

Note N°2-TCP/IP

Réseau ethernet-couche internet

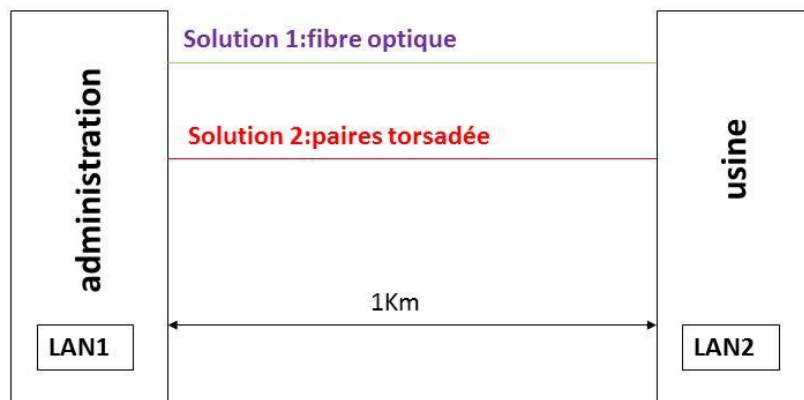
1. Résumé :

Technologie	Débit	Longueur maximale
Paire torsadée	10Mb/s;100Mb/s;1Gb/s	100m (le coût est variable)
Fibre optique	1Gb-10 Gb	2,5 Km
Sans fil	54Mb/s-100Mb	100m de rayon de couverture

2. Réseau ethernet :

Exercice illustratif :

On veut réaliser un câblage pour une usine constituée de deux réseaux LAN : un pour l'administration et l'autre dans la partie usine. Les deux emplacements sont distants d'1Km.



Si on veut un débit de 1Gb/s, deux choix sont possibles : la paire torsadée et la fibre optique.

- **La fibre optique :**

Pas d'escale, l'information passe de bout en bout directement.

- **Paire torsadée :**

On doit avoir 9 répéteurs + prise en considération du coût d'électricité nécessaire pour alimenter les répéteurs.

- ➔ On doit faire une étude comparative (étude technique et économique)
- ➔ Si on considère le coût de déploiement de la paire torsadée, ce coût dépasse largement le coût de la fibre optique.
- ➔ La fibre optique est donc la meilleure solution.

Le réseau ethernet :

Repose sur une technique aléatoire, prend en charge la gestion des collisions. L'entête d'une trame ethernet est composée des adresses sources et destination. L'adressage est un élément très important qui apparaît dans chaque couche du modèle. Selon la couche, l'adressage change.

Par exemple, au niveau couche application, l'adressage se réfère à des noms car plus pratiques. (exp :www.google.com).

Nom	Couche application
N° du port	Couche transport
Adresse IP	Couche IP
Adresse MAC	Couche physique

- **La nécessité de l'adressage IP :**

L'adresse MAC ne permet pas de distinguer les machines appartenant au même réseau ou qui appartiennent à des réseaux différents. Ce manque d'organisation des machines entre elles donne à l'adressage IP toute sa raison d'être. Le rôle de l'adressage MAC est restreint au plus bas niveau (niveau physique), alors que l'adressage IP permet de dire si deux machines appartiennent au même réseau. Si l'adressage IP n'a pas été développé, on aurait resté prisonnier du constructeur, car seules les machines fabriquées par un même constructeur pourraient éventuellement communiquer.

- **Règle d'art pour la mise en œuvre d'un réseau :**

Cette règle s'appelle « règle de 5-4-3 », c'est une norme de câblage qui a résulté de l'expérience dans le domaine et qui fixe 3 critères pour le bon fonctionnement d'un réseau, à savoir :

- ➔ 4 : quatre répéteurs au maximum.
- ➔ 5 : cinq segments au maximum.
- ➔ 3 : 3 segments peuplés (c'est-à-dire qui contiennent des machines).

Si on considère cette règle, alors la solution retenue dans l'exemple précédent (câblage de l'usine) est confirmée.

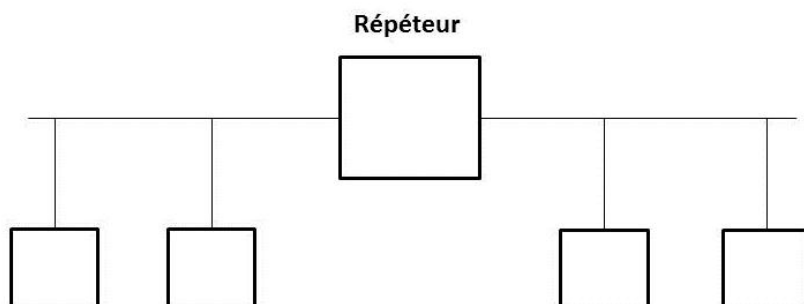
Les missions les plus importantes de l'ingénierie réseaux sont la réduction des collisions et des broadcasts. Les collisions provoquent une perte de temps, car il y a besoin de retransmettre l'information si une collision se produit, et les broadcasts provoquent la transmission d'informations qui peuvent être inutiles.

- **Définitions :**

- 1. Domaine de collision :**

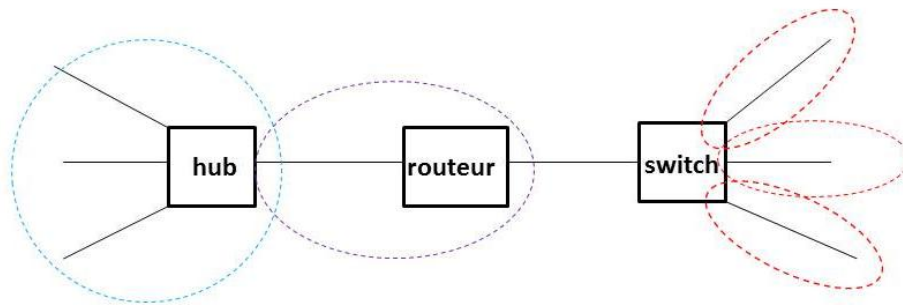
c'est un support partagé sur lequel sont connectées des machines qui peuvent entrer en collision.

Le répéteur, répétant le signal, augmente obligatoirement le domaine de collision, alors que les switches et les routeurs permettent la séparation. En effet, en utilisant un répéteur, quand une station transmet, les autres stations doivent écouter. Il n'y a donc pas de communication parallèle de part et d'autre d'un répéteur.



Le schéma ci-dessus présente un seul domaine de collision.

Exemple :



Le schéma ci-dessus présente 6 domaines de collision. Il est à noter que chaque port d'un switch constitue un domaine de collision à part.

2. Domaine de broadcast :

Le broadcast est une transmission qui doit être toujours effectuée. Le routeur est le seul équipement permettant d'arrêter le broadcast. Le broadcast doit rester en local, au niveau du LAN.

- **Fonctions d'un switch :**

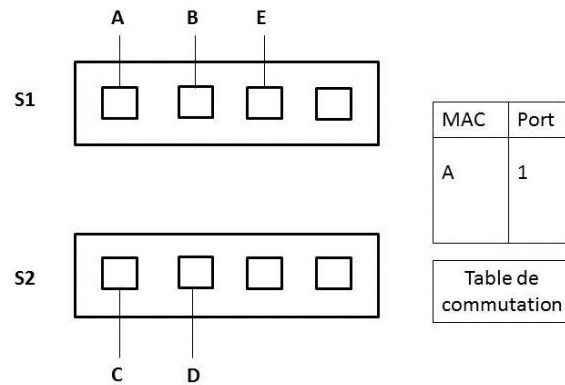
Le switch a deux fonctions principales : le filtrage et l'apprentissage.

➔ Le filtrage : c'est l'analyse avant la transmission du message.

➔ L'apprentissage : le filtrage est basé sur l'apprentissage. Si le mécanisme d'apprentissage n'était pas présent, alors il n'y aurait pas de filtrage.

L'apprentissage consiste à construire dynamiquement une table de commutation contenant les correspondances entre les adresses MAC et les ports de communication.

Exemple illustratif :



Initialement la table de commutation est vide. Quand A ping sur B, S1 détecte cette commande sur le port 1. Le switch identifie la machine source et inscrit dans la table l'entrée correspondante : A → 1. Ensuite, il identifie le destinataire (ici B). s'il ne reconnaît pas, c'est-à-dire s'il n'y a pas d'entrée correspondante dans la table, le switch envoie un broadcast à toutes les stations, mais seule B pourra répondre et consommer le message. Le broadcast dans ce cas est pertinent car il favorise l'apprentissage sans que les machines non destinataires ne consomment le message.

Quand B répond, il est également inscrit dans une nouvelle entrée de la table. Lors d'une deuxième transmission à B, le switch exerce un filtrage du message qu'il transmet directement au destinataire. C'est pour cela que le filtrage dépend de l'apprentissage.

L'information qui entre dans les switches est dynamique. Il y a nécessité de renouvellement d'apprentissage quand il y a risque d'incohérence des données, par exemple quand une machine est débranchée ou quand deux machines sont permutées. À ce moment les entrées correspondantes sont effacées de la table.

3. Couche internet :

Cette couche se charge du routage et de l'adressage. L'adressage repose sur un classement en 5 classes d'adresses IP.

Classes d'adressage :

- ➔ les classes A, B et C d'utilisation. Ces classes étaient utilisées pour connecter des réseaux à internet, et non pas des personnes.

- ➔ la classe D de multicast(n'identifie pas le réseau mais adresse le groupe (le groupe est identifié par une seule adresse IP affectée à une machine pour offrir un service supplémentaire.

Commandes utiles :

Ping 127.0.0.1	Tester si la carte réseau est bien configurée
Ping sur un voisin local	Tester la connectivité LAN
Ping sur une machine distante	Tester la connectivité WAN

Si la dernière commande marche, on est sûr que les deux premières marchent aussi. Sinon, il serait difficile d'identifier la source du problème.

Masque :

Fonctions du masque	Illustration
1. identifier le réseau auquel appartient une machine donnée.	
2. Savoir si un destinataire est local ou bien distant.	<p>Si A veut communiquer avec B, alors A doit tester la localité de B, en comparant <i>IPA & masqueA</i> et <i>IPB & masqueA</i> .</p> <p>Si égalité, A envoie à B physiquement (adresse MAC du destinataire=adresse MAC de B)</p> <p>Sinon,(B est distant), l'adresse MAC du destinataire est l'adresse de la passerelle par défaut de A (le passage par un routeur est obligatoire)</p>
3. Segmenter un réseau en sous-	

réseaux.	
4. Chercher une route dans la table de routage.	

Le protocole ARP :

Le protocole ARP est un protocole qui fait la correspondance ou le mapping entre les adresses IP et les adresses MAC.

Considérons le scénario suivant, ou A veut envoyer un ping sur B. l'adresse IP source est celle de A, et de destination est celle de B.

Si on descend à la couche physique, on doit connaître les adresses MAC de A et B. or l'adresse MAC de B n'est pas connu, donc ARP est appelé pour trouver l'adresse MAC de B. pour ce faire, il envoie un broadcast et répertorie les correspondances construites de cette manière dans son cache. Ce cache est dynamique. Son utilité réside dans le fait qu'il permet de réduire les broadcasts et donc d'accélérer les performances du système, en cherchant l'information localement.

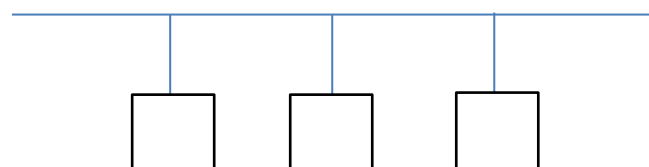
Le concept de cache est presque présent dans tous les protocoles de communication, par exemple, le cache web qui permet d'accélérer l'accès à internet.

NB : le protocole ARP n'est valable qu'en local.

l'adressage dynamique et le protocole DHCP :

DHCP permet la configuration des adresses IP de manière dynamique. Ceci permet de réduire le taux d'erreur dans la configuration manuelle.

Pour montrer l'utilité de DHCP, on considère la configuration suivante :



IP :10.1.1.1

IP :10.2.2.2

Masque :255.0.0.0

masque : 255.255.0.0

$IP_A \&\& masque_A = IP_B \&\& masque_A$, A a l'impression que B est local donc elle envoie le ping à l'adresse MAC de B. or du côté B,

$IP_B \&\& masque_B \neq IP_A \&\& masque_B$, donc B ne répond pas au ping de A, et la communication est impossible globalement (quoique possible de A vers B).

Un autre scénario est quand B n'est pas locale.

