

DS 1 : Internet (INTERNational NETwork).

I Une structure physique.

- Exercice 1.**
1. Expliquer la différence entre internet et le Web. Internet est un réseau d'ordinateurs qui communiquent entre eux à l'aide de protocoles
C'est comparable au réseaux routiers (le code de la route en est un protocole)
Le Web Le Web est l'une des applications qui utilise internet.
Il y en a d'autres : courrier électronique, transfert de fichiers, voip pour la téléphonie etc.
C'est comparable aux voitures sur le réseau routier (elles respectent le code de la route...)
 2. Citer différents éléments faisant partie du réseau physique.
Aujourd'hui, 99% du flux international passe par ces câbles sous-marins et l'utilisation de la fibre optique. Sinon ADSL, réseaux câblés urbain, 4G, satellite...
 3. Citer un ou plusieurs protocoles utilisé(s) sur le réseau internet.
TCP, IP, UDP, HTTP...
 4. Citer le protocole utilisé pour tout envoi sur internet.
Tous les envois sur Internet utilise le protocole IP (envoi par paquets IP)

II Adresse IP.

- Exercice 2.**
1. Donner le format d'une adresse IPv4.
Une adresse IP est, à ce titre, généralement représentée sous la forme de 4 octets de nombres allant de 0 à 255 et écrite sous forme décimale plutôt que sous forme binaire. Par exemple, l'adresse 168.212.226.204. Chaque nombre varie entre 0 et 255.
 2. Expliquer le rôle du DNS.
Le Domain Name System, généralement abrégé DNS, qu'on peut traduire en « système de noms de domaine », est le service informatique distribué utilisé pour traduire les noms de domaine Internet en adresse IP.
 3. A l'aide de **l'annexe 2**, déterminer si les adresses ci dessous sont privées ou public et à quelle classe elles appartiennent. Attention certaines de ces séries ne sont pas des adresses IP. Dans ce cas, indiquer le.

(a) 1.250.232.54 : Publique classe A	(c) 353.45.123.123 : Ce n'est pas une adresse IP puisque 353>255.	B.
(b) 194.233.234.12 : Publique classe C	(d) 172.162.123.234 : Privée classe	(e) 192.168.0.172 : Privée classe C.
		(f) 92.32.1.2 : Publique classe A.
 4. On vous donne un réseau privé pour lequel les adresses IP au sein du réseau commence par 192.168.9.*** (adresse IP de classe C). Donner approximativement le nombre maximal d'ordinateurs que peut gérer ce réseau privé.
Le nombre d'ordinateur peut être approximativement de 250 (en effet entre 0 et 255 moins certaines adresses pour la passerelle par exemple ou autre)
 5. Expliquer ce que représentent les informations encadrer ci-dessous et obtenues lors d'un ipconfig. (vous donnerez la classe des adresses IP présentes).

```

Suffixe DNS propre à la connexion. . . . :
Adresse IPv6 de liaison locale. . . . : fe80::11ad:8c8c:eaca:7bd%10
Adresse IPv4. . . . . : 192.168.9.103
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 192.168.9.1
-----
Carte Tunnel Local Area Connection* 13 :
Suffixe DNS propre à la connexion. . . . :
Adresse IPv6. . . . . : 2001:0:9d38:6abd:202b:25d4:d6aa:5e62
Adresse IPv6 de liaison locale. . . . : fe80::202b:25d4:d6aa:5e62%22
Passerelle par défaut. . . . . :

```

- 192.168.9.103 est l'adresse local de l'ordinateur au sein du réseau.
- 192.168.9.1 est l'adresse passerelle c'est-à-dire celle sur routeur permettant au ordinateur du réseau d'avoir accès au réseau Internet.
- (Bonus) Le masque (non évalué dans le barème) permet de savoir combien de nombre sont fixe dans le réseau ici les "3" 255 permettent de comprendre que les trois nombres 192.168.9.*** sont fixes dans le réseau local.

III Transport des données.

Exercice 3. 1. Expliquer en quoi le protocole TCP est-il un protocole dit *sûr*.

Grâce au protocole TCP, les applications peuvent communiquer de façon sûre grâce au système d'accusés de réception du protocole TCP.

- Lors de l'envoi un fichier par le protocole TCP, que ce passe-t-il si un paquet n'est pas reçu par le destinataire. Il n'y a pas d'accusé de réception et le paquet est alors renvoyé.
- Quel est le protocole qui s'occupe de l'envoi des paquets et celui qui permet de remettre les paquets en ordre ? Le protocole TCP est le protocole qui s'occupe de la gestion des paquets tandis que le protocole IP s'occupe de l'envoi des paquets.
- Recopier et compléter le texte ci-dessous à l'aide des étiquettes proposées.

Internet Protocol (IP) s'occupe de []. Un paquet IP émis contient [] du [] et de [].
 IP s'exécute sur chaque [] du réseau, appelé [].
 Transmission Control Protocol (TCP) assure la [] des échanges et découpe les données en [].
 Il s'exécute de [] et vérifie la réception des segments avec des [].

[bout en bout] [fiabilité] [l'acheminement des données] [les adresses]
 [segments numérotés] [destinataire] [l'expéditeur]
 [accusés de réception] [noeud d'interconnexion] [routeur]

Internet Protocol (IP) s'occupe de l'acheminement des données. Un paquet IP émis contient les adresses du destinataire et de l'expéditeur.

IP s'exécute sur chaque noeud du réseau, appelé routeur.

Transmission Control Protocol (TCP) assure la fiabilité des échanges et découpe les données en segments numérotés.

Il s'exécute de bout en bout et vérifie la réception des segments avec des accusés de réception.

Exercice 4. Lire l'annexe 1 sur le protocole UDP.

- Expliquer les différences et similitudes entre protocole TCP et UDP.

Les différences :

- Pas d'accusé de réception pour l'UDP, ensuite pas de connexion (pas d'échange) entre l'expéditeur et le destinataire.
- L'UDP est bien plus rapide que le TCP.
- Pas d'authenticité des données pour l'UDP.

Les similitude :

- L'UDP comme le TCP peut contenir l'adresse de l'expéditeur (doit pour le TCP bien sûr) .
- Ce charge de remettre en ordres les paquets.

- Expliquer pour quels types de fichiers l'on privilégiera le protocole TCP/IP et ceux pour lesquels on privilégiera le protocole UDP.

Pour les fichiers demandant une haute qualité de transmission : TCP.

Pour des données importante : TCP.

Pour des films ou des vidéos : UDP (perdre un peu de données n'est pas grave)

Pour des jeux.

IV Neutralité du Net.

Article du Monde (04 juillet 2014)

Qu'est-ce que la neutralité du Net ?

La neutralité du Net est le principe selon lequel tout le monde doit avoir un accès garanti aux mêmes contenus sur Internet, quel que soit son fournisseur d'accès.

Le Conseil supérieur de l'audiovisuel, les grandes chaînes françaises, une partie du gouvernement... Beaucoup de monde a l'air d'accord pour enterrer la neutralité du Net. Mais au fait, qu'entend-on par « neutralité du Net » ?

Définition

La neutralité du Net, c'est ce principe qui régit Internet depuis ses débuts, et qui garantit un traitement technique identique à tous les fournisseurs de contenus, petits ou grands, consensuels ou dérangeants.

En fait, il s'agit d'un principe simple de non-discrimination : tout le monde doit avoir un égal accès à Internet et aucun contenu (vidéo, site Web...) ne doit bénéficier d'un traitement préférentiel et s'afficher plus vite que les autres. Cette règle empêche le fournisseur d'accès à Internet d'influer sur ce que fait l'internaute ou sur la vitesse à laquelle sont transmis les paquets de données sur le réseau. Soit, comme dirait le comique britannique John Oliver : « La chose la plus ennuyeuse que j'aie jamais entendue. »

En réalité, la neutralité du Net est très importante. Elle intervient à chaque connexion à Internet, que vous vouliez regarder une vidéo sur YouTube, envoyer un mail... En clair, toutes les données doivent être traitées de la même manière, qu'elles proviennent de monsieur Tout-le-monde, du gouvernement ou des grosses entreprises. C'est comme ça que Google, YouTube, ou Facebook ont réussi à naître et à grandir, pour supplanter certaines compagnies.

Les conséquences ?

Aux États-Unis, les télécommunications ne sont pas vraiment d'accord avec ce principe. Comcast, un câblo-opérateur américain, a ainsi décidé de négocier avec Netflix pour diffuser ses contenus aussi rapidement que les autres, contre une participation financière. Netflix a fini par obtempérer après que Comcast a sensiblement ralenti la vitesse de téléchargement de ses contenus, obligeant ainsi les abonnés à attendre avant de pouvoir voir un film ou une série. Soudainement, la vitesse de téléchargement de Netflix a augmenté, ce qui fait dire à certains que l'on est en train de créer deux voies sur Internet, comme sur une autoroute. Les télécommunications se défendent en disant que ces deux voies permettent une voie rapide pour tout le monde et une voie ultrarapide pour les autres.

Si l'on va un peu plus loin, on peut imaginer un Internet à la carte.

En France

Le président du Conseil supérieur de l'audiovisuel, Olivier Schramek, a donc expliqué au Monde que selon lui : « Il faut en finir avec la conception absolutiste de la neutralité du Net. » Une clarification de la position du régulateur de l'audiovisuel, avec laquelle les groupes de télévision privés semblent majoritairement d'accord. Normalement, le principe de la neutralité du Net est protégé en France. Le Parlement européen le défend — tout en prévoyant des exceptions —, et plusieurs responsables politiques, à commencer par la secrétaire d'État au numérique, Axelle Lemaire, affirment vouloir le protéger. Elle déclarait ainsi en avril dernier dans une interview donnée au Point : « Je suis favorable à une neutralité qui est clairement affirmée et dont le principe s'applique aux réseaux comme aux grandes plates-formes de services. »

Le Monde

Exercice 5. 1. Que garantit la neutralité du net.

Un traitement technique identique à tous les fournisseurs de contenus.

2. Quelles seraient selon vous les conséquences de la fin de la neutralité du net pour certaines grandes entreprises.

La difficultés pour certaines d'être accessible par les particulier sans contribution financière auprès des opérateurs.

Une sélection des données diffusés par les opérateurs.

3. Quelles seraient selon vous les conséquences de la fin de la neutralité du net pour les particuliers.

Une tarification des abonnements en fonction de l'utilisation du réseau. Une connexion à la carte.

Annexe 1

Aperçu des propriétés de l'UDP

Afin de comprendre dans le détail comment la **transmission des paquets** est effectuée avec ce protocole, il est judicieux de se pencher plus précisément sur les caractéristiques du User Datagram Protocol déjà mentionnées.

1. **L'UDP est sans connexion** : le transport des données via le protocole UDP se démarque par le fait qu'il a lieu sans connexion existante entre l'expéditeur et le destinataire. Les paquets concernés sont ensuite envoyés à l'adresse IP privilégiée en **indiquant le port de destination**, sans que l'ordinateur auquel cette adresse est attribuée n'ait à envoyer une réponse. Si des paquets doivent être renvoyés à l'expéditeur, l'entête UDP peut également contenir le port source.
2. **Ports utilisés par l'UDP** : à l'instar du TCP, l'UDP a recours à des ports afin de remettre les paquets aux bons protocoles ultérieurs ou aux applications souhaitées sur le système de destination. Comme le modèle éprouvé, les ports sont définis à l'aide d'une numérotation, dont les numéros compris entre 0 et 1023 sont attribués à des services fixes.
3. **L'UDP permet une communication rapide, sans délai** : ce protocole de transport est adapté à une transmission rapide des données, car il n'établit pas de connexion. Ceci résulte également du fait que la perte de paquets individuels impacte uniquement la qualité de la transmission. En cas de connexion TCP, il est en revanche procédé automatiquement à une nouvelle demande des paquets perdus, ce qui bloque l'intégralité du processus de transmission.
4. **L'UDP n'offre aucune garantie quant à la sécurité et à l'authenticité des données** : le fait de renoncer à l'authentification mutuelle de l'expéditeur et du destinataire permet au protocole UDP d'assurer une vitesse de transmission exceptionnelle. Toutefois, le protocole ne peut garantir l'intégrité et la sécurité des paquets de données. L'ordre dans lequel les paquets ont été envoyés n'est pas non plus garanti. C'est pourquoi les services faisant appel à l'UDP doivent mettre à disposition des mesures de correction et de protection propres.

Annexe 2

Classes des adresses IP publiques

Classe	Valeur	1er octet binaire	nb de réseaux / nb hotes	Masque de sous-réseau
A	0.0.0.1 à 126.255.255.254	0xxx xxxx	126 réseaux 16 777 214 hotes	/8
B	128.0.0.1 à 191.255.255.254	10xx xxxx	16 384 réseaux 65 534 hotes	/16
C	192.0.0.1 à 223.255.255.254	110x xxxx	2 097 152 réseaux 254 hotes	/24
D	224.0.0.0 à 239.255.255.254	1110 xxxx	Multicast - Diffusion partielle	-
E	240.0.0.0 à 255.255.255.255	1111 xxxx	Expérimentale	-

Adresses IP privées

classe	Valeur	nb de réseaux / nb hotes	mask
A	10.0.0.0 à 10.255.255.254	1 réseau 16 777 214 hotes	/8
B	172.16.0.0 à 172.31.255.254	16 réseaux 65 534 hotes	/16
C	192.168.0.0 à 192.168.255.254	255 réseaux 254 hotes	/24

Attention dans ce tableau, on remarque que certaines adresses sont à classer à la fois dans les IP privées et publiques. Dans ce cas, elles seront privées.