Module: OSI, INTERNET ET PROGRAMMATION WEB

TP 1 – Architecture OSI et Réseaux locaux

Objectif : examiner l'architecture OSI, le principe de transmission aux différents niveaux en particulier physique, liaison et réseau. Présenter le protocole IP
Correction : la correction sera diffusée la semaine suivant la fin du TP sur le support cours.

I. Architecture OSI (Open System Interconnection)

1- Généralité

1.1Rappel du codage binaire

Les systèmes binaire et hexadécimal sont les systèmes de numération les plus utilisés en informatique. Le système binaire est un système de numération utilisant la base 2. On nomme couramment bit les chiffres de la numération binaire. Ceux-ci ne peuvent prendre que deux valeurs, notées par convention 0 et 1. Le système hexadécimal est un système de numération utilisant la base 16. Ce système utilise les
10 premiers chiffres et les 6 premières lettres comme montre le tableau suivant :

décimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
hexadécimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	10
binaire	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111	10000

La conversion de binaire en hexadécimal se fait facilement en regroupant les chiffres (les bits) quatre par quatre, ou inversement en remplaçant chaque chiffre hexadécimal par 4 chiffres binaires :

binaire	10101101010101100011110111						
regroupé par 4	1	0101	1010	1010	1100	1111	0111
regroupé en hexadécimal	1	5	A	A	C	F	7
hexadécimal	15AACF7						

La conversion avec le système décimal ne présente aucune difficulté particulière.
Ainsi 15AACF7 se convertit en calculant
1×166 + 5×165 + 10×164 + 10×163 + 12×162 + 15×161 + 7×160 = 22719735

Questions
1.1.1- Conversion en binaire :

a. $(125)_{10}$ = 1111101
b. $(92)_{10}$ = 1011100
c. $(27)_{10}$ = 11011
d. $(203)_{10}$ = 11001011
e. $(255)_{10}$ = 11111111

1.1.2. Conversion en décimal :
a. $(0000\ 0110)_2$ = 6
b. $(0110\ 0101)_2$ = 101
c. $(1000\ 1110)_2$ = 142
d. $(1010\ 1111)_2$ = 175
e. $(1100\ 0000)_2$ = 192

1.1.3. Conversion en décimal :
a. $(A1)_{16} = 161$
b. $(F2)_{16} = 242$
c. $(E2A)_{16} = 3626$
d. $(3B)_{16} = 59$
e. $(14D)_{16} = 333$

1.1.4. Conversion en binaire :
a. $(1F)_{16} = 11111$
b. $(2C)_{16} = 101100$
c. $(9E)_{16} = 10011110$
d. $(3B)_{16} = 111011$
e. $(B6)_{16} = 10110110$

1.2- Modes de transmission

1.2.1- Quelles sont les différences principales entre un réseau de transmission de circuit et un réseau de transmission à commutation par paquets ?

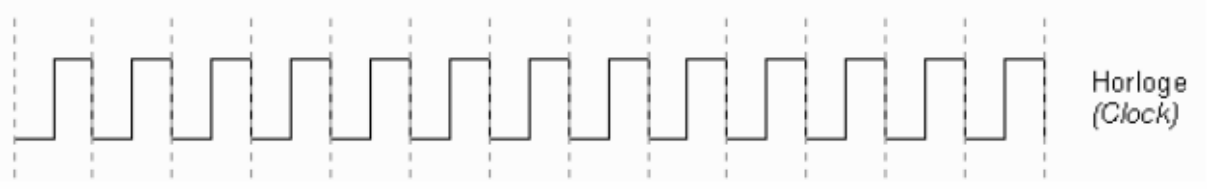
Dans les réseaux à commutation de circuit (e.g. réseau téléphonique), il y a de réservation de ressource réseau entre les interlocuteurs. La ressource réserve entre deux interlocuteurs peut être un circuit électrique continu (communication analogique) ou intervalle de temps (time slot) réservé dans une trame de données (communication numérique).
D'autre part, la communication à commutation par paquets (e.g. réseau TCP/IP), il n'y a pas de ressource réseau réservé entre les interlocuteurs. Donc, les paquets de la même communication peuvent être acheminés dans des chemins différents. Le chemin de chaque paquet dépend de l'état de réseau et des contenus des tables de routage au moment de son envoie.

1.2.2- Circuit virtuel
On dit le service Circuit Virtuel inadapté au transfert de SMS. Info ou intox ?

Tous les paquets (fragments) associés à un même message reçoivent un même n° de voie logique. Ceci identifie un circuit virtuel.
Les messages courts, encore appelés "SMS", s'echangent principalement entre terminaux mobiles, ils transitent par des serveurs spécialisés, routeurs, et peuvent être créés ou lus sur micro-ordinateurs. La réservation d'un circuit virtuel pour l'échange de brefs messages, faisant donc un seul paquet, conduit à un gaspillage de bande passante. L'on réserve plutôt des circuits virtuels pour les échanges où le flux de données est permanent.

2- Couche physique (codage Manchestter uniquement)

La transmission de données en mode série consiste à émettre dans le temps une suite d'éléments binaires (bits) ayant pour valeur "0" ou "1". En mode série dit "synchrone" cette transmission s'effectue au rythme d'une horloge associée :



2.1. Illustrez dans des figures (en synchronisant avec l'horloge) les codages bipolaire et Manchester des séries binaires suivantes :
a) 01001011000101
b) 10110100111010
c) 11010100011010

2.2- Quelle est votre observation sur ce codage ?

Le nombre de polarités « 1 » est égal au nombre de polarités « -1 » indépendant de séries binaires

3- Couches de liaison (et physique)

3.1- Hub
- Un hub permet-il de filtrer des paquets dynamiquement ?

Non, un hub n'est qu'un répétiteur.

- Un hub est-il un équipement de niveau 2 ?

Non, un hub est un équipement de niveau 1Il reçoit les trames (paquets de la couche liaison) d'un port et les diffusent (broadcast) sur toutes ses sorties. Ce qui est équivalent au répéteur multiport. Tel fonctionnement est mauvais du point de vue sécurité et utilisation des média (réservation inutile de ressource).

3.2- Ethernet
Que signifient les points suivants d'Ethernet ?
- accès avec écoute préalable en compétition (CSMA)
- détection de collisions (CD)

CSMA/CD (Carrier Sense Multiple Acces with Collision Detection) : Transmission partagée de données utilisant une méthode d'accès aléatoire coupant la transmission lors de la détection d'une collision, et la reprenant ensuite après une temporisation aléatoire. Avant de transmettre une donnée, le réseau est testé. Si la voie est libre, la transmission commence. Si une autre information arrive (collision), la transmission s'interrompt et recommence plus tard.

3.3- commutateur (switch)
Quel est le rôle d'un commutateur ?
Le commutateur reçoit les trames d'un port et les envoies juste vers le port connectant avec la destination correspondante en basant sur son adresse MAC (étant donné que la destination est situé localement) ; sinon, les trames vont être envoyé au gateway. Donc, le commutateur fait de routage au niveau liaison en disposant d'une table de routage contenant les adresses MAC et les sorties correspondantes. Ceci permet à un meilleur accès au média (bande passante dédiée, moins de conflits d'accès, collisions réduites).

3.4- WiFi
La norme WiFi 802.11 définit trois couches basses, alors que le modèle standard OSI n'en a que deux (physique et liaison). Est-ce incompatible ?

Les sous-couches LLC et MAC de la couche liaison correspondent à ces couches basses 802.11, avec la couche physique cela fait 3...

4- Couches 3 et 4 (généralité)

4.1- Interconnexion
Quel type d'équipement faut-il pour connecter un réseau en bus Ethernet à un réseau en anneau FDDI ?

Un routeur (penser au niveau de couche OSI nécessaire)

4.2- Routeur
Un routeur agit au niveau 4 du modèle OSI. Vrai ou faux ? Pourquoi ?

FAUX. Les routeurs travaillent au niveau 3 du modèle OSI avec comme unité de transmission les paquets.

4.3- TCP/IP
Dans la pile de protocoles TCP/IP, il y-a-t il un protocole de niveau 4 ?

Cette nomenclature en couche est propre au modèle OSI, où TCP se trouve sur la couche 4 (transport), IP étant sur la couche 3 (réseau)

4.4- IP
Est-ce que le protocole IP permet une transmission des données par messages, datagrammes ou paquets ?

Par paquet, il se situe au niveau de la couche réseau.

4.5- Quelques adresses spéciales
Que désigne précisément l'adresse IP 255.255.255.255 ? A quoi sert l'adresse IP 0.0.0.0 ? Et l'adresse 127.0.0.1 ?

C'est l'adresse dite de diffusion. 255.255.255.255 désigne l'ensemble des hôtes du réseau local auquel est relié le noeud qui émet cette adresse.
Sur une table de routage 0.0.0.0 désigne la ligne concernant la passerelle par défaut du réseau.
Elle peut aussi être utilisée dans un appel BOOTP ou DHCP lancé par un noeud pour connaître sa propre adresse IP.
127.0.0.1 est l'adresse IP interne de la machine elle-même, équivalente à localhost

4.6- manipulation de quelques commandes : Les commandes suivantes sont nécessaires pour identifier les paramètres réseau demandés :

- La commande **ipconfig /all** permet d'identifier beaucoup de paramètres réseaux comme par exemple l'adresse IP de ta machine, l'adresse MAC de la machine, l'adresse IP du gateway, l'adresse IP du serveur DNS et le subnet mask.

- La commande **Ping** permet d'envoyer une requête 'ICMP Echo Request' d'une machine à une autre machine. La machine doit répondre par un message 'ICMP Echo Reply'. Cette commande réseau de base permet d'obtenir des informations et en particulier le temps aller-retour entre les deux machines et aussi quel est l'état de la connexion avec la machine destination et son adresse IP.

- La commande **arp** permet d'afficher et modifier les entrées du cache ARP (Address Resolution Protocol), qui contient une ou plusieurs tables permettant de stocker les adresses IP et leurs adresses MAC résolues. À chaque carte réseau Ethernet installée sur l'ordinateur correspond une table distincte.

- La commande **netstat** (Unix) permet de (i) connaître les connexions TCP actives sur la machine sur laquelle la commande et activée, (ii) lister l'ensemble des ports TCP et UDP ouverts sur l'ordinateur, et (iii) obtenir des statistiques sur un certain nombre de protocoles (Ethernet, IPv4, TCP, UDP, ICMP). Utilisée sans aucun argument, la commande netstat affiche l'ensemble des connexions ouvertes par la machine. La commande netstat possède un certain nombre de paramètres optionnels, sa syntaxe est la suivante :
netstat [-a] [-e] [-n] [-o] [-s] [-p PROTO] [-r] [intervalle]

Utilisée avec l'argument -a, la commande netstat affiche l'ensemble des connexions et des ports en écoute sur la machine.
Utilisée avec l'argument -e, la commande netstat affiche les statistiques Ethernet.
Utilisée avec l'argument -n, la commande netstat affiche les adresses et les numéros de port en format numérique, sans résolution de noms.
Utilisée avec l'argument -o, la commande netstat détaille le numéro du processus associé à la connexion.
Utilisée avec l'argument -p suivi du nom du protocole (TCP, UDP ou IP), la commande netstat affiche les informations demandées concernant le protocole spécifié.
Utilisée avec l'argument -r, la commande netstat permet d'afficher la table de routage.
Utilisée avec l'argument -s, la commande netstat affiche les statistiques détaillées par protocole.

Enfin un intervalle optionnel permet de déterminer la période de rafraîchissement des informations, en secondes. Par défaut ce paramètre vaut 1 seconde.

Questions

*4.6.1- Depuis votre PC, faire un **ping** sur 134.59.1.7, puis examinez le cache **arp**, quelle est l'adresse physique de la passerelle entre les deux sous-réseaux ?*

```
C:\> ping 134.59.1.7
C:\> arp -a
Adresse Internet      Adresse physique      Type
  134.59.2.254         08-00-20-b0-8a-65     dynamique
```

4.6.2- Effectuez un ping sur une machine du réseau local ne figurant pas dans votre cache arp. Que constatez-vous sur les temps de réponse ? Comment l'expliquez-vous ?

```
$ ping 134.59.1.8
PING 134.59.1.8: 56 data bytes
64 bytes from 134.59.1.8: icmp_seq=0  ttl=255  time=9.304.ms
64 bytes from 134.59.1.8: icmp_seq=1  ttl=255  time=6.089.ms
64 bytes from 134.59.1.8: icmp_seq=2  ttl=255  time=6.079.ms
64 bytes from 134.59.1.8: icmp_seq=3  ttl=255  time=6.096.ms
^?
----134.59.1.8 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
```

```
round-trip  min/avg/max = 6.079/6.880/9.304

Le premier RTT est plus long que les suivants : cela est probablement dû à la requête
ARP et sa réponse.
```

5- Protocole IP (Internet Protocol)

5.1- Interface IP

5.1.1- Quels sont les éléments d'une interface IP pour une machine connectée à l'Internet ?

- une adresse IP
- une adresse IP de la passerelle par défaut
- un masque de sous-réseau sur lequel appartient la machine
- un algorithme de routage utilisant le protocole ARP (Address Resolution Protocol)

5.1.2- Soit 5 stations reliées à un dispositif d'interconnexion, considérons les adresses MAC et IP suivantes :

	POSTE 1	POSTE 2	POSTE 3	POSTE 4	POSTE 5
MAC	0028AF86CE51	0028AF86CF51	0028AFG6CD51	0028AF86CFF1	0028AF86CD1
IP	126.0.0.128	126.0.0.213	126.0.0.317	126.0.0.244	126.0.0.099

Relevez les 2 adresses MAC et l'adresse IP erronées, indiquez pourquoi elles le sont.

Les adresses MAC erronés sont celles indiqués pour le poste 3 (pas de lettre G dans la représentation hexadécimal) et le poste 5 (contenant 11 chiffres hexadécimal).

5.2- Subneting

L'utilisation de sous-réseau (Subnetting) dans un réseau IP permet de diviser un gros réseau unitaire en ce qui apparaît comme plusieurs sous-réseaux. Pour identifier le sous réseau, on utilise le masque de sous-réseau qui est une adresse de 32 bits contenant des 1 aux emplacements des bits qui sont réservées pour identifier le sous-réseau et des 0 pour la partie identifiant les hôtes. Une fois ce masque créé, il suffit de faire un ET (logique) entre l'adresse IP d'un host et le masque pour identifier l'adresse IP du sous-réseau où ce host appartient.

Considérons le réseau 131.107.0.0, une station de ce réseau ayant l'IP 131.107.24.100 avec le masque de sous-réseau 255.255.240.0.
a - Combien de sous-réseaux peuvent être gérés ?
b - Combien de stations peuvent être gérées dans chaque sous-réseau ?
c - A quel sous-réseau appartient la station 131.107.24.110 ?
d - Quel est le numéro de cette station dans les hôtes de ce sous-réseau ?

Dans cet exercice, le réseau de classe B et d'IP 131.107.0.0 est coupé en plusieurs sous-réseaux suivant le masque 255.255.240.0. Comme le réseau est de classe B, alors le masque de ce réseau est 255.255.0.0. Ceci implique que dans le masque de sous-réseaux, les seize 1 des premiers deux octets sont masqués pour représenter le réseau et les quatre 1 du troisième octet (240) sont masqués pour représenter le sous-réseau.
a/ Alors, le masque donné permet d'avoir 14 sous-réseaux dans le réseau 131.107.0.0.
Ceci est compte en calculant le nombre de combinaisons possibles des quatre bits et en éliminant les deux possibilités qui sont les 0000 (l'utilisation de cette combinaison pour représenter un sous-réseau aboutit à avoir l'adresse de ce sous-réseau identique à celui du réseau) et 1111 (l'utilisation de cette combinaison pour représenter un sous-réseau aboutit à avoir l'adresse de broadcast de ce sous-réseau identique à celui du réseau).

b/ Le nombre de zéro dans le masque nous indique le nombre de bits qui sont réservées pour l'identification des hôtes. Alors, on a dans ce cas 12 bits qui permettent d'avoir 4094 hôtes (2^{12} - 2) dans chaque sous-réseau.

c/ Pour la caractérisation du sous-réseau de l'IP donné (131.107.24.110), il faut appliquer le ET logique entre la valeur binaire de cet IP et la valeur binaire de l'IP de masque comme on a déjà indiqué. On obtient l'identificateur de sous-réseau de l'IP donné, qui est 0001, en lisant les bits qui sont à l'emplacement réservé pour l'identification de sous-réseau.

d/ On déduit aussi l'identificateur du host, qui est 2158 (100001101110), en lisant les bits qui sont à l'emplacement réservé pour la présentation des hôtes.

5.3- DNS

Le système DNS permet de servir de la résolution de noms de domaines (ou résolution d'adresses).

- La commande **hostname** pour trouver le nom symbolique de votre machine
- La commande **traceroute/ tracert** est un outil réseau qui permet de suivre le chemin qu'un paquet de données (paquet IP) va prendre pour aller d'une machine A à une machine B.

*Depuis votre PC, utilisez la commande **tracert** pour trouver le chemin emprunté pour atteindre taloa.unice.ft puis pour trouver le chemin emprunté pour atteindre une autre machine par exemple itanic.unice.fr. Analysez le résultat obtenu.*

```
C:\> tracert taloa.unice.fr
```

Les chemins sont différents

Par défaut, le paquet est envoyé sur Internet mais le chemin emprunté par le paquet peut varier, en cas de panne d'un lien (les protocoles de routage comme BGP calculent alors un nouveau chemin) ou bien en cas de changement des connexions d'un des opérateurs (connexion à un nouveau point d'échange, par exemple).
Après avoir été expédié au fournisseur d'accès, le paquet est transmis à des routeurs intermédiaires qui vont l'acheminer jusqu'à sa destination. Le paquet peut subir des transformations lors de son voyage. Il se peut aussi qu'il n'arrive jamais à destination si le nombre de noeuds intermédiaires est trop important.
Le principe de fonctionnement de Traceroute consiste à envoyer des paquets UDP (certaines versions peuvent aussi utiliser TCP ou bien ICMP avec des paquets ECHO Request, type 8) avec un TTL de plus en plus grand (en commençant à 1). Chaque routeur recevant un paquet IP en décrémente le TTL. Lorsque le TTL atteint 0, le routeur émet un paquet ICMP d'erreur (type 11, code 1). Traceroute découvre ainsi les routeurs de proche en proche.
Pour bien interpréter le résultat de traceroute, il faut garder en tête que :
- le chemin suivi par les paquets peut être asymétrique et traceroute ne montre que l'aller,
- traceroute est effectué depuis un point de l'Internet (votre machine) et peut être radicalement différent depuis un autre point, même proche (d'où l'intérêt du site traceroute.org),
- un routeur peut ne pas répondre aux requêtes ICMP. Dans ce cas, on voit généralement des signes astérisques (*) sur les noeuds intermédiaires qui ne répondent pas aux requêtes ICMP.
Sous Windows, on utilise l'utilitaire tracert. Un outil similaire est disponible sur les stations Unix avec traceroute. Les chemins joignant votre machine à un ensemble des destinations contiennent souvent au moins un routeur en commun. Alors, quand on utilise les mesures de traceroute pour déduire l'arbre IP joignant votre machine vers certaines destinations, il faut filtrer les routeurs communs entre les différents chemins mesurés.