

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

1.1- Rappel du codage binaire

1. Rappel 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	1010110101010110011110111						
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

$$1 \times 16^6 + 5 \times 16^5 + 10 \times 16^4 + 10 \times 16^3 + 12 \times 16^2 + 15 \times 16^1 + 7 \times 16^0 = 22719735$$

Questions

1.1.1- Conversion en binaire :

- a. $(125)_{10} =$
- b. $(92)_{10} =$
- c. $(27)_{10} =$
- d. $(203)_{10} =$
- e. $(255)_{10} =$

1.1.2. Conversion en décimal :

- a. $(0000\ 0110)_2 =$
- b. $(0110\ 0101)_2 =$
- c. $(1000\ 1110)_2 =$
- d. $(1010\ 1111)_2 =$

e. $(1100\ 0000)_2 =$

1.1.3. Conversion en décimal :

- a. $(A1)_{16} =$
- b. $(F2)_{16} =$
- c. $(E2A)_{16} =$
- d. $(3B)_{16} =$
- e. $(14D)_{16} =$

1.1.4. Conversion en binaire :

- a. $(1F)_{16} =$
- b. $(2C)_{16} =$
- c. $(9E)_{16} =$
- d. $(3B)_{16} =$
- e. $(B6)_{16} =$

1.2- Modes de transmission

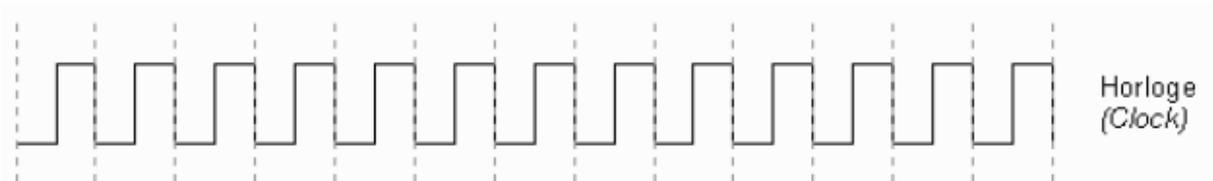
1.2.1- Quelles sont les différences principales entre un réseau de transmission de circuit et un réseau de transmission à commutation par paquets ?

1.2.2- Circuit virtuel

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

2- Couche physique (codage Manchester 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 ?

3- Couches de liaison (et physique)

3.1- Hub

- Un hub permet-il de filtrer des paquets dynamiquement ?
- Un hub est-il un équipement de niveau 2 ? pourquoi ?

3.2- Ethernet

Que signifient les points suivants d'Ethernet ?

- accès avec écoute préalable en compétition (CSMA)
- détection de collisions (CD)

3.3- commutateur (switch)

Quel est le rôle d'un commutateur ?

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 ?

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 ?

4.2- Routeur

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

4.3- TCP/IP

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

4.4- IP

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

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 ?

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 est 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

4.7.1- 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 ?

4.7.2- 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 ?

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 ?

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

	<u>POSTE 1</u>	<u>POSTE 2</u>	<u>POSTE 3</u>	<u>POSTE 4</u>	<u>POSTE 5</u>
<u>MA</u>	0028AF86CE	0028AF86CF	0028AFG6CD	0028AF86CF	0028AF86C
<u>C</u>	51	51	51	F1	D1
<u>IP</u>	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.

5.2- Subnetting

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 ?

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 **tracroute/ 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 *taloo.unice.fr* puis pour trouver le chemin emprunté pour atteindre une autre machine par exemple *itanic.unice.fr*. Analysez le résultat obtenu.