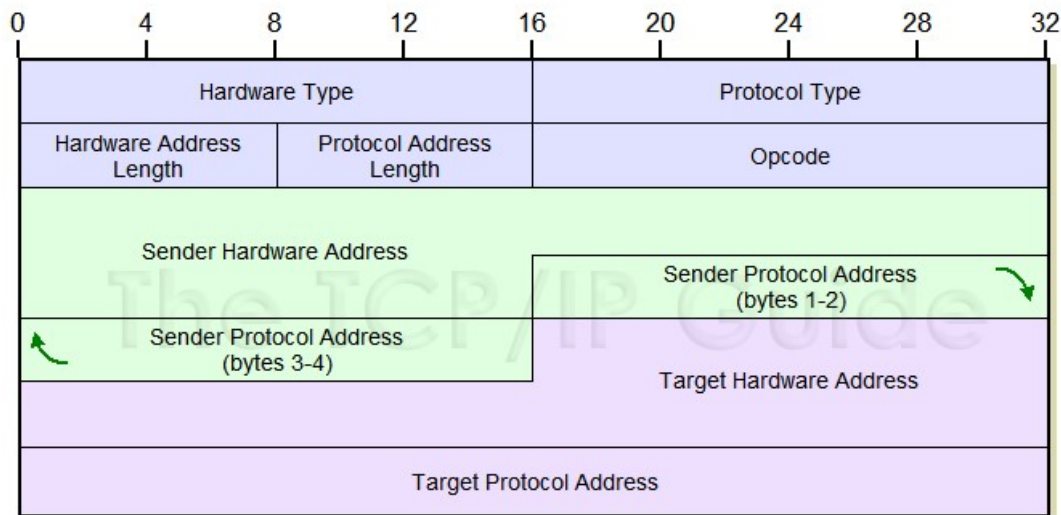
Question 7

Si une trame Ethernet part de l'interface `em0`. Quelle sera l'adresse MAC dans le champ source de cette trame ?

Question 8

La station `Client` ne connaît pas l'adresse Ethernet de l'interface du routeur reliée à son sous-réseau IP. Elle effectue donc une requête ARP (Address Resolution Protocol) pour la connaître.

On donne le format d'une requête ARP telle qu'elle est définie dans le document RFC826 de l'IETF et dessinée au lien http://www.tcpipguide.com/free/t_ARPMessageFormat.htm (consulté le 30/11/2016).



Format d'une ARP (demande ou réponse)

- Le champ `Hardware Type` vaut 1 pour des adresses Ethernet. Pour ARP "Hardware" est synonyme de Ethernet.
- Le champ `Protocol Type` vaut 0800 en hexadécimal pour Internet. Pour ARP "Protocol" est synonyme de Internet.
- `Opcode` vaut 1 pour une requête de résolution d'adresse IP ARP, et, 2 pour la réponse à une résolution d'adresse.
- `Sender` correspond à l'émetteur du message ARP.
- `Target` correspond au destinataire du message ARP.

A partir de la figure "Format d'une unité de données de protocole ARP", compléter la requête ARP ci-dessous en remplissant la partie manquante.

Question 9

Comme Client ne connaît pas l'adresse Ethernet qui correspond à l'adresse IP de destination 173.163.112.2 pour atteindre le routeur, va-t-il utiliser une adresse destination MAC d'Ethernet de type multicast (diffusion sur un groupe d'adresses MAC, par exemple un groupe de routeurs) ou broadcast (diffusion à toutes les adresses MAC du réseau local ff:ff:ff:ff:ff:ff) ?

On rappelle la structure d'une trame Ethernet :

Adresse MAC destination	Adresse MAC source	Type	Charge utile - Données	FCS- contrôle d'erreur
6 octets	6 octets	2 octets	46 à 1500 octets	4 octets

Question 10

Remplissez les champs Adresses MAC de la trame Ethernet envoyée par la carte Ethernet de Client (em0) et qui contient la requête ARP ci-dessus.

On vous indique que le champ type de la trame Ethernet transportant une requête ARP est 0x0806.

Adresse MAC destination	Adresse MAC source	Type	Charge utile - Données	FCS- contrôle d'erreur

Question 11

Va-t-il être nécessaire d'ajouter du bourrage dans la partie données de la trame Ethernet encore appelée charge utile ci-dessus. Si oui, combien d'octets de bourrage sont ajoutés.

Question 12

Donnez la réponse ARP du routeur si l'adresse Ethernet de son interface d'adresse IP 173.163.112.2 est 4C-ED-DE-E5-09-4B.

Remplissez la partie manquante de la réponse ARP ci-après.

0001		0800	
06	04	0002	
		173	163
.112	2	4C - ED	-
DE	E5	- A8	- 3A
173	163	112	28

On rappelle que le datagramme qui va du client vers le serveur est acheminé dans une trame qui le contient comme charge utile. Ce datagramme applicatif a l'entête ci-dessous. Seuls les champs qui sont les plus significatifs pour le problème à résoudre dans la question ci-après sont explicités.

0	1	2	3
0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0 1
+	+	+	+
4	5	0 0	Total Length
+	+	+	+
Identification	Flags	Fragment Offset	
+	+	+	+
Time to Live	06	Header Checksum	
+	+	+	+
173.163.112.28 (source client)			
+	+	+	+
173.163.193.12 (destination serveur)			
+	+	+	+

Entête du Datagramme IP envoyé de la source 173.163.112.28 à la destination 173.163.193.12

Question 13

Remplir tous les champs d'adresse MAC de la trame Ethernet qui va du Client au routeur B et qui contient le datagramme IP à émettre de la figure ci-après.

Adresse MAC destination	Adresse MAC source	Type	Charge utile - Données	FCS- contrôle d'erreur
			DDDDDDDD...DDD	XXXXXXXXXX

Question 14

Est-ce que le datagramme contenu dans la trame répondue à la question 13 va s'arrêter sur le prochain routeur ou va poursuivre son chemin ? Expliquer brièvement pourquoi.

Question 15

Pour le datagramme ci-dessus, qu'elle est la taille de l'entête IP en nombre d'octets ? Y a-t-il des options dans l'entête du datagramme ?

Le routeur destinataire de la trame est le routeur B. La table de routage du routeur B est la suivante :

lig	Destination	Next hop	Port	Type
1	0.0.0.0/0	193.98.116.12	c	distant
2	193.98.116.0/24	0.0.0.0	c	direct
3	173.163.112.0/24	0.0.0.0	d	direct

Question 16

Une fois le datagramme arrivé sur le routeur B. Quelle est la ligne de la table de routage de B qui va être sélectionnée pour le faire sortir et atteindre la destination Serveur qui a l'adresse IPv4 173.163.193.12. Expliquez brièvement pourquoi.

Question 17

Est-ce que les adresses IP source et/ou destination contenues dans le datagramme envoyé par Client vont être modifiées par le routeur B pour que le datagramme puisse atteindre sa destination finale qui est la machine Serveur ?

Question 18

Si l'adresse MAC de l'interface c du routeur B est : 4C-ED-DE-E5-08-5C, et, si l'adresse MAC de l'interface b du routeur A est : 4C-ED-DE-E5-07-6D.

Donner les adresses MAC source et destination de la trame qui circule entre les routeurs A et B. Vous remplirez le dessin ci-dessous.

Adresse MAC destination	Adresse MAC source	Type	Charge utile - Données	FCS- contrôle d'erreur
		0x0800	DDDDDDDD...DDD	XXXXXXXXXX

Soit la table du routeur A :

lig	Destination	Next hop	Port	Type
1	0.0.0.0/0	192.44.77.1	n	distant
2	192.44.77.0/30	0.0.0.0	n	direct
3	173.163.193.0/24	0.0.0.0	a	direct
4	193.98.116.0/24	0.0.0.0	b	direct
5	173.163.112.0/24	193.98.116.13	b	distant



Question 19

Une fois le datagramme arrivé sur le routeur A. Quelle est la ligne de la table de routage de A qui va être sélectionnée pour le faire sortir et atteindre la destination Serveur qui est d'adresse IPv4 173.163.193.12. Expliquez très brièvement pourquoi.

Correction :

- $173.163.193.12/0 = 0.0.0.0$, ligne 1 candidate résultat identique
- $173.163.193.12/30 = 173.163.193.12$, ligne 2 pas candidate résultat différent
- $173.163.193.12/24 = 173.163.193.0$, ligne 3 candidate
- $173.163.193.12/24 = 173.163.193.0$, ligne 4 pas candidate résultat différent
- $173.163.193.12/24 = 173.163.193.0$, ligne 5 pas candidate résultat différent

La ligne 3 a un masque plus long que la ligne 1, c'est donc la ligne retenue

Le datagramme poursuit sa route en étant émis par l'interface a du routeur A sur le réseau local Ethernet 1.

Question 20

Est-ce que la trame qui sera générée par le routeur A va atteindre l'hôte Serveur sans aucun relaying par un routeur ? Pourquoi ?

Question 21

Si l'adresse MAC de l'interface a du routeur A est : 4C-ED-DE-E5-06-5E. Et si l'adresse MAC de Serveur est 4C-ED-DE-E5-05-6F. Donner les adresses MAC source et destination de la trame qui est envoyée par le routeur A.

Adresse MAC destination	Adresse MAC source	Type	Charge utile - Données	FCS- contrôle d'erreur
		0x0800	DDDDDDDD...DDD	XXXXXXXX

Question 22

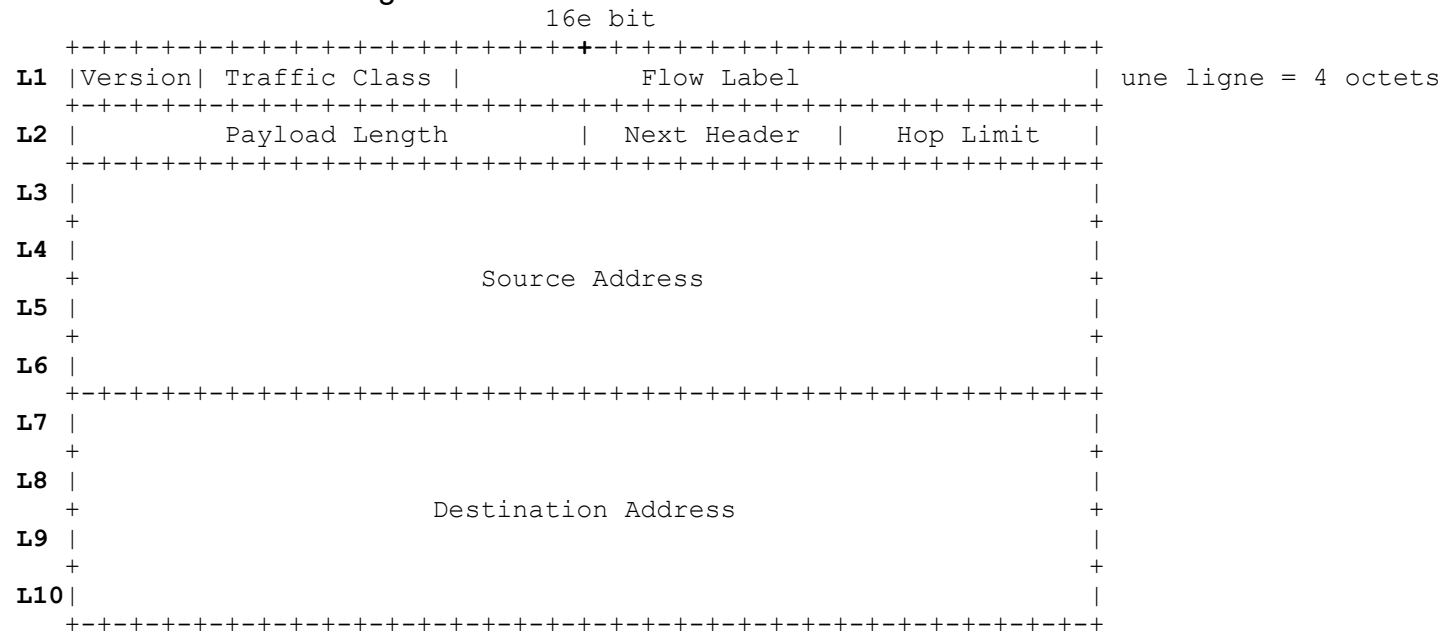
Si on effectue la commande `traceroute Serveur` sur la machine Client, donner la liste des adresses ip que va afficher le résultat de la commande.

Exercice 5 : Découverte d'un des services d'ICMPv6 : Neighbor Discovery équivalent à ARP pour IPv4 – facultatif mais recommandé pour tous ceux qui feront du réseau que ça soit un peu, beaucoup, passionnément ou à la folie !!!

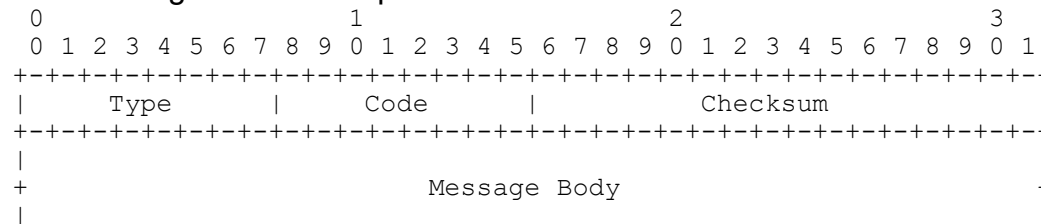
On donne la structure globale d'une trame Ethernet :

Ethernet II				
Destination MAC 6 Bytes	Source MAC 6 Bytes	Type 2 Bytes	Data 46 – 1500 Bytes	Frame Check Sequence 4 Bytes

On donne la structure de l'entête d'un datagramme IPv6 suivant la RFC8200 :



On donne le format d'un message ICMPv6 d'après la RFC 4443 :



On effectue la capture de trames suivante avec un analyseur de protocole, ici Wireshark :

Time	Source	Destir	Proto	Lengt	Info
1 0.000000	fe80::c001:2f...	ff...	IC...	86	Neighbor Solicitation for fe80::c002:3ff:fee4:0 from c2:01:02:40:00:00
2 0.024297	fe80::c002:3f...	fe...	IC...	86	Neighbor Advertisement fe80::c002:3ff:fee4:0 (sol, ovr) is at c2:02:03:e4:00:00
3 5.028119	fe80::c002:3f...	fe...	IC...	86	Neighbor Solicitation for fe80::c001:2ff:fe40:0 from c2:02:03:e4:00:00
4 5.055978	fe80::c001:2f...	fe...	IC...	78	Neighbor Advertisement fe80::c001:2ff:fe40:0 (sol)

Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
 Ethernet II, Src: c2:01:02:40:00:00 (c2:01:02:40:00:00), Dst: IPv6mcast_ff:e4:00:00 (33:33:ff:e4:00:00)
 > Destination: IPv6mcast_ff:e4:00:00 (33:33:ff:e4:00:00)
 > Source: c2:01:02:40:00:00 (c2:01:02:40:00:00)
 Type: IPv6 (0x86dd)
 Internet Protocol Version 6, Src: fe80::c001:2ff:fe40:0, Dst: ff02::1:ffe4:0
 0110 = Version: 6
 ▾ 1110 0000 = Traffic Class: 0xe0 (DSCP: CS7, ECN: Not-ECT)
 1110 00.. = Differentiated Services Codepoint: Class Selector 7 (56)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
 0000 0000 0000 0000 0000 = Flow Label: 0x000000
 Payload Length: 32
 Next Header: ICMPv6 (58)
 Hop Limit: 255
 Source: fe80::c001:2ff:fe40:0
 Destination: ff02::1:ffe4:0
 Internet Control Message Protocol v6
 Type: Neighbor Solicitation (135)
 Code: 0
 Checksum: 0x334f [correct]
 [Checksum Status: Good]
 Reserved: 00000000
 Target Address: fe80::c002:3ff:fee4:0
 ▾ ICMPv6 Option (Source link-layer address : c2:01:02:40:00:00)
 Type: Source link-layer address (1)
 Length: 1 (8 bytes)
 Link-layer address: c2:01:02:40:00:00 (c2:01:02:40:00:00)

00	33 33 ff e4 00 00 c2 01 02 40 00 00 86 dd 6e 00	33 - - - - - @ - - - - n -
10	00 00 00 20 3a ff fe 80 00 00 00 00 00 00 c0 01	- - - : - - - - - - - - -
20	02 ff fe 40 00 00 ff 02 00 00 00 00 00 00 00 00	- - - @ - - - - - - - - -
30	00 01 ff e4 00 00 87 00 33 4f 00 00 00 00 fe 80	- - - - - 30 - - - - - ..
40	00 00 00 00 00 00 c0 02 03 ff fe e4 00 00 01 01	- - - - - - - - - - - - - -
50	c2 01 02 40 00 00	- - - @ - - -

Question 1 : On s'intéresse pour l'instant à la trame 1.

- Délimiter l'entête de la trame Ethernet dans la capture en hexadécimal ci-dessous.
 - Délimiter l'entête du datagramme IPv6 dans la capture en hexadécimal ci-dessous.
 - Délimiter le message ICMPv6 dans la capture en hexadécimal ci-dessous.
 - A quelle couche appartient ICMPv6 d'après l'observation de la trace ? Pourquoi ?
- Ne pas hésiter à utiliser des couleurs différentes pour que votre réponse soit facile à lire.

```

0000      33 33 ff e4 00 00 c2 01      02 40 00 00 86 dd 6e 00
0010      00 00 00 20 3a ff fe 80      00 00 00 00 00 00 c0 01
0020      02 ff fe 40 00 00 ff 02      00 00 00 00 00 00 00 00
0030      00 01 ff e4 00 00 87 00      33 4f 00 00 00 00 fe 80
0040      00 00 00 00 00 00 c0 02      03 ff fe e4 00 00 01 01
0050      c2 01 02 40 00 00

```

Attention la colonne la plus à gauche numérote les lignes et cette numérotation est hexadécimale, pour ne pas confondre la police est différente.

Question 2 : Adresse Multicast MAC/Ethernet pour IPv6.

Wikipedia indique "Au niveau ethernet, un préfixe OUI est réservé aux adresses IPv6 multicast (33:33:xx)". "xx" figure les octets restants d'une adresse MAC sur 48 bits. L'OUI (Organizationally Unique Identifier) identifie un fabricant de carte Ethernet.

Combien d'adresses MAC peut-on associer à une OUI, justifiez votre réponse² ?

L'ordre des bits dans les documents des organismes de l'Internet, IETF (Internet Engineering Task Force) et les Request For Comments (RFC) par exemple, est différent de l'ordre des bits dans les documents IEEE (Institut of Electrical and Electronics Engineers) norme IEE802.3 Ethernet. Quel ordre sur les bits d'un octet a été choisi par l'IETF, et plus généralement l'ordre sur les octets d'un mot (IPv4 par exemple) ?

² Sans justification, même si la réponse est juste, elle n'est pas comptée et c'est 0.

Dans une adresse MAC, comme 33:33:FF:E4:00:00³, à quel bit reconnaît-on que c'est une adresse multicast, groupe de diffusion en français, et non une adresse broadcast (c'est très différent), quelle est sa position dans l'octet concerné ?

A votre avis, brièvement, pour quel usage a-t-on un préfixe OUI qui identifie toutes les adresses multicast MAC pour le multicast IPv6 ?

Question 3 : Format des adresses IPv6.

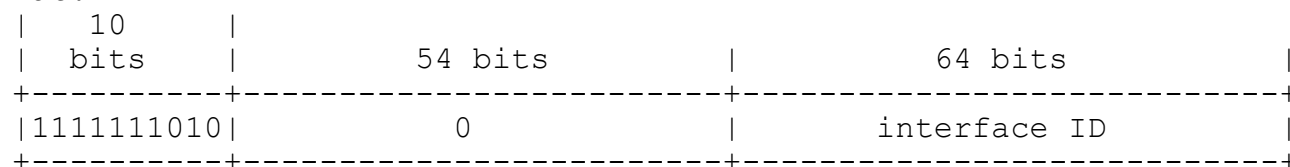
Une adresse IPv6 fait 128 bits. Combien cela représente d'octets et combien de mots de 4 octets ?

Les adresses IPv6 montrées dans la fenêtre explicative de Wireshark (celle du milieu) sont différentes de celles que vous avez trouvées dans la trace hexadécimale (fenêtre du bas). Expliciter complètement l'adresse `fe80::c001:2ff:fe40:0` de telle façon qu'il y ait 4 chiffres hexadécimaux séparés par ":".

Si on applique le masque en notation compacte /10 sur l'adresse `fe80::c001:2ff:fe40:0`, quelle est l'adresse IPv6 résultante ?

La RFC4291 section "2.5.6. Link-Local IPv6 Unicast Addresses" dit :

"Link-Local addresses are for use on a single link. Link-Local addresses have the following format:



Link-Local addresses are designed to be used for addressing on a single link for purposes such as automatic address configuration, neighbor discovery, or when no routers are present.

Routers must not forward any packets with Link-Local source or destination addresses to other links."

Puis dans son annexe A, y est écrit :

"[EUI64] defines a method to create an IEEE EUI-64 identifier from an IEEE 48-bit MAC identifier. This is to insert two octets, with hexadecimal values of 0xFF and 0xFE (see the Note at the end

³ Le préfixe 33:33:FF d'une adresse MAC est dédié à l'usage du protocole ICMPv6 Neighbor Discovery

of appendix), in the middle of the 48-bit MAC (between the company_id and vendor-supplied id). An example is the 48-bit IEEE MAC with Global scope:

```

| 0           1|1           3|3           4|
| 0           5|6           1|2           7|
+-----+-----+-----+
| ccccccc0gcccccccc | cccccccmmmmmmmm | mmmmmmmmmmmmmmmmm |
+-----+-----+-----+

```

where "c" is the bits of the assigned company_id, "0" is the value of the universal/local bit to indicate Global scope, "g" is individual/group bit, and "m" is the bits of the manufacturer-selected extension identifier. The interface identifier would be of the form:

```

| 0           1|1           3|3           4|4           6|
| 0           5|6           1|2           7|8           3|
+-----+-----+-----+-----+
| cccccclgcccccccc | ccccccc1111111 | 11111110mmmmmmmm | mmmmmmmmmmmmmmm |
+-----+-----+-----+-----+

```

When IEEE 802 48-bit MAC addresses are available (on an interface or a node), an implementation may use them to create interface identifiers due to their availability and uniqueness properties."

Donner les 64 derniers bits de l'adresse IPv6 multicast `fe80::c001:2ff:fe40:0` qui correspondent à l'identificateur d'interface EUI-64 associé. On y retrouve l'adresse MAC Ethernet `c2:01:02:40:00:00`. mais pourquoi a-t-on `c0` dans l'adresse IPv6 au lieu de `c2` qui est dans l'adresse MAC ?

Question 4 : ICMPV6 avec le service Neighbor Discovery a un rôle équivalent à ARP (Address Resolution Protocol) qui est utilisé en combinaison avec IPv4.

C2:01:02:E4:00

1 0.000000 fe80::c001:2f... ff... IC... 86 Neighbor Solicitation for fe80::c002:3ff:fee4:0 from c2:01:02:40:00:00

Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)

Ethernet II, Src: c2:01:02:40:00:00 (c2:01:02:40:00:00), Dst: IPv6mcast_ff:e4:00:00 (33:33:ff:e4:00:00)

Internet Protocol Version 6, Src: fe80::c001:2ff:fe40:0, Dst: ff02::1:ffe4:0

Internet Control Message Protocol v6

Type: Neighbor Solicitation (135)

Code: 0

Checksum: 0x334f [correct]

[Checksum Status: Good]

Reserved: 00000000

Target Address: fe80::c002:3ff:fee4:0

✓ ICMPv6 Option (Source link-layer address : c2:01:02:40:00:00)

Type: Source link-layer address (1)

Length: 1 (8 bytes)

Link-layer address: c2:01:02:40:00:00 (c2:01:02:40:00:00)

33:33:FF:E4:00

2 0.024297 fe80::c002:3f... fe... IC... 86 Neighbor Advertisement fe80::c002:3ff:fee4:0 (sol, ovr) is at c2:02:03:e4:00:00

Frame 2: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)

Ethernet II, Src: c2:02:03:e4:00:00 (c2:02:03:e4:00:00), Dst: c2:01:02:40:00:00 (c2:01:02:40:00:00)

Internet Protocol Version 6, Src: fe80::c002:3ff:fee4:0, Dst: fe80::c001:2ff:fe40:0

Internet Control Message Protocol v6

Type: Neighbor Advertisement (136)

Code: 0

Checksum: 0x0d2b [correct]

[Checksum Status: Good]

✓ Flags: 0x60000000, Solicited, Override

0 = Router: Not set

..... = Solicited: Set

...1 = Override: Set

...0 0000 0000 0000 0000 0000 0000 0000 = Reserved: 0

Target Address: fe80::c002:3ff:fee4:0

✓ ICMPv6 Option (Target link-layer address : c2:02:03:e4:00:00)

Type: Target link-layer address (2)

Length: 1 (8 bytes)

Link-layer address: c2:02:03:e4:00:00 (c2:02:03:e4:00:00)

C2:02:03:E4:00

C2:01:02:E4:00

3 5.028119 fe80::c002:3f... fe... IC... 86 Neighbor Solicitation for fe80::c001:2ff:fe40:0 from c2:02:03:e4:00:00

Frame 3: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)

Ethernet II, Src: c2:02:03:e4:00:00 (c2:02:03:e4:00:00), Dst: c2:01:02:40:00:00 (c2:01:02:40:00:00)

Internet Protocol Version 6, Src: fe80::c002:3ff:fee4:0, Dst: fe80::c001:2ff:fe40:0

Internet Control Message Protocol v6

Type: Neighbor Solicitation (135)

Code: 0

Checksum: 0x70d0 [correct]

[Checksum Status: Good]

Reserved: 00000000

Target Address: fe80::c001:2ff:fe40:0

▼ ICMPv6 Option (Source link-layer address : c2:02:03:e4:00:00)

Type: Source link-layer address (1)

Length: 1 (8 bytes)

Link-layer address: c2:02:03:e4:00:00 (c2:02:03:e4:00:00)

4 5.055978 fe80::c001:2f... fe... IC... 78 Neighbor Advertisement fe80::c001:2ff:fe40:0 (sol)

Frame 4: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)

Ethernet II, Src: c2:01:02:40:00:00 (c2:01:02:40:00:00), Dst: c2:02:03:e4:00:00 (c2:02:03:e4:00:00)

Internet Protocol Version 6, Src: fe80::c001:2ff:fe40:0, Dst: fe80::c002:3ff:fee4:0

Internet Control Message Protocol v6

Type: Neighbor Advertisement (136)

Code: 0

Checksum: 0xf6bf [correct]

[Checksum Status: Good]

▼ Flags: 0x40000000, Solicited

0... .. = Router: Not set

.1.. .. = Solicited: Set

..0. = Override: Not set

...0 0000 0000 0000 0000 0000 0000 0000 = Reserved: 0

Target Address: fe80::c001:2ff:fe40:0

Ci-dessus l'enchaînement de 4 trames qui portent les messages ICMP v6 avec les options liées à la découverte de voisins sur un lien.

[illegible]

"4.6.1. Source/Target Link-layer Address

[illegible]

```
Fields: /* Type; Longueur; Valeur */
        Type
```

```
1 for Source Link-layer Address
2 for Target Link-layer Address
```


Length	The length of the option (including the type and length fields) in units of 8 octets.
For	example, the length for IEEE 802 addresses is 1
Link-Layer Address	The variable length link-layer address.
Description	<p>The Source Link-Layer Address option contains the link-layer address of the sender of the packet. It is used in the Neighbor Solicitation, Router Solicitation, and Router Advertisement packets.</p> <p>The Target Link-Layer Address option contains the link-layer address of the target. It is used in Neighbor Advertisement and Redirect packets."</p>

On vous demande d'établir quelques points de comparaison entre les protocoles ARP/IPv4 et ICMPv6-Neighbor Discovery/IPv6. On vous demande pour cela de remplir le tableau ci-dessous (0,25 point par case juste) :

	ARP	ICMPv6-Neighbor Discovery
Protocole d'acheminement sous-jacent des messages		
Type d'adresse MAC pour l'envoi de la requête		
Un message est-il bloqué par un routeur ?		
Pourquoi ?		
Un message est-il bloqué par un commutateur ?		
Pourquoi ?		
Charge induite dans la partie information de la trame Ethernet		
Est-il nécessaire de faire du bourrage dans la trame Ethernet		

Question 5 : Dans l'entête IPv6 qui achemine la requête IPv6, le champ associé à la Qualité de Service contient la valeur CS7. Cette valeur est associée à la gestion du réseau et attribue une priorité très élevée au datagramme qui la porte. Sachant que les datagrammes échangés le sont entre deux extrémités en liaison directe, à quoi cette information pourrait-elle servir sur chacun des hôtes ? Pour trouver une réponse, il faut raisonner par rapport à la congestion des files de messages dans la couche IP qui offre un acheminement en mode datagramme donc non fiable. Est-ce qu'on peut associer une qualité de service CS7 pour une requête ou une réponse ARP ? (1 point).

Exercice 6 : Fragmentation IPv4 lors de la traversée d'un routeur.

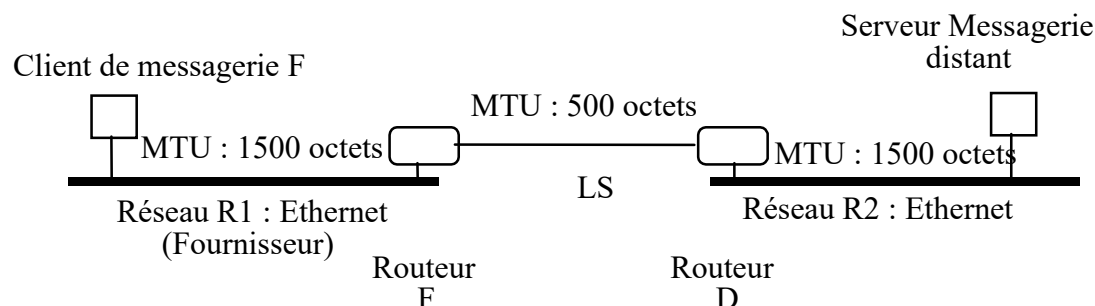
Question 1

Dans un réseau qu'est ce que la fragmentation ?

Question 2

Comment fonctionne la fragmentation en IP V4 (expliquez en les principes généraux) ?

Un client de messagerie F transfère un message électronique de 4000 octets de données vers un serveur distant en utilisant trois voies de communication successives selon la figure ci-après. On considère que toutes les entêtes ajoutées par les différentes couches de protocoles traversées au dessus de la couche IP font partie des 4000 octets. Dans les datagrammes IP l'entête est une entête standard de 20 octets (il n'y a pas d'options rajoutées en extensions dans les entêtes IP).



Question 3

Expliquez dans le fonctionnement de la fragmentation et décrivez précisément les entêtes des datagrammes IP échangés. Vous ne décrirez que les champs associés à la fragmentation et la longueur du datagramme ?

Question 4

Pourquoi la fragmentation est incompatible avec des flux de données nécessitant une QoS temps réel ? Quels paramètres de QoS : latence, gigue, débit, taux de perte vont être influencés par la fragmentation ?