Support de cours sur les réseaux informatiques

Dr Nadjia Khatir

Dr Abdelkader Belhadri

2020/2021

Avant-propos

La mise en place d'un réseau local ou longue distance peut être d'un grand intérêt technique au profit des utilisateurs. En effet, les domaines impactés sont très nombreux citons par exemple : dans l'entreprise, les réseaux informatiques permettent de partager des ressources matérielles (scanners, imprimantes, etc.) ou logicielle (base de données). Dans le domaine du commerce, les réseaux sont utilisés pour la vente par correspondance sur Internet. La science exploite aussi les réseaux pour le calcul réparti ; la télémédecine et le partage des connaissances grâce aux encyclopédies en ligne et l'enseignement à distance. Enfin l'utilisation des réseaux contribue dans la société via les réseaux sociaux.

Ce cours sur les réseaux informatiques est destiné aux étudiants de l'Ecole Supérieure en Génie Electrique et Energétique d'Oran (ESG2E). Il correspond au premier semestre du programme du module « Informatique » enseigné en deuxième année du cycle de spécialité.

Le polycopié est structuré autour de cinq chapitres. Le premier chapitre présente des généralités sur les réseaux informatiques, les différents types de réseaux et les supports de communication. Il est suivi du deuxième concernant les aspects théoriques du fonctionnement d'un réseau basés sur l'architecture en couches. Dans le troisième chapitre nous parcourons les différentes techniques de transmission des données numériques, les codages et les débits de transmissions. Le quatrième chapitre aborde les différentes méthodes de détection des erreurs de transmission. Finalement, le cinquième chapitre présente les domaines de collision et de diffusion.

Le polycopié comporte également une série d'exercices d'application intégrés au cours avec dont l'objectif est de permettre à l'étudiant de comprendre comment les concepts réseaux sont réellement mis en œuvre et de bien retenir les informations apprises.

Table des matières

Table des figures

Chapitre 1

Généralités sur les réseaux informatiques

Sommaire

1.1 Qu'est-ce qu'un réseau informatique ?

Un réseau informatique est un ensemble d'équipements (ordinateurs portables ou fixes, routeur, switch, etc.), situés à distance les uns des autres et reliés entre eux par des liaisons filaires (câbles) ou sans fils permettant aux utilisateurs de partager des ressources matérielles et logicielles.

1.2 Objectifs des réseaux informatiques

1. **Partage des ressources :** rendre accessible à chacun les données, les programmes et équipements indépendamment de leur situation physique par rapport à l'utilisateur.

   Exemple de ressources : fichiers, procédures, bases de données, logiciels, périphériques.
2. **Réduction des coûts :** plusieurs petits ordinateurs reviennent moins chers que de gros serveurs à performance égale.
3. **Communications entre les personnes :** par exemple les réseaux sociaux et la messagerie électronique.
4. **Travail coopératif :** des personnes éloignées géographiquement peuvent travailler et collaborer ensemble plus facilement.

1.3 Les composants de base d'un réseau

La mise en œuvre d'une communication entre deux ou plusieurs nœuds dans un réseau nécessite la mise en place de 3 types de composants :

1. **Les supports de transmission :** sont tout moyen permettant de transporter des données sous forme de signaux de leur source vers leur destination ;
2. **Les équipements d'interconnexion :** servent à connecter plusieurs machines entre elles, comme : les cartes réseaux, les switchs, les routeurs, les modems, etc ;

3. **Les protocoles de communication :** sont des règles établies entre l'émetteur et le récepteur des données.

1.4 Les différents types de réseaux

Selon le rayon de couverture géographique ainsi que le débit qu'ils peuvent atteindre, les réseaux peuvent être classés en quatre catégories : PAN, LAN, MAN, WAN.

PAN (Personal Area Natwork)

Un réseau personnel, interconnecte (souvent par des liaisons sans fil) des équipements personnels comme un ordinateur portable, une souris, un clavier, un agenda électronique, etc. Aujourd'hui, nous parlons, des réseaux domestiques (smart home), l'idée de base de ces réseaux est de faire communiquer des appareils des habitations et les rendre accessibles via Internet. Beaucoup d'appareils peuvent être interonnectés, tels que les appareils ménagers (micro-ondes, réfrigérateur, climatiseurs), les systèmes de télésurveillance (alarmes de vol et incendie, capteurs d'eau, thermostats,etc) [4].

LAN (Local Area Network)

S'étendant sur quelques dizaines à quelques centaines de mètres, le Local Area Network (LAN), en français Réseau local d'entreprise (RLE), sont utilisés principalement pour relier les ordinateurs personnels ou les stations de travail que l'on trouve dans les entreprises à des ressources partagées avec les quelles ils échangent des informations.

Les LANs sont de taille restreinte, mais leur débit de transmission est élevé. En effet, la plus part des réseaux locaux prenaient en charge des débits de 10 Mbits/s (10Base-T) et 100 Mbits/s (Fast Ethernet). Avec l'apparition de la nouvelle génération de produits multimédias : images et vidéos, les données ont submerger le réseau Ethernet assurant des débits classiques. D'où l(apparition des nouvelles interfaces réseau : Gigabit Ethernet (100Base-T)

ayant un débit de 1000 Mbits/s et aujourd'hui, il y a eu même 10 et 100 Giga-Ethernet (10 ou 100Gb/s).

Voici quelques caractéristiques des réseaux locaux :

- ◇ La courte distance entre les noeuds ($< 10km$).
- ◇ Un débit de transmission élevé : allant de 10 Mbit/s jusqu'à 100 Gbit/s.
- ◇ Un faible taux d'erreur de transmission.
- ◇ Plus sécurisé, vu la nature privée du réseau.

MAN (Metropolitan Area Network)

Le réseau Métropolitain Area Network (MAN) est également nommé réseau fédérateur. Il assure des communications sur des plus longues distances, interconnectant souvent plusieurs réseaux LAN, Il peut servir à interconnecter, par exemple, différents bâtiments distants de quelques dizaines de kilomètre.

WAN (Wide Area Network)

Les étendues de réseaux les plus conséquentes sont classées en Wide Area Network (WAN). Constitué de réseaux de type LAN, voire MAN, les réseaux étendus sont capables de transmettre les informations sur de milliers de kilomètres à travers le monde entier. Le WAN le plus célèbre est le réseau public internet dont le nom provient de cette qualité : Inter Networking ou interconnexion de réseaux.

1.5 Les supports de transmission

Nous appelons support de transmission tout moyen permettant de transporter des données sous forme de signaux de leur source vers leur destination.

Il existe deux types de supports :

1. **Les supports filaires :** la paire torsadée, le câble coaxial, la fibre optique ;
2. **Les supports sans fils :**tels que les ondes électromagnétiques.

1.5.1 Les supports filaires

Les principaux supports de transmission filaires utilisés dans les réseaux locaux sont les suivants : la paire torsadée, le câble coaxial et la fibre optique.

1.5.1.1 La paire torsadée

Le Câble à paires torsadées(voir la Figure 1) est actuellement le support physique le plus utilisé. Il est constitué de plusieurs fils de cuivre, torsadés par paires, ces paires sont eux même torsadées entre elles. Un câble peut regrouper de une à plusieurs paires torsadées.

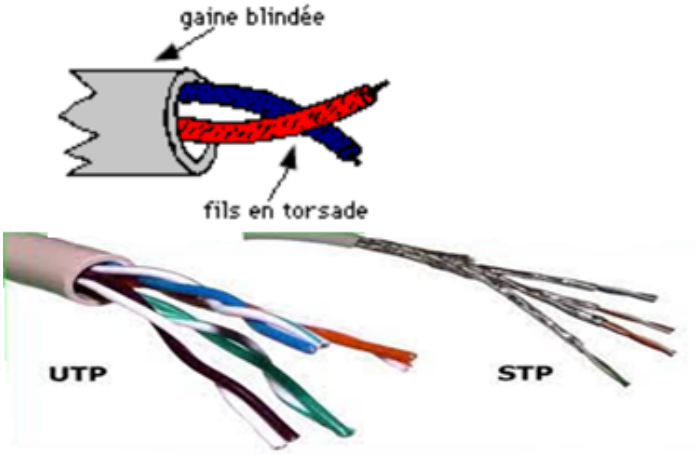


FIGURE 1 – La paire torsadée (STP et UTP).

Les connecteurs appropriés à ce type de câbles sont les connecteurs RJ-45 pour 4 paires et RJ-11 pour 2 paires (voir la Figure 2) :

Il existe des versions blindées (STP Shielded Twisted Pair) Et non blindées (UTP Unshielded Twisted Pair), Voici une comparaison entre la paire UTP et STP :

1.5.1.2 Le câble coaxial

Constitue une amélioration de la paire torsadée. C'est un câble électrique constitué de deux conducteurs à symétrie cylindrique de même axe, séparés

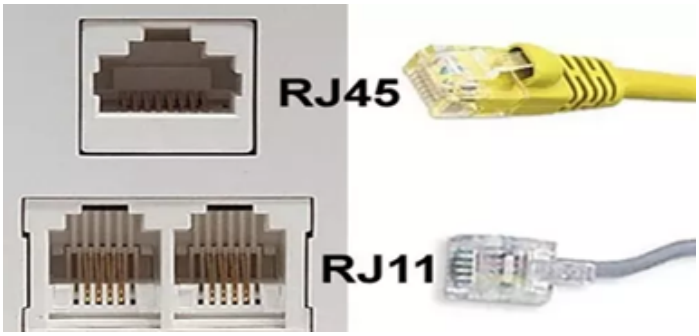


FIGURE 2 – Les connecteurs de paires torsadées.

Shielded (STP)	**Unshielded (UTP)**
-Vitesse : 10-1000 Mbits/s	-Vitesse : 10-1000 Mbits/s
-Longueur max : 100 m	-Longueur max : 100 m
-Raccordement : connecteur RJ-45	-Raccordement : connecteur RJ-45
-Impédance : 100 Ohms	-Impédance : 100 Ohms
-Coût : moyennement cher	-Coût : faible.
-Fournit une meilleur protection.	-Plus utilisé dans les LAN.

par un isolant. Le premier est un conducteur cylindrique creux de rayon R2, l'autre est central de rayon R1 appelé l'âme. Malgré de bonnes qualités intrinsèques (faible sensibilité aux perturbations électromagnétiques), voir la Figure 3 ,les câbles coaxiaux sont de moins en moins utilisés et laissent de plus en plus la main aux paires torsadées.

Ils sont utilisés dans des infrastructures longue distance et les réseaux de télévisions. Ils ont les caractéristiques suivantes :

- ◇ Vitesse : 10-100 Mbits/s.
- ◇ Longueur max : 500 m.
- ◇ Raccordement : connecteur BNC.
- ◇ Impédance : 150 Ohms.
- ◇ Coût : peu cher.

1.5.1.3 Fibre optique

C'est un fil dont l'âme (cœur) est en verre ou en plastique très fin (silicium) et qui a la propriété de conduire la lumière. Les bits sont codés sur

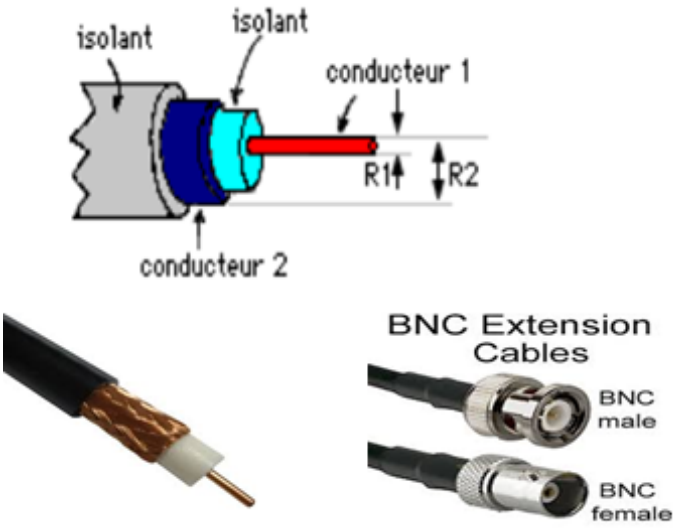


FIGURE 3 – Le câble coaxial.

la fibre sous forme d'impulsions lumineuses. Le câble à fibre optique sert à guider les ondes qui transmettent dans le centre de la fibre appelé cœur, voir la Figure 4. Les rayons entrants dans la fibre subissent des réflexions et se propagent jusqu'à l'autre extrémité. Une fibre optique transmet les données dans un seul sens, ainsi, deux fibres sont nécessaire : une pour la transmission et l'autre pour la réception.

Les connecteurs fibre optique (ST (Straight Tip), SC (Subscriber Connector)) sont des dispositifs terminant une fibre optique et permettant de les raccorder aux équipements terminaux comme les switchs.

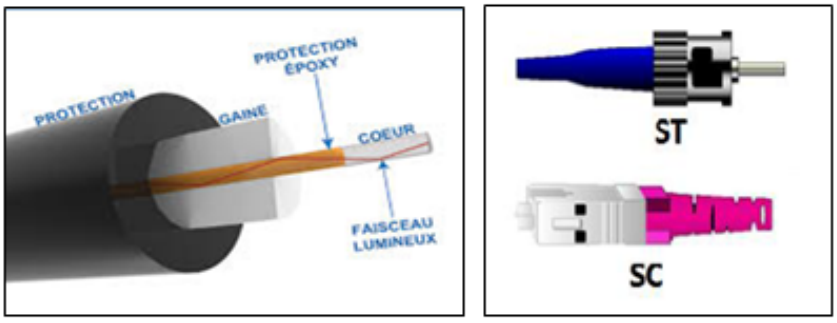


FIGURE 4 – La fibre optique.

Voici quelques caractéristiques de la fibre optique :

◇ Vitesse : +100 Mbits/s ;

◇ Longueur max : jusqu'à 220 Kms ;

◇ Raccordement :(ST(Straight Tip), SC(Subscriber Connector)) ;

◇ Coût : Le plus cher.

Une fibre optique transmettant un seul rayon est appelée fibre monomode, et fibre multimode lorsqu'elle transmet plusieurs rayons dans son cœur.

1.5.2 Les supports sans fils

Certains milieux comme l'aire et le vide permettent la transmission des ondes électromagnétiques, ces dernières sont utilisées par les réseaux sans fils comme supports de transmissions. Les caractéristiques principales d'une onde électromagnétique sont :

◇ La fréquence : mesurée Hertz (Hz).

◇ La longueur d'onde (portée) : mesurée en mètre.

◇ Le débit : mesuré en bits/s.

Ainsi, les supports sans fils sont classés en plusieurs familles selon la fréquence et la longueur d'onde qui les caractérisent, voir la Figure 5.

La technologie Wi-Fi (IEEE 802.11x) où x désigne les différentes variantes comme : 802.11a, 802.11b, 802.11g,etc. Elle s'opère dans la bande de fréquences de 2,4 ou 5 GHz et permet de relier des équipements informatiques dans un réseau sans fil haut débit. Les vitesses de connexion varient selon la norme 802.11 utilisée avec des portés de communication de plusieurs centaines de mètres.

La technologie de la téléphonie mobile ou cellulaire(GSM, 3G) emploi des fréquences autour de 900 MHz et permettent des communications à plusieurs dizaines de kilomètres en plus de la 3G+ et 4G qui sont des technologies cellulaires employées de nos jours.

Nous ajoutons à ces exemples les technologies de courte portée telles que :

◇ Bluetooth, permet les transmissions à faible distance ;

- ◇ Zigbee est utilisée par certains capteurs tels que les détecteurs de fumée ;
- ◇ Near Field Communication (NFC) pour les objets équipés d'une puce électronique RFID.

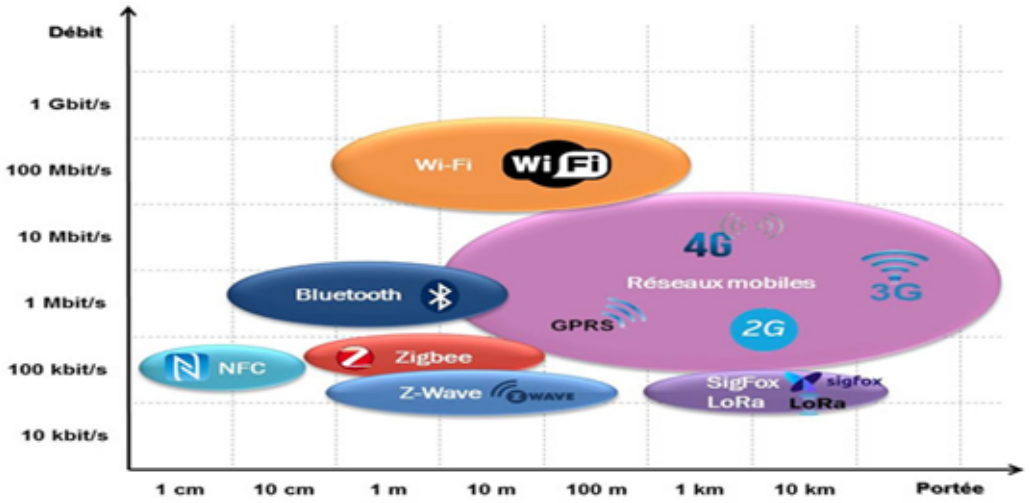


FIGURE 5 – Les technologies sans fils.

1.5.3 Autres supports : les CPL

Nous pouvons citer également la technologie des courants porteurs en ligne (CPL) comme un autre support de communication qui ne fait pas partie des réseaux informatiques classiques mais qui est utilisée dans le domaine de la domotique. Elle permet de transmettre des données numériques (binaires) sur une ligne électrique de courant porteur : le 220V, elle constitue une innovation la plus récente. Le CPL est un second courant transmis sur la même ligne en utilisant autres fréquences éloignées de la ligne électrique domestique allant de 1.6 MHz à 30 MHz. La standardisation du CPL par IEEE est le homeplug.

FIGURE 6 – Une prise de CPL.

1.6 La technologie Ethernet

1.6.1 Présentation

Ethernet est une technologie et un protocole universel de réseaux locaux qui a été développé bien avant Internet entre 1973 et 1975 par la société Xerox Parc [7]. Les réseaux Ethernet s'articulent autour d'un bus de diffusion par analogie avec les réseaux de distribution d'eau ou gaz ou de télévision. A l'époque, le support de communication était des câbles coaxiaux. Désormais, Ethernet est utilisée sur paires torsadées pour la connexion des postes clients, le cable coaxial a été remplacé par des hubs (concentrateurs) puis des switchs (commutateurs), ainsi que des versions sur fibre optique. Cette configuration a largement influencé les topologies, d'ou l'apparition d'autres standards comme le Token Ring et le FDDI. Finalement, ces dernières années sont apparues des variantes sans fil d'Ethernet (la norme IEEE 802.11x)pour le Wi-Fi.

1.6.2 Spécification des câbles

La section ci-dessous donne des exemple de types de média d'Ethernet suivant le type et le diamètre des câbles utilisés :

- **10Base2** : est un réseau utilisant un câble coaxial fin (ainsi appelé thin Ethernet) avec connecteurs BNC en T. Il est capable de transférer des

données à un débit allant jusqu'à 10 Mbits/s. Cependant comme les connecteurs affaiblissent le signal, on ne peut mettre que 30 stations sur le câble [4].

- ◇ **10Base5** : utilise un câble coaxial épais(appelé thick Ethernet), ce qui permet d'augmenter les distances couvertes en remplaçant notamment les connecteurs BNC par des MAU.
- ◇ 10Base-T : Le câble utilisé est une paire torsadée (le T signifie twisted pair), le débit atteint est d'environ 10 Mbps.
- ◇ **100Base-FX** : Permet d'obtenir un débit de 100 Mbps en utilisant une fibre optique multimode.
- ◇ **100Base-TX** : Comme 10Base-T mais avec un débit 10 fois plus (100Mbps).
- ◇ **1000Base-T** : Utilise une double paire torsadée de catégorie 5e et permet un débit d'un Gigabit par seconde.
- ◇ **Ethernet 40GB/s et 100GB/s** : ont été définies en 2010 sous la norme IEEE 802.3ba.
- ◇ **Ethernet 200GB/s et 400GB/s** :ont été définies en décembre 2017 sous la norme IEEE 802.3bs

1.6.3 Structure des trames Ethernet

Les données sont transmises sous forme de trame (frame en anglais) ; Une trame est un bloc de bits organisés en champs qui diffèrent selon le type de la trame. La structure d'une trame Ethernet est décrite dans la Figure suivante 7 :

FIGURE 7 – Structure d'une trame Ethernet.

- ◇ Le champ Préambule : Le champ Préambule à 7 octets et le champ Délimiteur de début de trame (SFD) à 1 octet sont utilisés à des fins

de synchronisation entre les périphériques d'envoi et de réception. Les huit premiers octets de la trame réseau servent à attirer les nœuds de réception. Les premiers octets demandent essentiellement aux récepteurs de se préparer à recevoir une nouvelle trame dans ce réseau informatique.

- ◇ Champ Adresse MAC de destination : Ce champ de 6 octets identifie l'adresse du destinataire concerné.
- ◇ Champ Adresse MAC source : Le champ Adresse MAC source (6 octets) identifie la carte réseau ou l'interface d'origine de la trame. Les commutateurs utilisent cette adresse pour les ajouter à leurs tables de recherche.
- ◇ Champ Longueur/Type : Ce champ de 2 octets définit la longueur exacte du champ de données informatiques de la trame. Ce champ est utilisé par la suite dans le cadre de la séquence de contrôle de trame réseau (FCS) pour s'assurer que le message a été reçu comme il se doit. Si le champ a pour but de désigner un type, le champ Type indique alors quel protocole réseau est mis en place.
- ◇ Champs de données et remplissage : Ces deux champs de 46 à 1 500 octets contiennent des données informatiques encapsulées d'une couche supérieure.
- ◇ Champ Séquence de contrôle de trame : Le champ de séquence de contrôle de trame (4 octets) permet de détecter les erreurs survenues dans une trame réseau.

1.7 Les méthodes d'accès aux supports

Pour que les messages circulent sur le réseau sans se perturber, il faut employer des règles d'accès au support. Ces règles d'accès peuvent être classées en familles de méthodes : les méthodes avec contention et les méthodes méthodes sans contention [7].

1.7.1 Les méthodes avec contention

Dans un accès de type contention, toutes les stations sont à l'écoute du support physique de liaison (câble ou fibre) afin de déterminer si une autre station transmet une trame de données par la détection de surtension électrique ou d'une présence de lumière. Si tel n'est pas le cas (donc s'il n'y a pas de signal), elle suppose qu'elle peut émettre. Cependant, il se peut que deux stations se décident à émettre au même instant, on dit alors qu'il y a contention (collision) des messages émis. En effet, lors d'une collision, le signal électrique sur a ligne va correspondre au cumule des émissions ce qui provoque une surtension. Afin de résoudre ce problème les méthodes avec contention peuvent soit détecter les collisions après coup (la méthode CSMA/CD), ou de les prévenir (la méthode CSMA/CA).

1.7.1.1 La méthode CSMA/CD

La méthode Carrier Sense Multiple Access with Collision Detection est appliquée à une topologie en bus. Rappelons que dans une telle topologie, les stations partagent le même média de communication et qu'il n'y a pas de priorité d'émission. Elle est normalisée par IEEE sous la référence 802.3 et elle est utilisée dans les architectures des réseaux locaux Ethernet (802.3), fast Ethernet (802.3u) et Gigabit Ethernet (802.3Z) et 10 Gigabit Ethernet 802.3ae.

La méthode CSMA/CD suit le processus suivant :

- ◇ La station qui est en cours d'émission surveille tout d'abord le support de transmission (listen before talking).
- ◇ C'est uniquement lorsque le support est libre, que la station émet.
- ◇ Toutefois, la station émettrice continue de surveiller le support de transmission (listen while talking) afin de vérifier si ses données n'ont pas été perturbées (collision). Les adaptateurs des stations émettrices détectent les collisions en comparant ce qu'elles envoient avec le signal présent sur le support. Si les deux signaux sont identiques, alors il n'y a pas eu de collision.

- ◇ Dans le cas contraire, il y a collision et les stations émettrices interrompent leur transmission et envient un signal indiquant la collision (trame de brouillage, bourrage ou trame JAM) afin de prévenir les autres stations de la collision.
- ◇ Elles attendront un délai aléatoire (calculé par l'algorithme BACKOFF) et essaient à nouveau de retransmettre.
- ◇ l'algorithme «backoff exponentiel» fonctionne comme suit : Soit n le nombre de collisions consécutives de la même trame. La station émettrice calcule un nombre entier aléatoire r entre 0 et 2^{n-1}. Avant de retransmettre la trame, la station doit attendre un délai backoff $= r * timeslot$, où timeslot est une durée constante (qui est strictement supérieur à deux fois le temps de propagation maximal entre deux stations du réseau).
- ◇ Le délai d'attendre doit être aléatoire pour chaque station afin que la probabilité que les deux stations émettrices choisissent à nouveau le même moment de transmission faible.

1.7.1.2 La méthode CSMA/CA

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) est utilisée par les technologies des réseaux sans fils de type Wi-Fi (802.11). Elle a pour but de prévenir la contention (collision) plutôt que de la subir. Elle utilise un mécanisme basé sur un principe d'accusé de réceptions et fonctionne comme suit (voir la Figure 8) :

- ◇ La station qui veut émettre commence par écouter si le support est libre (Carrier Sense).
- ◇ Si le réseau est encombré, la transmission est différée.
- ◇ Dans le cas contraire, si le support est libre pendant un temps donné (appelé DIFS : Distributed Inter Frame Space), alors la station peut émettre.
- ◇ La station envoie une petite trame RTS (Ready To Send) à toutes les stations pour leur indiquer son intention de transmettre ses données. La

trame RTS indique : la source, la destination et une durée de réservation de la transmission.

- ◇ La station de destination répond (si le support est libre) par une petite trame de contrôle CTS (Clear To Send) qui reprend ces informations, puis la station commence l'émission des données. A réception de toutes les données émises par la station, le récepteur envoie un accusé de réception (ACK).
- ◇ Toutes les autres stations recevant un RTS ou un CTS doivent attendre la fin de la transmission.
- ◇ Les temporisateurs : le SIFS (Short Inter Frame Space) est utilisé pour séparer les transmissions appartenant à un même dialogue et le DIFS (Distributed IFS) est l'intervalle utilise par une station voulant commencer une nouvelle transmission.
- ◇ Du fait que RTS et CTS sont des trames courtes, le nombre de collisions est réduit puisque ces trames sont reconnues plus rapidement que si tout le paquet devait être transmis.

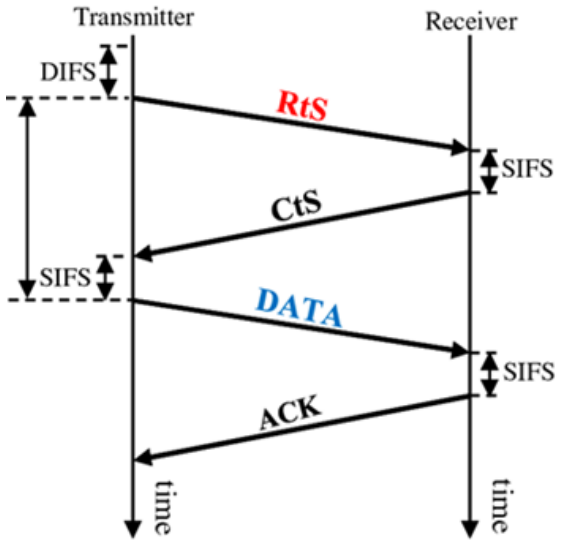


FIGURE 8 – Principe de fonctionnement de la méthode CSMA/CA.

1.7.2 Les méthodes sans contention

Par analogie avec la prise de la parole dans une classe, une organisation particulière est réalisée pour qu'aucune collision ne soit produite. On trouve deux sous-catégories de méthodes sans contention :

- ◇ **TDMA (Time Division Multiple Access)** pour partage le support de communication entre stations, le temps est découpé en périodes eux mêmes découpées en intervalles (appelés time slot. Les communications GSM de téléphonie mobile utilise cette méthode.
- ◇ **FDMA(Frequeny Division Multiple Access)** se base sur un partage de fréquence. Sachant qu'un support de communication a une certaine bande passante, il est possible de la découper en petits intervalles de fréquences et d'allouer chacun des sous canaux crées à une station. L'ADSL utilise la méthode FDMA pour partager la ligne téléphonique entre appels vocaux et données (Internet haut débit).

1.8 Topologies des réseaux

La topologie est la manière dont les ordinateur sans interconnectés dans le réseau. On distingue la topologie physique des réseaux de la topologie logique :

- ◇ **La topologie physique :** est l'arrangement physique ou la configuration spatiale du réseau.
- ◇ **La topologie logique :** représente la façon dont les données transitent dans les supports de communication.

On distingue généralement dans les réseaux les topologies physiques suivantes :

- ◇ Topologie en bus ;
- ◇ Topologie en étoile ;
- ◇ Topologie en anneau ;
- ◇ Topologie en arbre ;
- ◇ Topologie maillée.

Topologie en bus

- ◇ C'est l'organisation la plus simple d'un réseau, voir la Figure 9.
- ◇ Le mot «bus» désigne le segment central où les machines viennent s'y accrocher.
- ◇ Chaque extrémité est terminée par un bouchon.
- ◇ Une seule station peut émettre à la fois.
- ◇ Lorsqu'une station émet des données, celles-ci circulent sur tout le bus , et la station destinataire peut la récupérer.
- ◇ Le média utilisé est un câble coaxial fin (fil de cuivre).
- ◇ Débit : 10 Mbits/s.
- ◇ Longueur : 185 m max.
- ◇ La norme utilisée est l'Ethernet 10BASE2 ou 10BASE5.

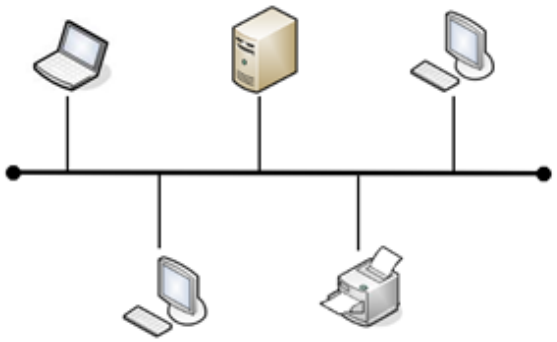


FIGURE 9 – Représentation schématique d'un réseau en bus.

Topologie en étoile

- ◇ La forme physique du réseau ressemble à une étoile, voir la Figure 10.
- ◇ C'est la topologie la plus courante aujourd'hui.
- ◇ La communication entre machine se fait via un matériel central qui peut être un commutateur (switch) ou bien un concentrateur (hub).

- ◇ Si le média utilisé est un fil de cuivre à paires torsadées (STP), alors : Débit : 100 Mbits/s Longueur : 100 m max La norme utilisée est l'Ethernet 100BaseTX.
- ◇ Si le média utilisé est la fibre optique Débit : 155 Mbits/s à 10 Gbits/s Longueur : pas de max La norme utilisée est l'Ethernet 100BaseF.

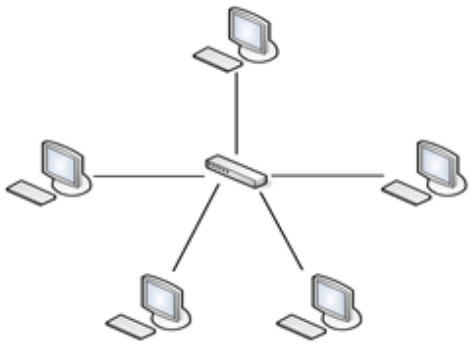


FIGURE 10 – Représentation schématique d'un réseau en étoile.

Topologie en anneau

- ◇ La forme physique du réseau ressemble à un anneau, voir la Figure 11.
- ◇ Les ordinateurs sont situés sur une boucle et communiquent chacun à son tour.
- ◇ Un équipement appelé : MAU (Multistation Access Unit) est utilisé pour gérer la communication en impartissant le temps de parole pour chacune des stations.

La méthode d'accès au support de communication est dite ≪Token ring≫ dont le principe est : Une station connectée au réseau possède un jeton virtuel, ce jeton est une autorisation de communication. Une fois la station a transmis, elle passe le jeton à la station suivante et ainsi de suite.

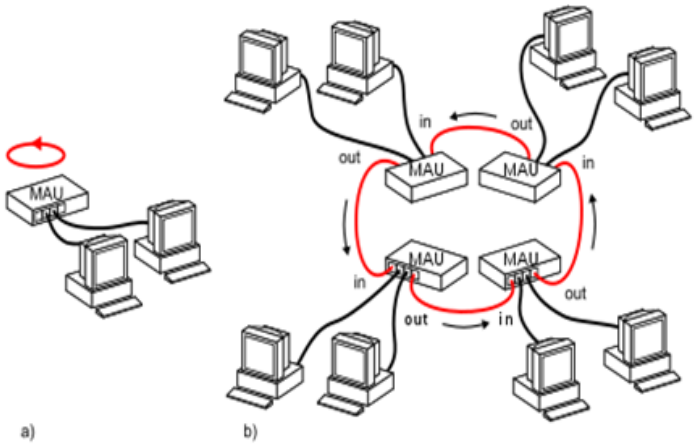


FIGURE 11 – Représentation schématique d'un réseau en anneau.

Topologie à deux anneaux

Le FDDI (Fiber Distributed Data Interface) est une topologie réseau constituée de deux anneaux, l'un est dit « primaire », il assure la transmission de données. L'autre est dit «secondaire», assure la détection et la correction des erreurs, voir la Figure 12. La technologie FDDI utilise en générale la fibre optique multimode comme support de transmission. Elle fonctionne avec un débit nominal de 100 Mbit/s pour une distance maximal de 100 km, et peut supporter jusqu'à 1000 stations. Le jeton circule entre la machine à une vitesse très élevée. Si celui-ci n'arrive pas au bout d'un certain délai, la machine considère qu'il y a eu une erreur sur le réseau. La topologie FDDI ressemble de près à celle de TOKEN RING à la différence près qu'un ordinateur faisant partie d'un réseau FDDI peut aussi être relié à un concentrateur MAU «Multi station Access Unit » d'un second réseau ; on parle alors de système bi connecté.

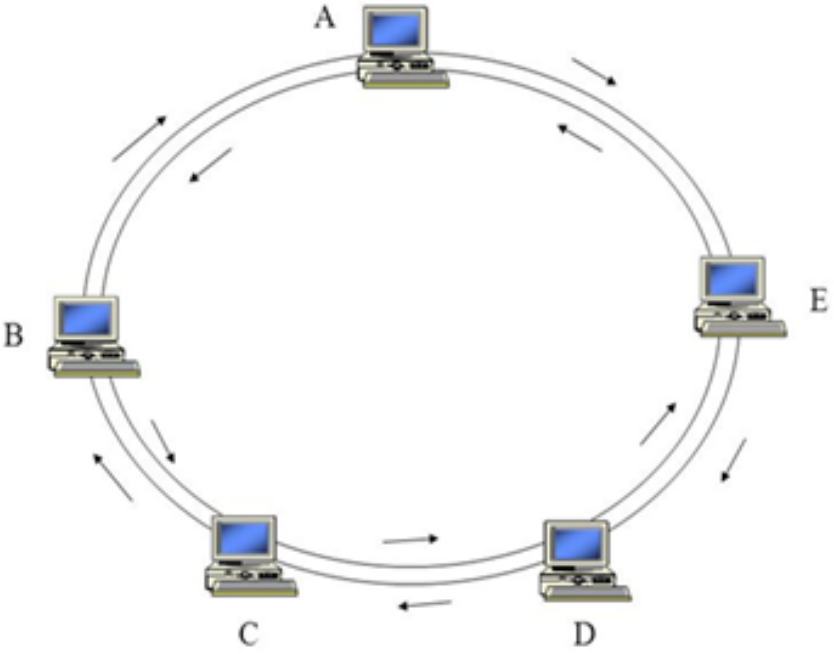


FIGURE 12 – Représentation schématique d'une topologie à deux anneaux.

Topologie en arbre (hiérarchique)

Cette topologie est dérivée des réseaux en étoile, les réseaux hiérarchiques sont constitués d'un ensemble de réseaux étoiles reliées entre eux par des concentrateurs cascadables (stackable hubs) jusqu'à un nœud unique, voir la Figure 13.

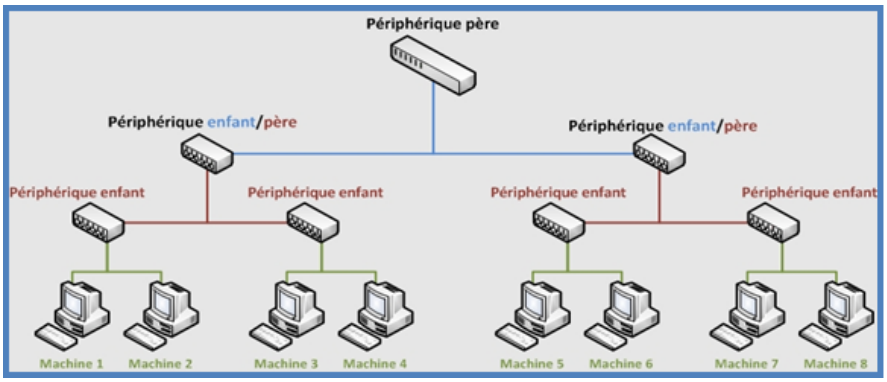


FIGURE 13 – Représentation schématique d'un réseau en arbre.

Topologie maillée

Le réseau maillé est une topologie de réseau dont tous les ordinateurs sont connectés point à point sans hiérarchie centrale, voir la Figure 14. Cette topologie permet de multiples choix de chemins vers une même destination, Ainsi, elle est très résistante à la défaillance d'un nœud. Le réseau Internet est basé sur une topologie maillée.

Il existe deux types de maillage :

- ◇ **Maillage complet** :

  La topologie est dite à maillage complet, lorsque chaque noeud possède un circuit le connectant à chaque autre noeud dans un réseau. Ainsi, dans le cas où l'un des noeuds échoue, le trafic peut dirigé vers l'un des autres noeuds. Cette topologie est coûteuse à mettre en oeuvre en plus du problème de la redondance.

- ◇ **Maillage partiel** :

  La topologie est dite à maillage partiel, lorsque certains noeuds du réseau sont organisés en maillage complet mais d'autres ne sont pas connectés à un ou deux dans le réseau. Cette topologie est moins coûteuse à mettre en oeuvre que la précédente et donne moins de redondance.

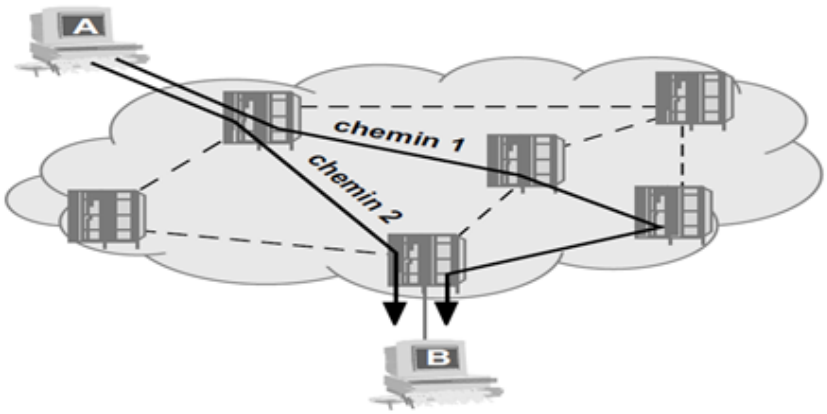


FIGURE 14 – Représentation schématique d'un réseau maillé.

Topologie mixte (hybride)

Il s'agit d'un regroupement de plusieurs topologies différentes étudiée ci-dessus, voir la Figure 15 .

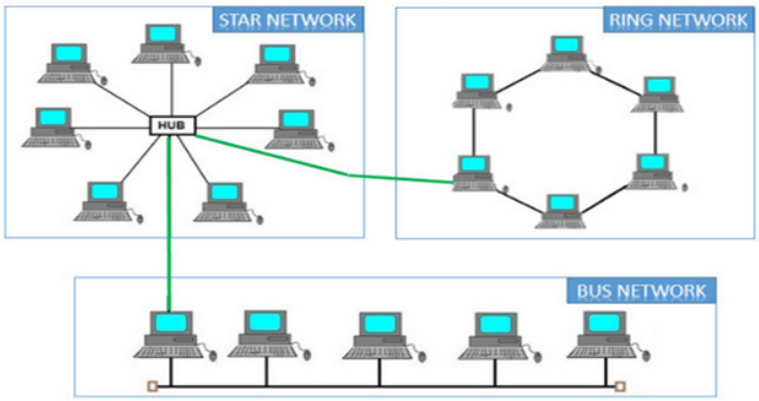


FIGURE 15 – Représentation schématique d'un réseau hybride.

Topologie cellulaire

La topologie cellulaire est employée dans les réseaux sans fils. les réseaux cellulaires utilisent des protocoles dits : à diffusion, c'est-à-dire, tous les noeuds (téléphones mobiles) reçoivent es transmissions depuis un site central sur un canal fixé (appelé : contrôle). L'un de ces noeuds (appelé station de base) utilise ce canal commun pour fournir à un noeud le numéro de canal spécifique (appelé : utilisateur) afin d'établir sa connexion ; pendant tout la durée de la connexion, le téléphone communique simultanément avec la station de base au moyen du canal de contrôle et du canal utilisateur.

1.9 Les équipements d'interconnexion

Comme nous l'avons vu précédemment dans la section des supports de transmission, il y a des contraintes sur la longueur des câbles utilisés pour interconnecter les équipements sur un réseau local en fonction du débit, de la vitesse de propagation et de la taille du message. En plus des contraintes

physiques (tel que l'atténuation du signal due à la distance). Ainsi, afin d'interconnecter plusieurs équipements filaires et créer des réseaux locaux, on utilise des équipements intermédiaires [7], appelés : équipements d'interconnexion.

Les équipements d'interconnexion servent à connecter plusieurs machines entre elles, comme les cartes réseaux, les hubs ou les switchs (commutateurs), les routeurs, etc. Ces équipements sont détaillés par la suite.

1.9.1 La carte réseau (Network Interface Card)

C'est une interface qui permet de connecter un ordinateur au support de transmission utilisé par le réseau. Elle a pour fonction de préparer, d'envoyer et de contrôler le flux de données sur le réseau. La carte réseau peut être directement incluse dans la carte mère (cas de nombreux portables), mais peut également se trouve sous la forme d'une carte PCI ou d'une clé USB (cas wi-fi).

La carte réseau se connecte à la Carte mère de l'ordinateur via un bus informatique, Il existe donc plusieurs modèles de cartes réseau selon le type des bus suivants :

- ◇ **ISA** (pour Industry Standard Architecture), un bus parallèle de 8 bits apparu en 1981.
- ◇ **L'EISA** (Extended Industry Standard Architecture), extension à 16 bits du bus ISA, apparue en 1988.
- ◇ **Le PCI** (Peripheral Component Interconnect), un bus parallèle de 32 bits, apparu en 1994.
- ◇ **Le PCI Express** apparu en 2004.

La carte réseau possède généralement deux témoins lumineux (LEDs) qui sont :

- ◇ Le led vert correspond à l'alimentation de la carte ;
- ◇ Le led orange [10Mbps] ou rouge [100Mbps] indiquent une activité du réseau (envoi ou réception des données).

Les principaux fabricants de cartes réseau sont : TP-LINK, D-Link, Asus, TRENDnet, Gigabyte Technology, voir la Figure 16.

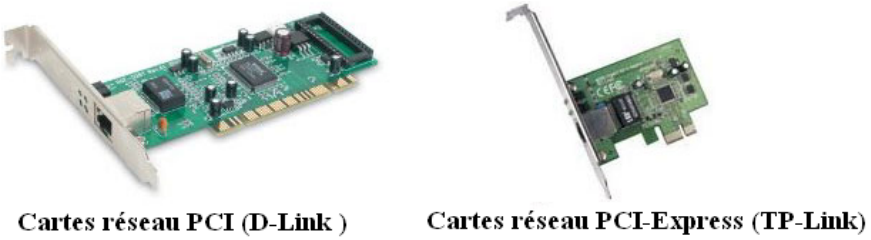


FIGURE 16 – Exemples de carte réseau.

1.9.1.1 Cartes réseau sans fils

Pouvoir être connecté à un réseau sans fil, un PC portable ou de bureau doit être équipé d'une carte réseau sans fil Wi-Fi (Wireless Fidelity), voir la Figure 17. Il possible de relier deux ordinateurs directement par Wi-Fi (on parle alors de l'architecture ad hoc) comme en Ethernet filaire, pour relier plus de deux machines on utilise généralement un matériel spécifique appelé routeur Wi-Fi.

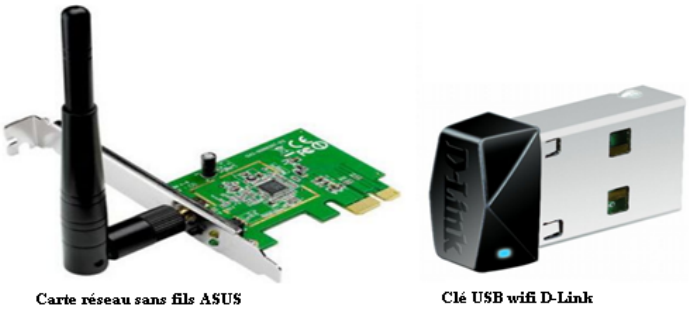


FIGURE 17 – Exemples de carte réseau wi-fi.

1.9.1.2 L'adresse MAC

Chaque carte réseau possède une adresse exclusive appelée une adresse MAC (Media Access Control), aussi nommée adresse physique. L'adresse

MAC est affectée par le constructeur de la carte et est inscrite sur la puce de la carte, c'est un identifiant physique stocké dans une carte réseau ou une interface réseau similaire. Elle sert à identifier la carte dans le réseau lorsque les informations sont envoyées ou reçues au sein du réseau. L'adresse MAC est définie sur 48 bits. Elle est représentée sous la forme de 6 blocs de deux chiffres hexadecimaux (base 16), chaque bloc étant séparé par un double point ou un tiret selon le type du système d'exploitation (Windows ou Linux), voir la Figure 18. Un constructeur de carte réseau se voit attribuer par l'IEEE un numéro de constructeur unique sur 24 bits, ce numéro est appelé OUI(Organizationally Unique Identifier). les 24 bits restants sont laissés à la discrétion du constructeur afin d'identifier de manière unique une carte parmi celles qu'il fabrique [7]. Parmi les 24 bits du numéro OUI, deux bits ont une signification particulière. Si le bit de poids faible del'octet de poids fort est à zéro, cela signifie qu l'adresse identifie un seul équipement. Si le bit est positionné à un, l'adresse identifie un groupe d'équipements. Ce qui s'avère utile dans le cas de communication de groupe (multicast). Le deuxième bit de poids faible de l'octet de poids fort permet de stipuler si l'adresse est administrée localement (bit positionné à 1) ou est globale (bit positionné à zéro). L'adresse MAC est utilisée pour savoir qui est l'émetteur et qui est le récepteur d'un message. En effet, à la réception d'un message, la carte réseau vérifie l'adresse destination du message, Si elle correspond à sa propre adresse MAC,dans ce cas le message est traité. Sinon, le message est rejeté tout simplement. Une adresse particulière peut être utilisée pour qu'un message soit envoyé vers toutes les machines du réseau, il s'agit de l'adresse de diffusion (broadcast, en anglais), elle est représentée par : ff :ff :ff :ff :ff :ff (il n'y a pas de de distinction entre la casse minuscule et majuscule), cette adresse ne peut jamais être attribuée à une machine unique.

1.9.2 Le répéteur (Repeater)

Parmi les nombreux composants réseau qui font partie de la couche physique, le plus simple est le répéteur. C'est un équipement non intelligent, qui répète automatiquement tous les signaux qui lui arrivent et transitent d'un

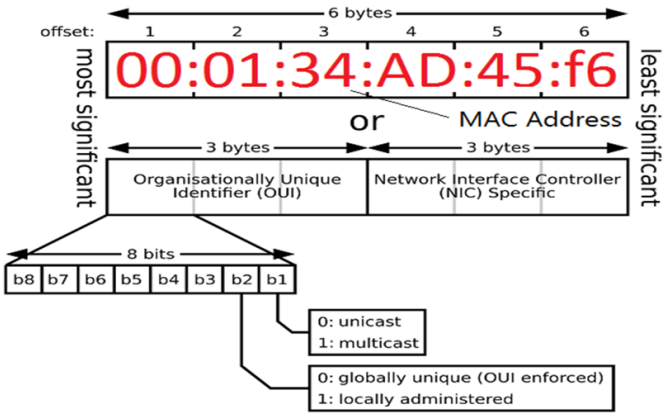


FIGURE 18 – Adresse MAC (Media Access Control).

support vers un autre support. Dans le même temps, le répéteur régénère les signaux, ce qui permet de prolonger le support physique vers un nouveau support physique[5].

1.9.3 Hub (concentrateur)

C'est un équipement permettant de régénérer le signal entre deux nœuds de réseau, il permet de prolonger facilement un support de transmission existant et d'interconnecter deux segments d'un même réseau. Il sert d'emplacement central pour relier les ordinateurs et autres périphériques. Le concentrateur dispose d'un certain nombre de ports auxquels viennent se connecter les PC clients. On utilise quelque fois le terme de répéteur multi-ports car il transfère ou renvoient tous les paquets qu'il reçoit à tous ses ports. Les concentrateurs n'effectuent aucun contrôle ou filtrage de données qui les traversent. La Figure 19illustre le symbole représentant un hub dans une architecture réseaux.

Les hubs sont souvent utilisés quand il s'agit de relier quelques ordinateurs ensemble pour un petit réseau local. Donc, pour pouvoir connecter plus d'ordinateurs, on a inventé les ponts ensuite les switchs.

Concentrateur

FIGURE 19 – Symbole représentant un hub.

1.9.4 Le pont (Bridge)

Le pont se présente sous forme d'un boîtier munie d'un nombre limité de ports, il permet d'interconnecter des réseaux travaillant avec le même protocole. Ainsi, contrairement au répéteur, qui travaille au niveau physique (signal), le pont travaille également au niveau logique (adresse IP), c'est-à-dire, qu'il est capable de filtrer les messages en ne laissant passer que ceux dont l'adresse correspond à une machine située à l'opposé du pont. Le pont permet de segmenter un réseau local en deux pour améliorer les performances. En effet, cela permet de réduire le trafic (les collisions notamment) sur chacun des réseaux et d'augmenter le niveau de confidentialité car les messages destinés à un réseau ne peuvent pas être reçus par l'autre segment. La Figure 20illustre le symbole représentant un pont dans une architecture réseaux.

Pont

FIGURE 20 – Symbole représentant un pont.

1.9.5 Switch (ou commutateur)

Le switch est un pont multiports, il permet de connecter plusieurs appareils en réseau. C'est généralement un boitier disposant plusieurs ports Ethernet (entre 4 et plusieurs dizaines). Les switchs sont un peu plus intelligents que les hubs. En effet, La différence avec le hub, c'est que le switch sait quels sont les ordinateurs qui sont autour de lui. Ainsi, si il reçoit une trame pour l'ordinateur X, il ne l'envoie qu'à l'ordinateur X et pas aux autres. Il commute (il branche) l'entrée des données vers la sortie où est l'ordinateur concerné. C'est pour cela qu'on appelle ça un commutateur en français. La principale caractéristique d'un switch est de savoir déterminer sur quel port il doit envoyer une trame en fonction du destinataire. Ce qui limite l'encombrement du réseau (bande passante). La Figure 21illustre le symbole représentant un switch dans une architecture réseaux.

FIGURE 21 – Symbole représentant un switch.

1.9.6 Routeur (Router)

Il permet d'interconnecter des réseaux de même ou différentes technologies et d'assurer un acheminement (routage) des paquets entre équipement et réseaux selon les adresses logiques. En effet, à la différence du HUB et du SWITCH qui permettent de connecter des appareils faisant partie d'une même classe d'adresse IP ou d'un même sous réseau. Le routeur est un équipement capable de diriger les paquets transitant entre des réseaux indépendants. Cette opération, appelée routage, traite les paquets en fonction de leurs adresses IP de provenance et de destinations, grâce à des algorithmes et des tables de routage. La Figure 22illustre le symbole représentant un routeur dans une architecture réseaux.

FIGURE 22 – Symbole représentant un routeur.

1.9.7 Multilayers switch

C'est un commutateur multicouches capable de remplir en plus de la tâche de commutationdes, la tâche de routage. Il est aussi appelé : switch de niveau 3. Il s'agit d'un véritable routeur dédié au réseau LAN d'entreprise. La Figure 23illustre le symbole représentant un commutateur multicouche dans une architecture réseaux.

FIGURE 23 – Symbole représentant un commutateur multicouche.

1.10 Conclusion

Nous avons exposé dans ce chapitre des concepts généraux sur les réseaux informatiques du point de vue : fonctionnement, composants de base, différentes topologies et supports de transmission. Ainsi qu'aux différents équipements d'interconnexion nécessaires à la transmission de données dans un réseau. Nous aborderons par la suite l'architecture en couche et modèle TCP/IP.

Chapitre 2

Architecture en couches et modèle TCP/IP

Sommaire

2.1 Introduction

Après avoir fait un tour sur le fonctionnement théorique du réseau ainsi que du matériels utilisés, nous allons étudier maintenant comment communiquent les machines dans un vaste réseau tel qu'Internet.

Pour réaliser un système complexe, on le décompose en éléments plus simples. Dans ce même contexte qu'un réseau d'ordinateurs peut être vu comme une architecture formée de plusieurs niveaux de communication, appelées couches. L'intérêt de la hiérarchisation des différentes couches de communication est de séparer les différentes fonctions de communication.

Au début des années 70, chaque constructeur a développé sa propre architecture de réseau informatique ; Ceci a créé des problèmes variés, notamment l'impossibilité de communication via des équipements de constructeurs différents.

Dans ce contexte, des normes (aussi appelés standards) devraient être élaborées par des organismes internationaux afin de répondre à un besoin naturel de communication. Ces organismes ont adopté des normes proposées par un groupement de constructeurs après s'être mis d'accord sur des règles communes.

Durant les années 1980, deux organismes de normalisation internationaux : l'UIT (Union Internationale des Télécommunications) et l'ISO (International Organization for Standardization) ont créé un modèle permettant d'exécuter et de maintenir des protocoles de communication de données [1].

Dans ce qui suit, nous aborderons un modèle normalisé d'une architecture des réseaux, appelé modèle OSI (Open System Interconnection).

2.2 Modèle OSI

Le modèle OSI (en anglais Open Systems interconnexion, interconnexion de systèmes ouverts) a été conçu dans les années 1970 par Hubert Zimmermann, et normalisé en 1984 par ISO. Il est devenu l'archétype des réseaux informatiques [1]. Il définit comment interconnecter des réseaux et des systèmes

d'information hétérogènes. C'est un modèle abstrait qui détermine une terminologie sans donner des précisions sur les technologies employés.

2.2.1 Concepts et principe de fonctionnement

L'architecture en couches du modèle OSI est définie par les concepts de **service**, **d'interface** et de **protocole** (voir la Figure 24).

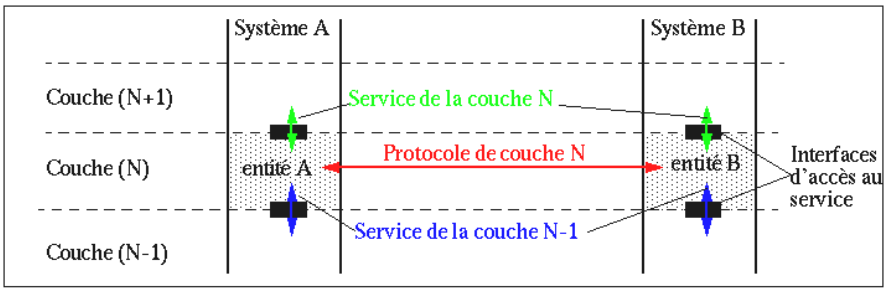


FIGURE 24 – Le mécanisme de fonctionnement du modèle OSI.

Le système de communication informatique est découpé en couches superposées, tel qu'une couche d'un système (*système A*) est en relation avec la même couche d'un autre système (*système B*). Le modèle OSI conçoit un **dialogue horizontal** entre les couches, alors que l'information est véhiculée **verticalement**.

Le dialogue vertical correspond au transfert d'informations d'une couche à une autre (couche adjacente), ce dialogue est réalisé à l'aide de **primitives de service**, telles que les demandes de connexion ou reception de données.

Ainsi, une couche (N) s'adresse à la couche immédiatement inférieur $(N-1)$ en lui demandant un service. De même, la couche $(N-1)$ s'adresse à la couche (N) en lui rendant un service.

Une interface (« point d'accès au service » dans la norme) est le moyen concret d'utiliser le service. Dans un programme, c'est typiquement un ensemble de fonctions de bibliothèque ou d'appels systèmes. Dans une réalisation matérielle, c'est par exemple un jeu de registres à l'entrée d'un circuit.

On appelle **protocole** l'ensemble des règles qui définissent le dialogue entre 2 couches de même niveau.

Une entité est un élément actif d'une couche. Le protocole (N) est réalisé par des entités de la couche (N), qui sont situées sur les sites distants. Pour mettre en oeuvre le protocole (N), les entités (N) utilisent le service de la couche inférieure $(N-1)$.

2.2.2 Les sept couches du modèle OSI

Le modèle OSI est organisé en couches de communication (voir la Figure 25), afin de diminuer la complexité des environnements informatiques. en effet, cette conception permet d'éviter une trop grande remise en cause si un changement ou une modification technologique apparaît. C'est le principe d'indépendances des couches.

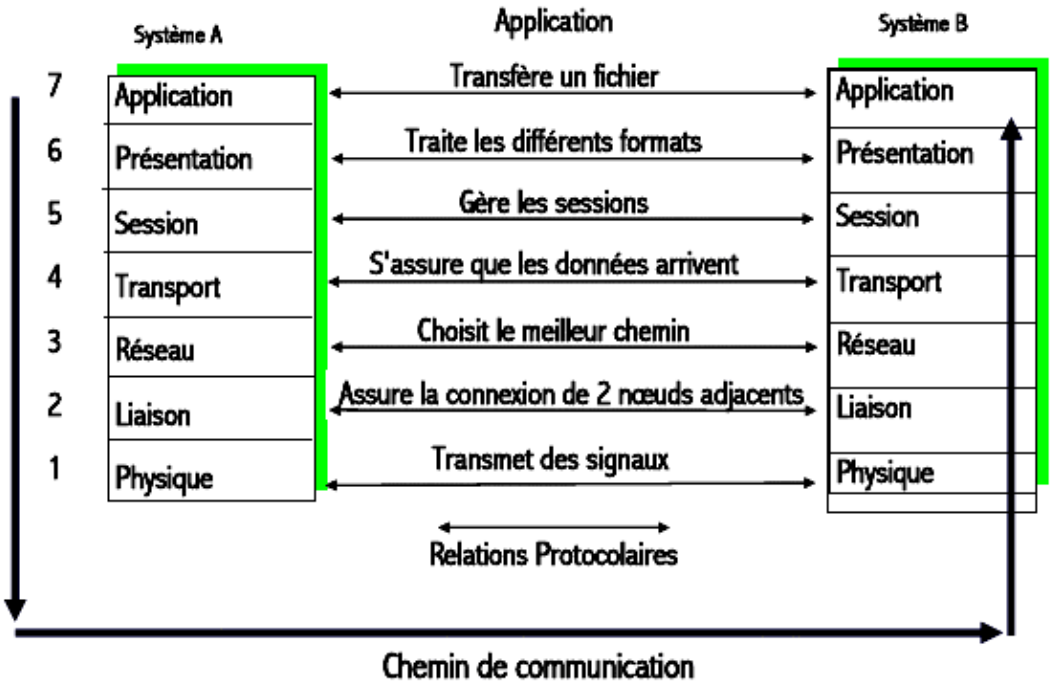


FIGURE 25 – Les sept couches du modèle OSI.

Le modèle OSI comporte sept couches, numérotées de 1 à 7, de la plus basse vers la plus haute comme suit : 1-la couche physique, 2-la couche liaison

de données, 3-la couche réseau, 4- la couche transport, 5-la couche session, 6-la couche présentation et 7-la couche application. Les couches sont classées par ordre d'abstraction, de la moins logique à la plus logique. Les couches "basses" correspondent aux couches 1 à 3. Les couches "hautes" définissent les couches 4 à 7. Chaque couche est définie par un nom, un niveau et un rôle spécifique. L'UIT et l'ISO ont créé des unités de données correspondantes à chaque couche appelées PDU (Protocol Data Unit)[1].

- ◇ **Couche1- Physique :**cette couche est chargée de la transmission des données en binaires sur les différents supportes physiques (électriques, électromagnétique, optique, etc.). C'est au niveau de cette couche que le type de codage et de modulation sont choisis. L'unité de données (PDU) correspondante à cette couche est le bit.
- ◇ **Couche2- Liaison de données :** la PDU de cette couche est appelée "trame". Cette couche se charge d'adressage et d'échanges des trames, de contrôler les erreurs survenues dans la couche physique, ainsi que du contrôle du flux (régulation du débit d'émission des trames)[7].
- ◇ **Couche3- Réseau :**la PDU de cette couche est appelée "paquet". Cette couche gère les communications entre les ordinateurs placées sur différents réseaux. Elle se charge de l'adressage logique des équipements (adressage IP)et d'acheminer les données d'un réseau à un autre en empruntant le meilleur chemin en utilisant les routeurs et de protocoles de routage.
- ◇ **Couche4- Transport :** Cette couche s'occupe de la fragmentation des données en petits paquets, appelés "segments" et elle se charge éventuellement de la gestion des problèmes liés au transport (renvoi des données si manquantes). A la réception, la couche transport assemble tous les segments pour reformer le message originel, ce qui assure une fiabilité des communications de bout-en-bout. Elle contrôle également le flux (débit) et permet d'utiliser en simultanée plusieurs applications utilisant des protocoles/ports différents.
- ◇ **Couche5- Session :** cette couche se charge de la mise en oeuvre des fonctions d'organisation et de synchronisation de la communication

entre les applications. Elle prend également des mesures de sécurité, telle que la validation des mots de passe.En pratique, ces fonctions sont intégrées dans la couche application (couche7).

- ◇ **Couche6- Présentation :** pour palier aux problèmes d'hétérogénéité syntaxique des données, cette couche se charge de la traduction des données échangées par les applications dans un format d'encodage standard. Comme la couche session, les fonctions de cette couche sont intégrées dans la couche application (couche7).
- ◇ **Couche7- Application :** dans cette couche sont définis les différents protocoles qui servent de support aux applications les plus familières aux utilisateurs, comme les protocoles de messagerie électronique, de navigation sur e web (HTTP), de transfert de fichiers(FTP), etc.

2.3 Modèle Internet ou TCP/IP

Le modèle TCP/IP (Transmission Control Protocol/ Internet Protocol) a été proposé à partir de 1969 avant le modèle OSI dans le cadre du projet ARPA (Advanced Research Project Agency) de la défense américaine. Son implementation réelle date des années 80 avec le projet ARPANET, réseau scientifique dans les universités américaines, mise au point par deux chercheurs Vinton Cerf et Robert Kahn.

Quoi que les deux modèles Internet ou TCP/IP et le modèle OSI sont nés pratiquement dans la même période mais développés séparément. Le modèle TCP/IP utilise également un modèle protocolaire en couches, comparable à son homologue OSI. Toutefois, c'est un modèle à quatre couches qui ne comprend ni couche Présentation, ni couche Session [1], ces deux couches étant groupées dans la couche 7 (application). La Figure 26 donne un schéma global du modèle TCP/IP.

en partant des couches du haut vers les couches du bas, nous décrirons dans ce qui suit en détail les quatres couches du modèle TCP/IP.

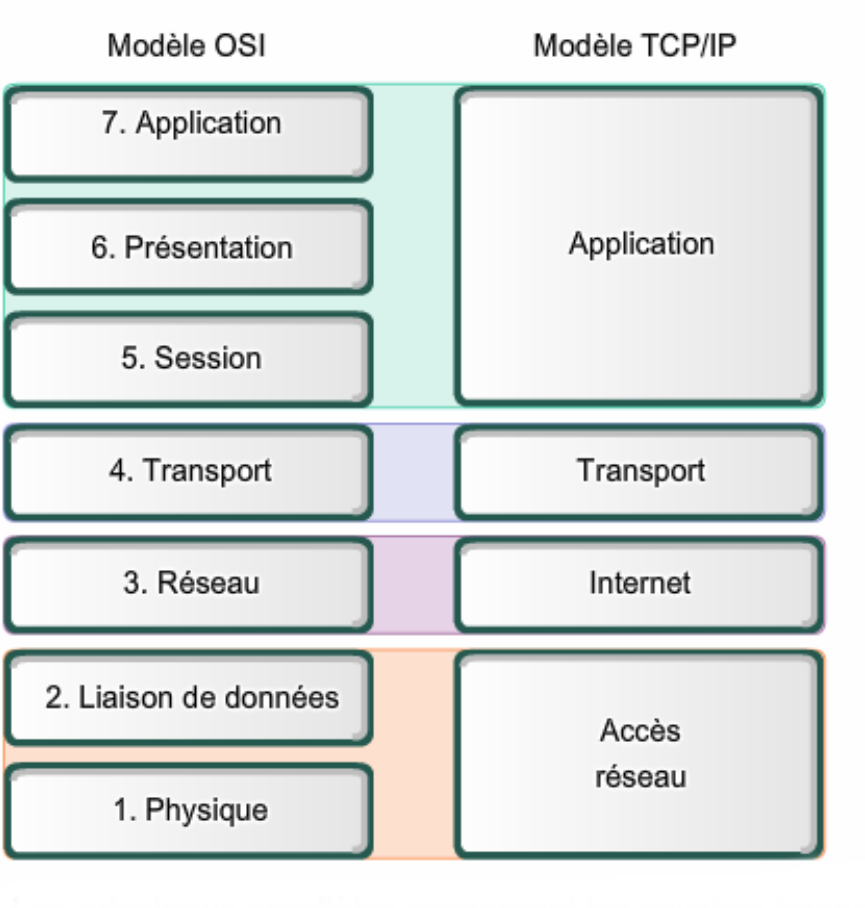


FIGURE 26 – Les couches du modèle TCP/IP.

2.3.1 La couche application

Les applications se situent au sommet du modèle TCP/IP, Ce sont des logiciels de communication qui accèdent au réseau. Leurs objectifs sont divers, outre la messagerie électronique, la transmission de voix et vidéos , transfert de fichiers, elles permettent le travail collaboratif (calcul réparti, jeux multi-joueurs et les réseaux sociaux). Ces applications sont à l'origine de croissance d'Internet puisqu'on voit apparaître de manière continue de nouvelles applications en réponse aux nouveaux usages. Exemples de protocoles de cette couche : FTP (File Transfert Protocol), SMTP (Simple Mail Transfert Protocol), HTTP ((HyperText Transfert Protocol)), etc.

2.3.2 La couche transport

La couche transport est la couche sur laquelle s'appuient directement les applications. Deux protocoles incontournables sont définis dans cette couche. Le protocole TCP (Transmission Control Protocol) et UDP (User Datagram Protocol). Les deux protocoles sont employés par la quasi totalité des applications. Néanmoins, ils ont des objectifs sensiblement différents :

- ◇ **TCP**procure une couche de transport fiable (données transmises sans erreur et reçues dans l'ordre de leur émission).
- ◇ **UDP**ne fait que transporter de manière non fiable des datagrammes IP (voir sections suivantes).

2.3.2.1 Le protocole TCP

Le protocole TCP est développé pour assurer un service de communication fiable et orienté connexion. Le terme "orienté connexion" signifie que deux applications qui dialoguent à travers TCP sont considérées l'une comme un serveur, l'autre comme un client et qu'elles doivent établir une connexion avant de dialoguer (comme le fonctionnement de la communication téléphonique). Le protocole TCP traite les données venant de la couche supérieure et les découpent en paquet TCP (appelé segment TCP), qui seront par la suite communiqués à la couche inférieure pour être soit transmis à travers le réseau, soit retransmis lorsqu'il ne reçoit pas d'acquittement de réception de la part du destinataire. A la réception, le protocol TCP s'assure du bon acheminement des paquets, détecte d'éventuelles erreurs de transmission comme il s'occupe du contrôle de flux d'informations afin de garantir que l'émetteur ne surcharge pas le tampon du destinataire. Finalement, le protocol reassemble les segments reçus.

La Figure 27 donne le format d'un segment TCP. Examinons les différents champs du segment TCP :

- ◇ **Port source** permet d'identifier l'application qui s'execute sur la machine locale, et **port destination** permet d'identifier le service ou l'application sollicité sur l'ordinateur distant.

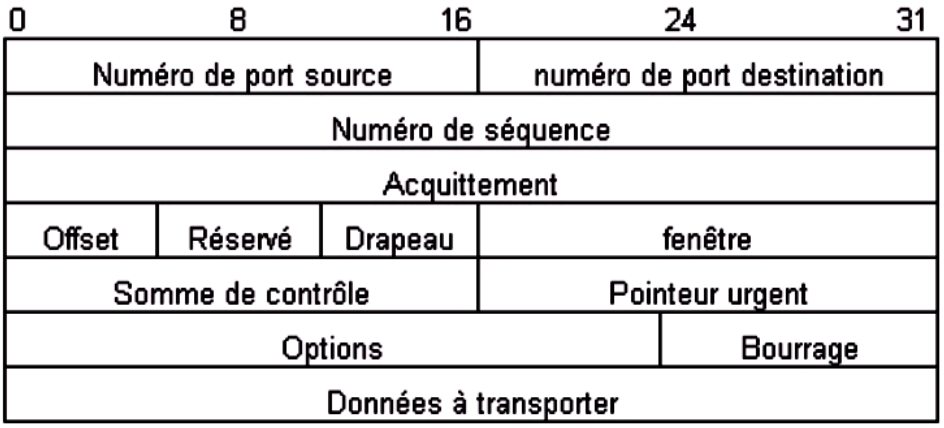


FIGURE 27 – Le format du segment TCP.

◇ **Numéro de séquence** les segments TCP portent un numéro de séquence qui permet de les ordonner.

◇ **Numéro d'acquittement** Si les paquets précédents ont été reçus sans erreurs ni perte, alors, le numéro d'acquittement contiendra le numéro de séquence du prochain paquet (ou segment) que l'on veut recevoir.

◇ **Taille (offset)** c'est un champ de 4 bits qui indique la longueur de l'en tête du paquet TCP en multiple de 32 bits permettant ainsi de repérer le début des données dans le paquet.

◇ **Réservé**ce champ composé de 6 bits n'est pas renseigné,il est réservé pour un usage futur.

◇ **Le champ code ou drapeau** ce champ de 6 bits représente des informations supplémentaires sur le rôle et le contenu du segment TCP. Quand tout les bits sont fixés à 1, leurs signification comme suit :

- ✓ URG : le paquet doit être traité de façon urgente.
- ✓ ACK : le paquet est un accusé de réception.
- ✓ PSH : le paquet fonctionne suivant la méthode PUSH. Certaines applications demandent que les données soient émises, même si le tampon n'est pas plein.
- ✓ RST : la connexion est réinitialisée.
- ✓ SYN : indique une demande d'établissement de connexion.

✓ FIN : interruption de la connexion.

◇ **Le champ fenêtre (window)** ce champ de 16 bits sert au contrôle de flux selon le principe de fenêtre glissante : permet de définir le nombre d'octets que le récepteur est prêt à accepter. Ainsi, l'émetteur augmente ou diminue sont flux de données en fonction de cette fenêtre.

◇ **Le champ checksum (somme de contrôle)** c'est un champ de 16 bits qui permet de vérifier l'intégrité de l'en-tête et des données. Il est calculé par l'émetteur et vérifié par le récepteur.

◇ **Le pointeur d'urgence**ce champ de 16 bits communique le numéro d'ordre à partir duquel l'information devient urgente en donnant son décalage par rapport au numéro de séquence.

◇ **Le champ option** ce champ est de taille variable permet de mettre en oeuvre des fonctions spécifiques à un transfert de données, par exemple, il permet au récepteur de diminuer la taille des paquets envoyés par l'expéditeur.

◇ **Le champ bourrage (padding)** remplit l'espace restant après les options avec des zéros pour avoir une longueur multiple de 32 bits ;

◇ **Les données à envoyer**

2.3.2.2 Le protocole UDP

Le second protocole de la couche transport est le protocole UDP. A l'inverse du protocole TCP, il travail en mode non connecté. Il existe deux principaux types d'applications utilisant le protocole UDP : es applications temps réel et les applications de multicasting.

◇ Dans les applications temps réel (real time) comme le transport de la voix, la retransmission des paquets erronés est inutile. En effet, rien ne sert la réexpédition de début de phrase alors que les utilisateurs poursuivent leur conservation, d'où l'utilisation du protocole UDP (livraison rapide) plutôt que TCP (une livraison exacte).

◇ Les applications de multicasting permettent l'expédition d'une même information à plusieurs utilisateurs simultanément. Exemple : une radio

diffusant ses programmes sur Internet, dans ce cas, si tout les utilisateurs renvoient un accusé de réception, l'émetteur risque d'être submergé, d'où l'utilisation du protocole UDP qui ne suggère pas les accusés de réception.

Le format détaillé d'un paquet UDP est donné dans la Figure 28. De même que TCP, UDP utilise la notion de port,qui permet de distinguer entre les différentes applications. Le champ "longueur" donne la longueur (en octets)du paquet UDP. Le champ checksum (somme de contrôle) est présent, mais permet seulement de détecter les erreurs et non pas les corriger.

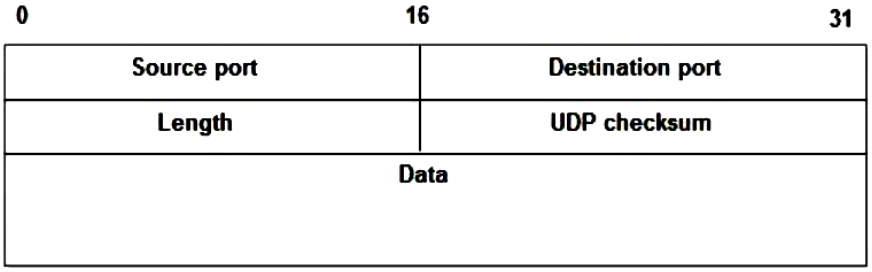


FIGURE 28 – Le format du paquet UDP.

2.3.3 La couche réseau

C'est la couche la plus importante du modèle TCP/IP. Elle est aussi appelée couche IP (Internet Protocol), elle est chargée d'attribuer une adresse unique à chaque machine du réseau, elle permet également la gestion de la circulation de paquets à travers le réseau en assurant leur routage, ainsi que la gestion de leurs fragmentation. Elle comprend également les protocoles ICMP (Internet Control Message Protocol) et IGMP (Internet Group Management Protocol).

2.3.3.1 Le protocole IP

Comme le protocole UDP, IP est un protocole sans connexion qui ne contrôle pas les erreurs de transmission. Les principales fonctions de ce protocole que nous examinerons dans les sections suivantes concernent : l'adressage

IP, la fragmentation et le routage. L'unité de données (PDU) correspondante à cette couche est le datagramme.

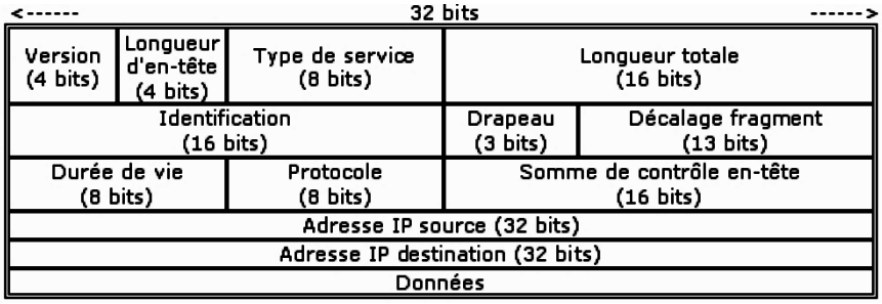


FIGURE 29 – Structure d'un datagramme IP.

Dans ce qui suit partie, nous examinerons la structure du datagramme IP (voir la Figure 29). Les différents champs du datagramme IP sont :

- ◇ **Version :** ce champ est codé sur 4 bits,il permet d'identifier la version du protocole IP utilisé, exemple IPv4.
- ◇ **Longueur :** ce champ est codé sur 4 bits,il indique la longueur de l'entête IP en multiple de 32 bits ce qui marque le début des données dans le datagramme.
- ◇ **TOS(Type Of Service) :** ce champ est codé sur 8 bits,il indique la façon dont le datagramme doit être traité : avec priorité,en minimisant le délai de son acheminement, maximiser le débit de transmission, etc.
- ◇ **Longueur total :**indique la longueur totale du paquet en octets
- ◇ **Identification :**ce champ est codé sur 16 bits, ce champ est donné par l'émetteur et permet au récepteur d'identifier les fragments d'un même datagramme. Tous les fragments d'un même datagramme porteront le même numéro.
- ◇ **Drapeaux :**ce champ est codé sur 3 bits, son rôle est de renseigner les systèmes intermédiaires sur la possibilité ou non de fragmenter le datagramme.
- ◇ **Position du fragment :**ce champ est codé sur 13 bits indique la position du fragment dans le datagramme d'origine.

- ◇ **Durée de vie(ou TTL, Time To Live) :**ce champ est codé sur 8 bits indique le nombre maximale de routeurs que peut traverser un datagramme, sa valeur est décrémentée de 1 à chaque passage d'un routeur qui reçoit le datagramme et le réxpédie. Quand un routeur reçoit un datagramme avec le champ TTL=0 il le détruit ce qui évite que le datagramme circule éternellement si une adresse est introuvable.
- ◇ **Protocole :**ce champ est codé sur 8 bits, contient le numéro du protocole de niveau supérieur (couche transport). Exemple : la valeur 6 identifie le protocole TCP et la valeur 17 UDP.
- ◇ **Checksum de l'entête :** il s'agit d'un code arithmétique détecteur d'erreurs permettant de s'assurer que les données de l'entête n'ont pas été altéré durant la transmission.
- ◇ **Adresses IP source et destination :** ce sont les informations les plus importantes puisqu'elles permettent d'acheminer les données à la bonne destination.
- ◇ **Option et bourrage :**le champ *option* est de taille variable permet de faire certains transferts particuliers, il est souvent complété par des bits de *bourrage* pour assurer à l'entête une taille totale multiple de 32 bits. Le bourrage se fait par des bits à zéro.

2.3.3.2 La fragmentation

La taille maximale d'un datagramme IP est 65536 octets (équivalent à 64 MO). Toutefois si les paquets issus de la couche transport ont une taille plus grande que le MTU du réseau, la couche réseau doit assurer leur fragmentation. En effet, chaque réseau dispose de ses propres caractéristiques physiques, dont la taille maximale des trames appelées MTU (Maximum Transfer Unit) exprimée en octets. La fragmentation d'un paquet est contrôlée par les champs du datagramme IP suivants : longueur totale, identification, drapeaux et le champ position du fragment. Ces quatre champs véhiculent toutes les informations nécessaires permettant au récepteur de réassembler les datagrammes.

2.3.3.3 L'adressage IP

Dans un réseau informatique, chaque périphérique doit disposer d'une adresse IP unique sous un format normalisé. Contrairement à l'adresse physique, l'adresse IP est une adresse logique qui ne dépend pas de la machine, elle est choisie pour pouvoir désigner une machine en tant que membre d'un réseau ou d'un sous-réseau.

Structure d'une adresse IP L'adresse IP est codée sur 32 bits pour IPv4, représentée dans une notation décimale pointée constituée de 4 nombres compris chacun entre 0 et 255.

Exemple :

- ◇ Notation décimale : 197.75.200.22
- ◇ Notation binaire : 11000101.01001011.11001000.00010110

L'adresse IP comporte deux parties :

- ◇ Les bits de poids forts forment l'identifiant du réseau (Network ID).
- ◇ Les bits de poids faibles forment l'identifiant de la machine (Host ID).

Les classes d'adresses Les adresses de réseaux sont affectées par un organisme international : ICANN (Internet Corporation for Assigned Name and Numbers). Pour simplifier, l'ICANN a découpé l'espace d'adressage IPv4 en cinq classes d'adresses :

- ◇ **Classe A :** cette classe sont attribuées aux réseaux qui comportent un nombre élevé d'hôtes. L'ICANN fixe les 8 premiers bits (bits de poids fort) pour identifier le réseau et les 24 autres bits pour identifier l'hôte.
- ◇ **Classe B :**les adresses de cette classe sont attribuées à des réseaux de taille moyenne à grande. L'ICANN fixe les 16 premiers bits (bits de poids fort) pour identifier le réseau et les 16 autres bits pour identifier l'hôte.
- ◇ **Classe C :**les adresses de cette classe sont généralement employées pour les petits réseaux locaux. L'ICANN fixe les 24 premiers bits (bits

de poids fort) pour identifier le réseau et les 8 autres bits pour identifier l'hôte.

- ◇ **Classe D :**cette classe est prévue pour les communications de groupes appelées "multicast". contrairement aux trois premières classes qui sont dédiées à "l'unicast", communication point à point.
- ◇ **Classe E :**il s'agit d'une classe expérimentale réservée pour un usage future.

Masque de réseau Le masque de réseau (Netmask, en anglais) est un autre élément important du système d'adressage IP. Le masque à la même structure qu'une adresse IP, son rôle est d'identifier les deux parties de l'adresse IP, à savoir : l'identifiant du réseau (NetID) et l'identifiant de l'hôte (HostID). Autrement dit, le masque de réseau (ou sous-réseau) s'obtient en mettant à "1" tous les bits de la partie NetID de l'adresse IP et à "0" la partie HostID.

Les premiers bits d'une adresse IPv4 permettent d'identifier sa classe et par conséquent son masque. Les classes d'adresses sont illustrées dans le tableau 1 suivant [7] :

TABLE 1 – *Classes d'adresses IPv4*

Classe	Premiers bits	Début de plage	Fin de plage	Masque
A	0...	1.0.0.0	126.255.255.255	255.0.0.0
B	10...	128.0.0.0	191.255.255.255	255.255.0.0
C	110...	192.0.0.0	223.255.255.255	255.255.255.0
D	1110...	224.0.0.0	239.255.255.255	/

Exemple :

Soit une adresse IP d'une machine de classe C en notation décimale : 192.168.1.2 (en binaire : 11000000.10101000.00000001.00000010), son masque est 255.255.255.0 (en binaire : 11111111.11111111.11111111.00000000)

Ainsi, pour obtenir le NetID , il faut effectuer un ET logique (AND) bit à bit entre l'adresse IP et le masque, voir la Figure 30. Le résultat représente

l'adresse IP du réseau auquel appartienne cette machine, soit en décimale : 192.168.1.0.

```
Adresse IP  11000000.10101000.00000001.00000010
Masque    & 11111111.11111111.11111111.00000000
Résultat  = 11000000.10101000.00000001.00000000
```

FIGURE 30 – Opération logique pour obtenir l'adresse ip d'un réseau.

Adresses réservées Un certain nombre d'adresse IP sont réservées à un usage sur des réseaux privés, c'est à dire tout réseau non connecté à Internet. Ces adresses sont donc non routables et sont généralement utilisées par des réseaux individuels (domestiques) ou entreprises. Les plages d'adresses suivantes (Tableau 2) sont réservées aux réseaux privés par classes :

TABLE 2 – *Plages d'adresses IPv4 réservées*

Classe	Début	Fin
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

Adresses de diffusion (broadcast) C'est une adresse qui dans sa partie HostID, tous les bits sont mis à "1". Elle st utilisée pour diffuser un message à'attention de l'ensemble des machines du réseau.

Exemple : 192.168.1.255 est une adresse de diffusion du réseau dont l'adresse IP est 192.168.1.0 de classe C.

Adresses de bouclage (loop back) Chaque ordinateur dispose d'une adresse locale qui permet de communiquer avec sa propre machine via le protocole IP. Cette adresse est sous a forme : *127.x.y.z.* Leur rôle est de permettre de vérifier que TCP/IP est bien configuré sur la machine locale (local host).

Les sous-réseaux (subnetting) Le subnetting consiste à utiliser une seule adresse IP pour créer d'autres sous-réseaux. Pour créer des sous-réseaux, les bits sont empruntés de la partie HostID. Ainsi, pour un bit emprunté,il est possible de créer deux sous-réseaux car seulement 0 ou 1 sont possibles. Pour créer plus de sous-réseaux, plus de bits doivent être empruntés.

Exemple :

Soit l'adresse d'un réseau de classe C : 192.168.1.0 ayant un masque par défaut 255.255.255.0. L'objectif est de découper ce réseau en deux sous-réseaux.

Pour créer les deux sous-réseaux, nous allons suivre les étapes suivantes :

1. **Chercher le nombre de bits nécessaires**

   En empruntant un bit seulement de la partie HostID ($2^1 = 2$), nous pouvons avoir deux sous-réseaux :

   (192.168.1.00000000 et 192.168.1.10000000) mais le premier sous-réseau n'est pas autorisé puisqu'ils'agit de l'adresse du réseau.

   Donc on utilise deux bits ($2^2 = 4$) pour avoir quatre sous-réseaux , mais il n'y a que deux qui sont utilisables.

2. **Calculer le masque de sous-réseaux**

   Le masque de réseau par défaut est : 255.255.255.0, en ajoutant 2 bits on obtient un nouveau masque : 255.255.255.192.

3. **Calculer les adresses des sous-réseaux**

   - 192.168.1.00000000 (adresse du réseau lui même)
   - 192.168.1.01000000 (adresse du premier sous-réseau)
   - 192.168.1.10000000 (adresse du deuxième sous-réseau)
   - 192.168.1.11000000 (adresse de sous-réseau non utilisable)

   Les deux sous-réseaux sont donc : 192.168.1.64 et 192.168.1.128.

4. **Adresses de diffusion de chaque sous-réseaux**

   Pour obtenir l'adresse de diffusion dans chacun des deux sous-réseau, on met à 1 tous les bits de la partie HostID.

Ainsi, l'adresse de diffusion du premier sous-réseau est (192.168.1.127) et l'adresse de diffusion du deuxième sous-réseau est 192.168.1.10111111 (192.168.1.191).

Notation CIDR Il existe une autre forme pus courte du masque réseau connue sous le nom *CIDR* (Classless Inter-Domain Routing). Elle donne l'adresse IP du réseau suivi par un slash (/) et le nombre de bits mis à "1" dans la notation binaire du masque.

Exemple :

Dans l'exemple précèdent, l'adresse IP du réseau peut être écrite en notation CIDR comme suit : 192.168.1.0/24

2.3.3.4 Le routage

Afin d'interconnecter des réseaux, il faut déterminer un chemin (une route). Cet objectif est réalisé par des algorithmes implémentés dans un équipement appelé *routeur* , passerelle ou gateway, relié à au moins deux réseaux. Ainsi, un routeur réémettra des datagrammes venus d'une de ses interfaces réseau vers une autre. Chaque datagramme IP contient l'adresse IP de l'émetteur et du récepteur (destinataire). Lorsqu'un datagramme est émis, la station regarde si l'adresse IP du récepteur appartient au même réseau à laquelle elle apparient, grâce au masque réseau. Si c'est le cas, le datagramme est envoyé directement vers le récepteur. Dans le cas contraire, le datagramme est envoyé vers le routeur par défaut. Les routeurs disposent d'une table de routage qui leur permet de choisir la route pour arriver à une destination. Il s'agit d'un fichier où chaque ligne indique la route d'un réseau à atteindre en associant des adresses des réseaux à des interfaces de routeurs pour y parvenir. Afin d'éviter toute impasse, il y a toujours une entrée indiquant un chemin par défaut.

La mise à jour des tables de routage s'effectue de deux manières :

- ◇ Procédure manuelle ou routage statique : pour les petits réseaux, l'administrateur peut effectuer des modifications manuelle de la table de routage.

- ◇ Procédure automatique ou routage dynamique : il est effectué par un algorithme (protocole) de routage. Trois grandes catégories de protocoles de routage existent pour les réseaux locaux : à vecteur de distance (tel que l'algorithme RIP (Routing Information Protocol)) , à état des liens (tel que OSPF (Open Shortest Path First))et à vecteur de chemin (tel que BGP (Border Gateway Protocol)).

Il est claire qu'une solution automatique est choisie dès que le réseau devient conséquent.

2.3.3.4.1 La table de routage Une table de routage est un élément central du routage IP. Il s'agit d'une structure de données permettant à un routeur ou un ordinateur en réseau d'accéder à un segment précis du réseau sur lequel se trouve la machine de destination.

La table de routage IPv4 contient en général les informations suivantes :

- ◇ Les adresses des réseaux de destination,
- ◇ Les masques de sous-réseaux,
- ◇ Les adresses des routeurs intermédiaires (passerelles) permettant de les atteindre,
- ◇ L'adresse de l'interface réseau (la carte réseau) par laquelle le paquet sortira du routeur.

Exemple : Considérons l'exemple d'un réseau comportant : deux routeurs (RT1 et RT2) pour séparer les 4 segments dont les adresses sont indiquées en rouge sur la Figure 31.

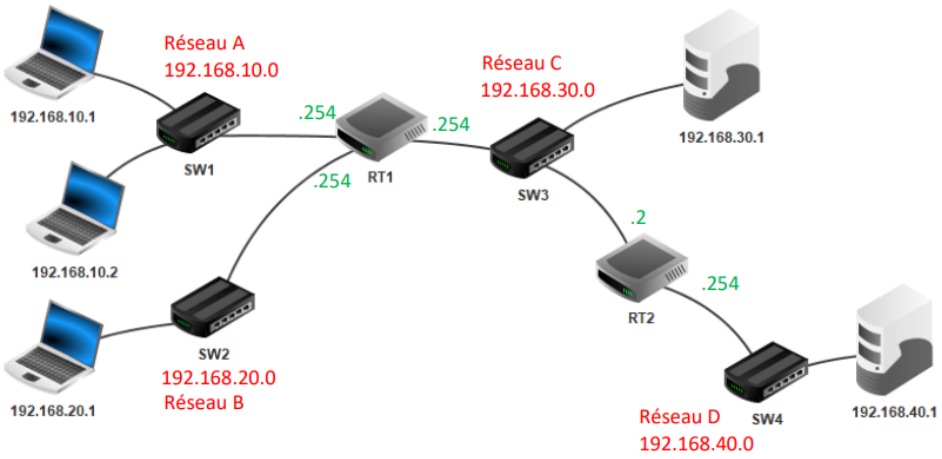


FIGURE 31 – Exemple d'un réseau comportant deux routeurs et 4 segments.

La figure suivante (Figure 32) représentent les deux tables de routages du premier routeur (RT1) et du second routeur (RT2).

Routeur RT1			
Destination	Masque	Passerelle	Interface
192.168.10.0	255.255.255.0	192.168.10.254	192.168.10.254
192.168.20.0	255.255.255.0	192.168.20.254	192.168.20.254
192.168.30.0	255.255.255.0	192.168.30.254	192.168.30.254
192.168.40.0	255.255.255.0	192.168.30.2	192.168.30.254

Routeur RT2			
Destination	Masque	Passerelle	Interface
192.168.40.0	255.255.255.0	192.168.40.254	192.168.40.254
192.168.30.0	255.255.255.0	192.168.30.2	192.168.30.2
192.168.20.0	255.255.255.0	192.168.30.254	192.168.30.2
192.168.10.0	255.255.255.0	192.168.30.254	192.168.30.2

FIGURE 32 – Tables de routages des routeurs RT1 et RT2.

Chaque routeur doit donc connaître la route vers chacun des noeuds et segments du réseau pour pouvoir les joindre. Cependant, le réseau Internet est composé d'un grand nombre de noeuds et segments ce qui rend les tables de routage énormes. Afin de résoudre ce problème, on indique une route

par défaut. La route par défaut est la route qui sera utilisée lorsque aucune route spécifique pour aller vers la destination spécifiée n'aura été trouvée. Une destination par défaut peut être notée 0.0.0.0 et a pour masque 0.0.0.0. Ainsi, la Figure 33 représente une table de routage simplifiée pour le second routeur (RT2).

Routeur RT2			
Destination	Masque	Passerelle	Interface
192.168.40.0	255.255.255.0	192.168.40.254	192.168.40.254
192.168.30.0	255.255.255.0	192.168.30.2	192.168.30.2
0.0.0.0	0.0.0.0	192.168.30.254	192.168.30.2

FIGURE 33 – Tables de routages simplifiée.

2.4 Conclusion

Nous avons présenté dans ce chapitre les concepts et fonctionnements des modèles réseau en couches à savoir le modèle OSI et le modèle TCP/IP. En effet, cette modélisation en couches permet de définir au départ la division de la problématique générale de communication en plusieurs sous-problèmes qui sont résolus par des couches matérielles et logicielles relativement indépendantes les unes des autres mais qui collaborent pour le bon fonctionnement du réseau. Aussi, l'intérêt de cette approche permet aux étudiants de situer dès le départ les éléments conceptuels et physiques par rapport à des niveaux de fonctionnement tels que le niveau 1 physique et niveau 2 liaison de données. Nous aborderons par la suite les bases théoriques sur les quels repose la transmission des données.

Chapitre 3

Les bases théoriques de la transmission des données

Sommaire

3.1 Introduction

Les supports de communication permettent de transmettre des signaux physiques. Ces signaux, qui peuvent être de nature différente (électrique, optiques ou ondes électromagnétiques), sont codés de sorte à transporter les bits c'est-à-dire les 0 et les 1. La transmission des bits repose sur des principes théoriques de transmission du signal, que nous abordons brièvement dans ce chapitre [7].

3.2 Transmission numérique et analogique

Le but des réseaux est de transmettre des informations d'un ordinateur à un autre. Afin de transmettre des informations binaires (suites binaires composée de 0 et 1) sur un support de communication, Il est nécessaire de les transformer au préalable en un signal électrique. La technique de codage choisie diffère selon le type de données qui s'agir de : données textuelles, données audio ou données vidéos... Par exemple, un enregistrement vidéo ou audio est représenté par un signal analogique, c'est donc une courbe (avec un rait continu). Par contre, un texte ne peut prendre que des valeurs bien définies, en nombre limité, on parle alors de signal numérique. Un signal analogique est de type sinusoïdal par contre un signal numérique est un signal discret, voir la Figure 34 .

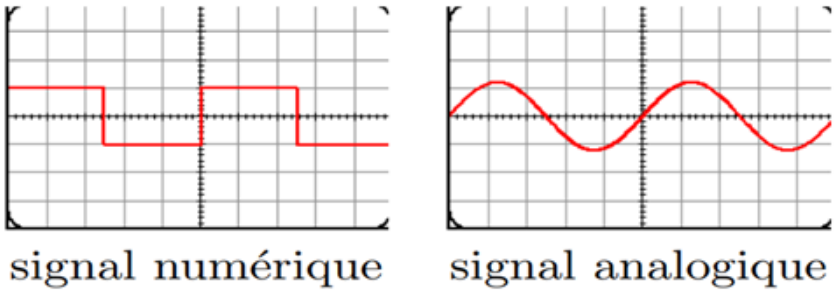


FIGURE 34 – Transmission numérique et analogique.

Lorsque l'information est représentée par la variation d'une seule grandeur physique (tension électrique, intensité lumineuse, etc), on parle dans

ce cas de *transmission numérique*. lorsque l'information est représentée par la variation des paramètres intrinsèques de l'onde, on parle dans ce cas de *transmission analogique* [4]. Une onde électromagnétique est caractérisée par *une fréquence*, *une amplitude* et *une phase*. Le signal est obtenu par la fonction : $Y = A\sin(2\pi ft + \varphi)$, où A est l'amplitude, $f = 1/P$ la fréquence (en Hertz) et P la période (en seconde), φ la phase (en radian).

Dans ce contexte, lorsque les données sont transmises, elles peuvent se trouver sous forme : numérique ou analogique .D'où les deux techniques de transmission des signaux : la transmission en bande de base et la transmission en large bande (par modulation).

3.2.1 Transmission en bande de base

Lorsque la transmission des données se fait sur quelques centaines de mètres, les informations peuvent être transmises sur le support de liaison à l'aide d'un signal numérique. Pour différentes raisons, le signal numérique n'est généralement pas transmis directement sur la ligne [3]. En effet, afin de pouvoir transmettre plus loin, le spectre du signal va être adapté à la bande passante du support d'où l'appellation : transmission en bande de base.

3.2.1.1 Codage en ligne

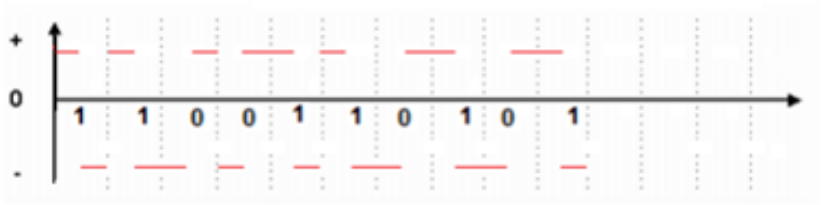
Codage en ligne, ou le transcodage est l'opération qui consiste à substituer au signal numérique (représentation binaire) un signal électrique mieux adapté à la transmission [3]. Les codages les plus utilisés peuvent être classés en deux catégories suivantes :

- ◇ Les codages à deux niveaux : le signal peut prendre uniquement une valeur strictement négative ($-X$) ou strictement positive($+X$), X représente une valeur de la grandeur physique permettant de transporter le signal.
- ◇ Les codages à niveaux multiples : le signal peut prendre une valeur strictement négative, nulle ou strictement positive ($-a$, 0 et $+a$).

Parmi les principaux codes utilisés, nous citons : NRZI, Manchester, Manchester Différentiel, Miller.

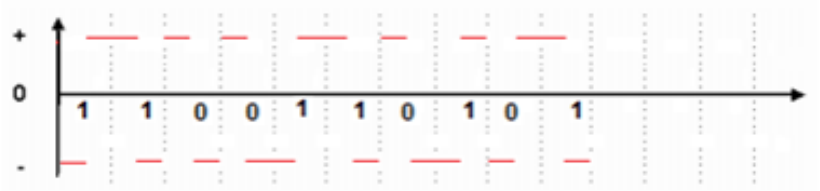
Exemple : Représentation de la suite binaire 1100110101 selon les codages : NRZI, Manchester, Manchester Différentiel, Miller. En considérant l'état initial $-a$, voir la Figures 36 et la Figures 35.

- Manchester $\begin{cases} si\ a_i = 1\ alors\ front\ descendant \\ si\ a_i = 0\ alors\ front\ montant \end{cases}$



- Manchester Différentiel (état initial= -a)

$\begin{cases} si\ a_i = 1\ alors\ pas\ de\ transition\ en\ début\ de\ bit \\ si\ a_i = 0\ alors\ transition\ en\ début\ de\ bit \end{cases}$



- Miller (état initial= -a)

$\begin{cases} si\ a_i = 1\ alors\ transition\ en\ milieu\ de\ bit \\ si\ a_i = 0\ alors\ pas\ detransition\ en\ milieu\ de\ bit \\ \quad et\ transition\ en\ début\ de\ bit\ 0 \\ \quad s'il\ est\ précédé\ par\ un\ bit\ 0 \end{cases}$

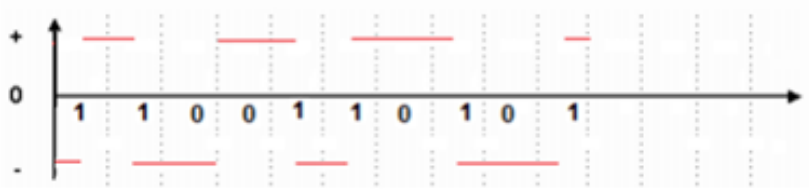


FIGURE 35 – Codages Manchester, Manchester Différentiel et et Miller.

• NRZI (état initial= -a) $\begin{cases} si\ a_i = 1\ alors\ transition \\ si\ a_i = 0\ alors\ pas\ de\ transition \end{cases}$

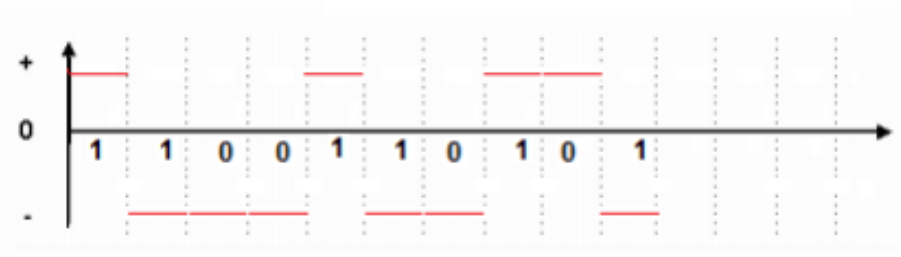


FIGURE 36 – Exemple de codages : NRZI.

3.2.2 Transmission par modulation

Dans le cas ou on souhaite transmettre des signaux numériques sur des distances qui vont au-delà d'un Kilomètre, alors il convient d'adapter le signal à transmettre. En effet, si la ligne de transmission est trop longue, même avec des vitesses de transmission peu élevées, les signaux numériques sont rapidement déformés [3]. Le signal numérique n'étant plus adapté, d'où la nécessité d'utiliser un signal de forme plus adaptée. Il s'agit du signal sinusoïdal.

Ainsi, pour transmettre les données numériques, on modifie, en fonction des données à transmettre, une ou plusieurs caractéristiques d'un signal sinusoïdal, appelé : signal porteur ou la porteuse.

Modifier une caractéristiques du signal porteur revient à effectuer ce qu'on appelle : la modulation. Ainsi, à l'émission on module la porteuse et à la réception l'opération inverse est effectuée : la démodulation. Le dispositif permettant d'effectuer ces deux opérations est : le modem (MODulation-DEModulation).

Moduler un signal sinusoïdal, c'est faire varier un ou plusieurs de ces paramètres. Suivant le type de paramètre, on distingue plusieurs types de modulations [3], voir la Figure 37 :

- ◇ Modulation d'amplitude.
- ◇ Modulation de fréquence.
- ◇ Modulation de phase.

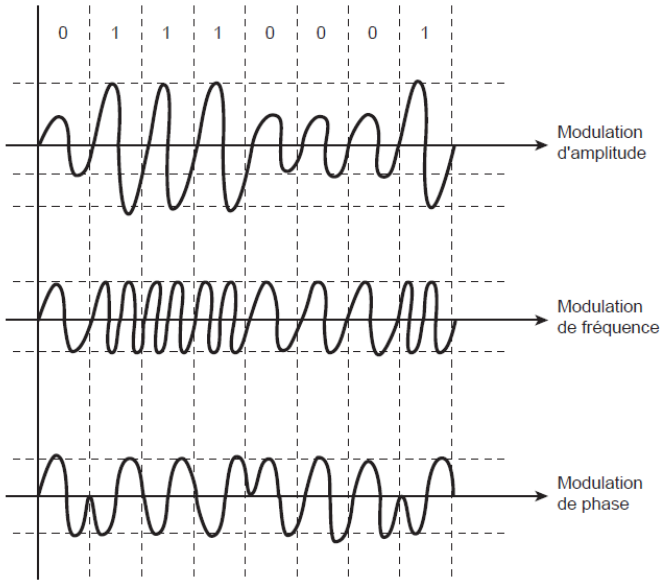


FIGURE 37 – Exemples de modulations simples [2].

3.3 Les modes de transmission

La transmission de données entre deux machines diffère selon :[4] :

- ◇ Le sens des échanges : Simplxe, half duplex et full duplex.
- ◇ Le mode de transmission : il s'agit du nombre de bits envoyés simultanément.
- ◇ La synchronisation entre émetteur et récepteur.

3.3.1 Simplxe, half duplex et full duplex

Trois modes d'exploitation peuvent être définis sur une liaison point à point reliant deux stations émettrices et réceptrices :

3.3.1.1 Mode simplex

En simplexe les données peuvent être transmises dans un sens fixé à l'avance. La commande d'un relais ou l'affichage sur un moniteur vidéo sont des exemples de ce type de transmission d'ailleurs très peu utilisé en

téléinformatique. Exemple : la liaison vers une imprimante réseaux. Voir la Figure 38.

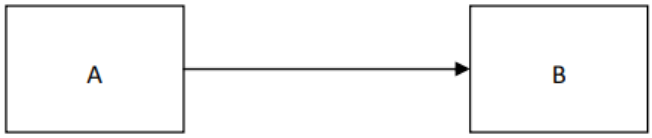


FIGURE 38 – Mode de transmission simplex.

3.3.1.2 Mode semi-duplex (half duplex)

En semi-duplex, les données peuvent être transmises dans un sens ou dans l'autre, nécessitant comme support deux fils seulement. Le choix du sens de transmission est commandé par le terminal. Exemple : une liaison avec câble coaxial. Voir la Figure 39.

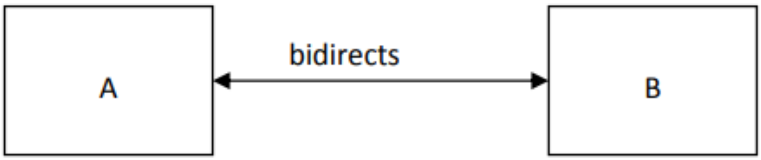


FIGURE 39 – Mode semi-duplex (half duplex).

3.3.1.3 Mode duplex(full duplex)

En duplex ou en duplex intégral, les données peuvent être échangées dans les deux sens à la fois, nécessitant ainsi deux paires de fils. Ce type de transmission est peu utilisé en téléinformatique. Exemple : une liaison à l'aide d'une paire torsadée. Voir la Figure 40.

3.3.2 Transmission série et parallèle

- ◇ **Transmission série :**en transmission série, tous les bits d'un mot ou d'un message sont transmis successivement sur une même ligne.

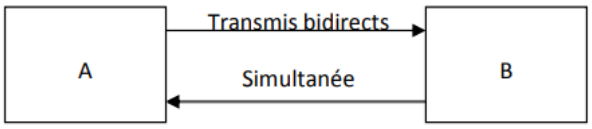


FIGURE 40 – Mode duplex(full duplex).

Ce mode de transmission n'utilise, pour la transmettre des données, que deux conducteurs. D'un coût moins élevé. Elle est adaptée aux transmissions sur des distances importantes.

◇ **Transmission parallèle :** La transmission parallèle est caractérisée par un transfert simultané de tous les bits d'un même mot. Ainsi, elle nécessite autant de conducteurs qu'il y a de bits à transmettre. Elle est utilisée pour des liaisons entre un calculateur, ses périphériques et ses unités de calcul esclaves.

La transmission parallèle est très performante en terme de débit. Cependant,étant donné que les fils conducteurs sont proches sur une nappe, des perturbations (notamment à haut débit), peuvent être générées dégradant ainsi la qualité du signal [6].

3.3.3 Transmission synchrone et asynchrone

◇ **Transmission synchrone :** Il s'agit de transmettre dans un intervalle constant sur lequel l'émetteur et le récepteur se sont accordés. La répétition de cet intervalle est continue. Les caractères sont envoyés de manière séquentielle, sans séparateurs. Ce mode convient aux débits importants.

◇ **Transmission asynchrone :** pas de relation établie à l'avance entre émetteur et récepteur. Deux signaux, les bits start et stop, encadrent les bits de chaque caractère. Une transmission débute à un instant quelconque.

3.4 Grandeurs caractéristiques d'une voie de transmission

Afin de transmettre un signal, on utilise des supports de transmissions. Quelques soit la nature du support utilisé, quelques propriétés communes caractérisent tous les supports de transmissions. Dans ce cours, nous présentons ces caractéristiques.

La bande passante (Bandwidth)

La bande passante est la caractéristique la plus importante d'un support de transmission, qui se comporte généralement comme un filtre qui ne laisse donc passer qu'une bande limitée de fréquences appelée bande passante ou intervalle de fréquences : $[W_{min}, W_{max}]$.

La largeur de la bande (W)

Il est important de distinguer la bande passante de la largeur de la bande. Cette dernière est calculée par : $W = W_{max} - W_{min}$, elle est exprimée en Hertz (Hz).

Exemples :

Une ligne téléphonique ne laisse passer que les signaux de fréquence comprise entre 300Hz et 3400Hz. Au dehors de cette bande les signaux sont fortement atténuée et ne sont plus compréhensible, on dit alors que la bande passante d'une telle ligne est de 3100Hz soit 3400–300 Hz. Par contre un câble coaxial utilisé dans les réseaux locaux a une bande passante nettement supérieure dont la largeur est de l'ordre des centaines de MHz (300 à 400 MHz).

La rapidité de modulation (R)

La rapidité de modulation ou la vitesse de modulation représente le nombre d'intervalles élémentaires dans une unité de temps (seconde) pour envoyer un symbole. Elle est exprimée en bauds. $R = \frac{1}{\Delta}$.

Autre définition : la rapidité de modulation est le nombre de changements d'états du signal par second.

Remarque :

Une voie de transmission ayant une largeur de bande passante W (Hz), ne peut transmettre des signaux dont la vitesse de modulation est supérieure à $2W$ (bauds) c'est-à-dire : $R \leq 2W$.

Exemple :

Une ligne téléphonique a une bande passante comprise entre 300 et 3400 Hz. La rapidité de modulation maximale est donc : R_{max} = 2.*(3100) = 6200(bauds).

La valence (v)

Est le nombre d'états (niveaux) nécessaires pour transmettre simultanément n bits. Elle est calculée comme suit : $v = 2^n$.

Rappel mathématique :

$y = a^x \Rightarrow x = \log_a(y)$, ainsi, $v = 2^n \Rightarrow n = \log_2(v)$.

Exemples :

Sur la Figure 41, un signal bivalent ce dit d'un signal qui présente 2 états correspondants à la valeur du bit (0 ou 1). Un signal quadrivalent présente 4 états significatifs et donc, il est possible de coder 2 bits avec une information électrique, par exemple 00 = -3V, 01 = -1V, 10= +1V, 11= +3V.

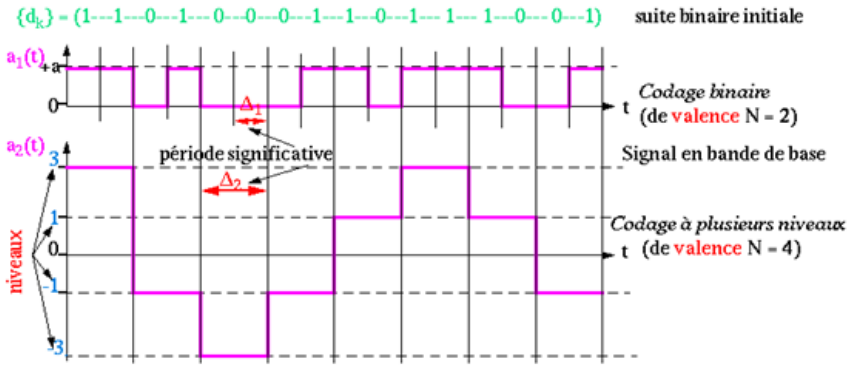


FIGURE 41 – Notion de valence d'un signal.

Le débit effectif ou utile (D)

Est la quantité d'information effectivement transmise par unité de temps. Il est calculé comme suit :

$D = \frac{Quantiteinformation(bits)}{Temps(secondes)}$, il est mesurée en (bits/s).

Le débit binaire maximum ou capacité D_{max}

Le débit maximum ou aussi appelé la capacité du canal, est mesurée en (bits/s) et il est calculé de deux manières différentes selon les cas : ligne bruitée ou sans bruit.

Le débit maximum sur ligne sans bruit

Dans le cas d'une ligne sans bruit, nous appliquons le (**théorème de Nyquist**) : $D_{max} = \frac{n}{T} = Rn = R\log_2(v) = 2W\log_2(v)$.

Le débit maximum sur ligne bruitée

La transmission de données sur une ligne ne se fait pas sans pertes. En effet, des parasites ou des dégradations du signal peuvent apparaître. Les parasites (souvent appelés bruit) sont l'ensemble des perturbations modifiant la forme du signal. On distingue généralement deux types de bruit :

- ◇ **Le bruit blanc :** c'est une perturbation uniforme du signal, c'est-à-dire qu'il rajoute au signal un petite amplitude dont la moyenne sur le signal est nulle. Le bruit blanc est généralement caractérisé par un ratio appelé rapport signal/bruit qui traduit le pourcentage d'amplitude du signal par rapport au bruit, son unité st le décibel (dB).
- ◇ **Les bruits impulsifs :** sont de petits pics d'intensité provoquant des erreurs de transmission.

Dans le cas d'une ligne bruitée, nous appliquons le (**théorème de Shannon**) :

$D_{max} = W \log_2(1 + \frac{PS}{PB})$, où $\frac{PS}{PB}$) est la puissance du signal sur puissance du bruit, ce rapport s'exprime sous forme logarithmique en décibel : $\frac{S}{B} = 10 \log_{10} \frac{PS}{PB}$

Le temps de propagation d'un signal (T_p)

Le temps de propagation T_p est le temps nécessaire à un signal pour parcourir un support d'un point à un autre. Ce temps dépend de la nature du support, de la distance et également de la fréquence du signal.

Le temps de propagation d'un signal (T_p)

Le temps de transmission T_t(dépend de la taille du message à transmettre et du débit supporté par la voie de transmission. Il correspond au rapport entre la taille du message et le débit de la ligne.

Le délai d'acheminement (D_a)

Correspond à la somme des temps de propagation et de transmission, $D_a = T_p + T_t$.

3.5 Conclusion

Nous avons présenté dans ce chapitre les éléments théoriques de base sur lesquels repose la transmission des données, tels que les signaux, la modula-

tion, les grandeurs caractéristiques comme le débit, la valence, la rapidité de modulation, etc. Le chapitre suivant concernera les méthodes déployées pour la gestion des erreurs de transmission.

Chapitre 4

Gestion des erreurs de transmission

Sommaire

4.1 Introduction

Le support physique n'est pas parfait et des problèmes (pertes, corruption, ...) peuvent survenir au cours de la transmission d'un message (trame) entre deux machines. Par exemple : un 1 s'est transformé en 0 ou vice versa, cela se produit, par exemple, lorsque les câbles dépassent la longueur maximale. Cela signifie qu'un signal de tension de 1 bit perd de l'amplitude lorsque l'énergie passe du signal au câble,ce problème est dit d'atténuation du signal, voir la Figure 42.

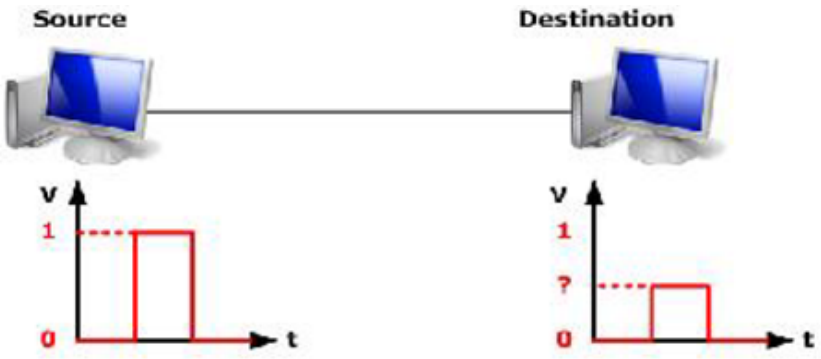


FIGURE 42 – Le problème d'atténuation.

Ces erreurs peuvent être détectées en rajoutant des bits de contrôle, aussi appelé des bits de redondance complétant les bits d'information et forment une suite de bits qui sera envoyée sur le support de transmission. Lorsque l'hôte reçoit la suite de bits, il applique les règles de décodage pour vérifier si les bits reçus comportent des erreurs. De ce fait, les équipements doivent posséder au minimum la propriété ou la fonctionnalité de détection d'erreurs survenue dans une trame reçue. Nous présentons dans ce cours les principales méthodes employées.

4.2 La détection des erreurs

Une méthode de détection d'erreurs doit permettre de constater qu'une erreur est apparue dans une trame. Elle ne fournit aucun détail sur le nombre d'erreurs, leur localisation, leur conséquence sur les données. Son seul but

est de signaler que la trame reçue est différente de celle envoyée, et donc de demander à l'émetteur une retransmission de la trame endommagée. Parmi ces méthodes, nous citons :

- ◇ La méthode de bit de parité.
- ◇ La méthode de redondance cycliques (CRC).

4.2.1 La méthode de bit de parité

Le contrôle de parité (appelé parfois VRC, pour Vertical Redundancy Check) est un des systèmes de contrôle d'erreurs les plus simples. La méthode utilise un seul bit de contrôle de la chaîne binaire. Il consiste à ajouter un bit supplémentaire (appelé bit de parité) aux trames envoyées de telle sorte qu'elles contiennent toujours un nombre de ≪1≫ pair (ou impaire dans le cas de code à bit de parité impaire). Pour être plus explicite il consiste à ajouter un ≪1≫ si le nombre de bits de la trame est impair, 0 dans le cas contraire. A l'arrivé, le récepteur vérifie pour chaque chaîne binaire reçue que la somme des ≪1≫ est paire (ou impaire), si ce n'est pas le cas, une erreur est détectée.

Avantages et inconvénients de la méthode

L'avantage de la méthode est qu'elle limite de données de contrôle de données insérées (un seul bit).

Parmi les inconvénients de cette méthode est qu'elle n'est pas très fiable :

- ◇ Si par exemple un bit à O est modifié à 1, et un autre bit passe de 1 à 0, le récepteur ne détecte pas d'erreur.
- ◇ Si une erreur survient sur le bit de parité, la vérification est faussée.

Exemple : Message original : 101010101

Message altéré : 101010110

4.2.2 Contrôle de parité croisé

Le contrôle de parité croisé (appelé LRC, pour Contrôle de redondance longitudinale ou Longitudinal Redundancy Check). Consiste à contrôler

l'intégrité des bits de parité d'un bloc de caractères. La Figure 43 est un exemple de cette méthode.

		LRC
	1001000	0
	1000101	1
	1001100	1
	1001100	1
	1001111	1
VRC	1000010	0

FIGURE 43 – Le contrôle de parité croisé.

4.2.3 Code de redondance cyclique

Aussi appelé le code polynomial ou contrôle de redondance cyclique. La méthode est très utilisée dans les protocoles réseaux de niveau liaison comme Ethernet ou Wi-Fi [7].

4.2.3.1 Principe de fonctionnement

Le CRC est basé sur le fait qu toute chaîne binaire permet de construire un polynôme, $I(x)$, tel que, chacun des bits donnant sa valeur au coefficient polynomial correspondant.

Exemple :

La suite 0101 sera associée au polynôme $0x^3 + 1x^2 + 0x^1 + 1x^0$ c'est à dire $x^2 + 1$.

Le CRC nécessite de choisir un polynôme dit générateur de degré "r" noté $G(x)$, qui va permettre le contrôle.

Exemple :

Un exemple de polynôme générateur normalisé : $x^{16} + x^{12} + x^5 + 1$

Avant l'émission, l'émetteur effectue un codage qui consiste à multiplier le polynôme associé à la chaîne binaire $I(x)$ par x^r, puis de le diviser par le polynôme générateur $G(x)$.

Le reste de la division $R(x)$ est concaténé à $x^r * I(x)$. Ce reste est appelé champ de contrôle d'erreur.

A la reception de la trame (message accompagné de plusieurs autres champs tel que l'adresse IP source et destination), le polynôme constitué à partir des données et du champ de contrôle est divisé parle polynôme générateur $G(x)$. Ainsi, deux cas peuvent se présenter :

- ◇ Cas 1 : Si le reste est nul, le récepteur déduit qu'aucune erreur n'est survenue.
- ◇ Cas 2 : Erreur, il demande à l'émetteur de lui retransmettre la trame.

4.2.3.2 Exemple :

Soit la chaîne binaire à transmettre 10001101. Soit le polynôme générateur $x^4 + x + 1$.

1. $G(x) = x^4 + x + 1 \Rightarrow r = 4$, $G(x) = 1x^4 + 0x^3 + 0x^2 + 1x^1 + 1x^0$. Ainsi, la chaîne binaire associée à $G(x)$ est $G(x) = 10011$;
2. Effectuer la multiplication $x^r * I(x) = x^4 * I(x) = 100011010000$;
3. On réalise la division polynômial de $x^r * I(x)$ par $G(x)$, il suffit de soustraire successivement $G(x)$ à $x^r * I(x)$ à partir de la partie gauche, voir La Figure 44.

Le polynôme à transmettre est $T(x) = 100011011010$. Le reste de la division de $T(x)$ par $G(x)$ est nul, ce qui peut être vérifié à titre d'exercice. Sinon, si on suppose qu'une erreur est apparue sur le cinquième bit par exemple, le reste de la division par $G(x)$ va être non nul.

Remarque :

Les opérations sur les bits sont des opérations Modulo 2. L'addition et la soustraction sont équivalentes et correspondent au "ou exclusif". La Figure 44 montre la division polynômial de $x^r * I(x)$ par $G(x)$.

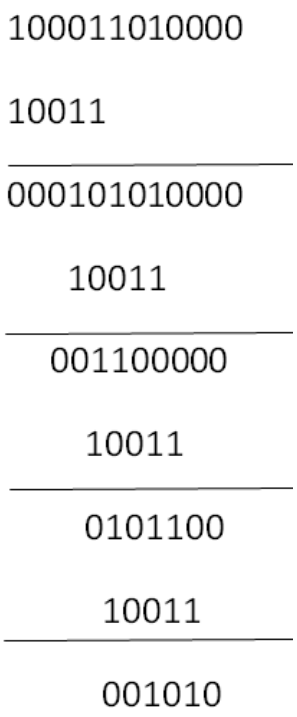


FIGURE 44 – La division polynômial.

4.3 La correction des erreurs

Une méthode de correction d'erreurs est beaucoup plus complexe qu'une méthode simplement détectrice. Elle doit transmettre en plus des données tout les bits nécessaires à la reconstitution du message en cas d'erreur à l'arrivée. Parmi ces méthodes, citons la méthode de Proposé par R. Hamming (1952).

4.4 Conclusion

Nous avons présenté dans ce chapitre quelques méthodes de gestion des erreurs de transmission, à savoir, la méthode de bit de parité,Contrôle de parité croisé ainsi qu'au Code de redondance cyclique. Le chapitre suivant concernera la segmentation des réseaux en domaines de diffusion et de collision dans les réseaux locaux.

Chapitre 5

Domaines de diffusion et domaines de collision

Sommaire

5.1 Introduction

Dans ce chapitre, nous présentons simplement les domaines de diffusion et de collision, ces deux notions ont un rapport avec les équipements d'interconnexion étudiés dans le chapitre précèdent, à savoir, le HUB, le SWITCH et le routeur. Mais avant cela, nous définissons quelques autres concepts liés.

5.1.1 Unicast, multicast et broadcast

Dans un réseau informatique, les termes unicast, multicast et broadcast sont des méthodes de transmission de l'information. En unicast(ou en français, monodiffusion), une machine transmet le message à une seule machine réceptrice. En multicast(ou multidiffusion), une machine transmet le message à un groupe de machines réceptrices conernées. Autrement dit, l'unicast est une communication un-à-un, tandis que multicast est un processus de communication un-à-plusieurs. Finalement, les messages diffusés (Broadcast messages) sont envoyés à toutes les machines du réseau. La Figure 45 illustre les trois concepts.

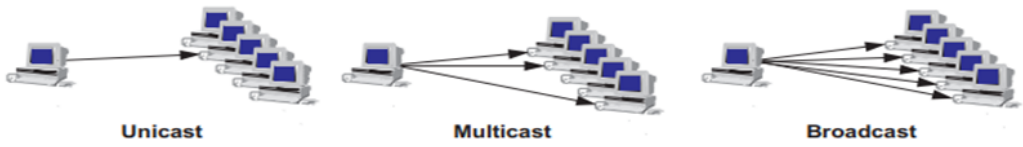


FIGURE 45 – Unicast, multicast et broadcast.

5.1.2 Définition d'un domaine de collision

Le problème de la collision se produit lorsque deux ordinateurs émettent simultanément des signaux sur le même média. Dans ce cas, les tensions des deux signaux binaires s'additionnent et génèrent un troisième niveau de tension, voir la Figure 46.

Un domaine de collision est un segment de réseau dans laquelle les paquets de données peuvent entrer en collision les uns des autres.

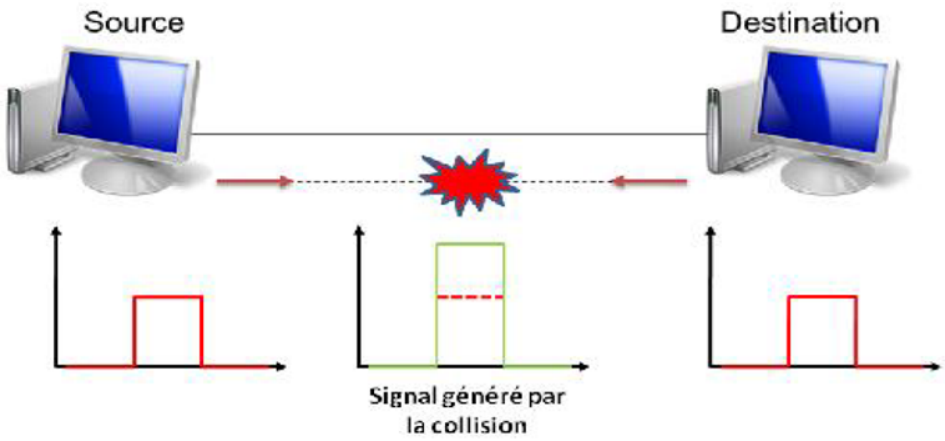


FIGURE 46 – Le problème de la collision.

5.1.3 Définition d'un domaine de diffusion

La diffusion est un mécanisme qui assure que tous les machines (hôtes) d'un réseau local reçoivent les messages de diffusion émises par n'importe quelle autre machine de ce même réseau. On appelle domaine de diffusion(broadcast domain) une zone d'un réseau informatique à l'intérieur duquel toutes les machines peuvent émettre et doivent recevoir des trames de diffusion. Comme dans le cas précédent, plus le nombre de machines présents dans le domaine de diffusion est important, plus les performances se dégradent. Ainsi, afin de garantir les meilleures conditions de communication, on cherche à réduire l'étendue du domaine de diffusion.

5.1.4 Comment réduire la taille des domaines de collision et de diffusion ?

Afin de garantir de meilleures conditions de communication, on cherche à réduire au maximum l'étendue du domaine de collision. Sur les réseaux filaires actuels, les domaines de collision ne posent plus de problèmes depuis que l'on utilise des commutateurs (switchs, ces derniers ont la vocation de constituer un circuit de communication unique entre deux hôtes. Une fois le circuit constitué, toute collision sera impossible.

Ainsi, La réduction des collisions se fait par l'installation des équipements

réseau : commutateurs (switchs), ponts (bridges) et routeurs qui sont capables de filtrer et de transmettre les paquets par leur adresse MAC.

Les concentrateurs (hubs) forment un seul domaine de collision alors qu'un routeur ou un commutateur (switch) en créent un par port ce qui réduit les risques de collisions.

Le routeur est le seul équipement qui segmente à la fois des domaines de collision et de diffusion.

5.1.5 Pourquoi segmenter les domaines ?

Segmenter les domaines de collision permet de :

◇ Réduction du nombre de collisions ;

◇ d'économiser la bande passante disponible.

Segmenter les domaines de diffusion permet :

◇ d'améliorer la sécurité ;

◇ de diminuer la taille des réseaux.

5.1.6 Types de segmentation

Les aptitudes des switchs, ponts et des routeurs à segmenter les réseaux en domaines de collision et/ou de diffusion sont une source de confusion. Comme chacun de ces équipements opère un niveau différent du modèle en couche (OSI, à voir dans les chapitres suivants) chacun réalise un type de segmentation différent. Il existe 3 types de segmentation :

◇ La segmentation par pont.

◇ La segmentation par commutateur (switch).

◇ La segmentation par routeur.

5.1.6.1 La segmentation par pont

Permet de segmenter le domaine de collision en deux grâce au pont, voir la Figure 47.

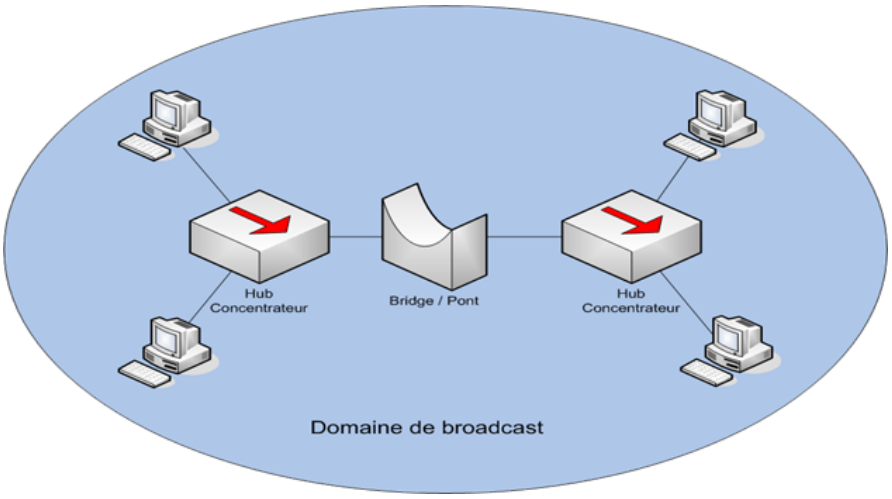


FIGURE 47 – La segmentation par pont.

5.1.6.2 La segmentation par commutateur(switch)

Permet de segmenter le domaine de collision par la mise en place de chemins commutés entre l'hôte et la destination. Cependant, tous les hôtes connectés au commutateur restent dans le même domaine de diffusion, voir la Figure 48.

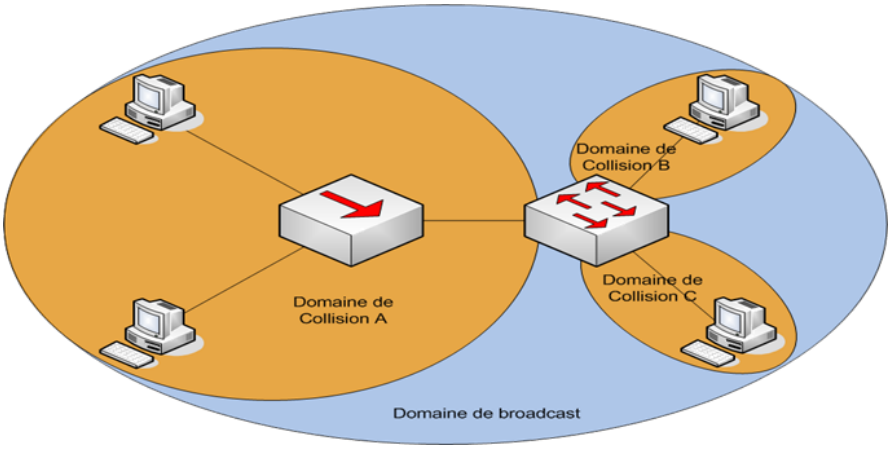


FIGURE 48 – La segmentation par commutateur(switch).

5.1.6.3 La segmentation par routeur

Permet de segmenter le domaine de diffusion en fonction des adresses réseau (adressages IP), voir la Figure 49.

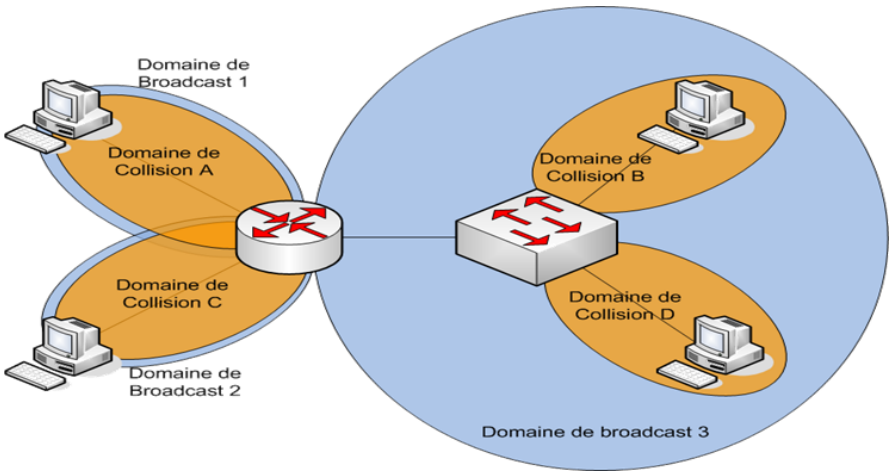


FIGURE 49 – La segmentation par routeur.

5.1.7 Réseaux locaux virtuels : VLANs

Nous avons vu que dans les réseaux locaux, les routeurs sont les seuls équipements permettant de segmenter les domaines de diffusion. Cependant, les commutateurs (switch)ont beaucoup évolués et disposent d'une fonctionnalité qui permet de segmenter logiquement le domaine de broadcast en plusieurs domaines de broadcast plus petits pour exploiter au maximum la bande passante de chaque domaine de collision. C'est le VLAN (Virtual LAN).

Le VLAN est un réseau local regroupant un ensemble de machines de façon logique et non physique.

A un VLAN correspond un domaine de broadcast.

La communication n'est autorisée qu'entre machines d'un même VLAN.

Les communications inter-VLAN doivent transiter par un routeur.

5.1.8 Quels sont les avantages des VLANs ?

L'utilité des VLANs apparaît,par exemple dans les points suivants :

- ◇ L'utilisation d'un seul switch physique pour plusieurs réseaux physiquement distincts.
- ◇ Plus de souplesse pour l'administration et la modification du réseau car toute l'architecture peut être modifiée par simple paramétrage des commutateurs.
- ◇ Gain en sécurité en contrôlant et empêchant tout dialogue entre équipent interconnectés sur un même commutateur, par des listes de contrôle d'accès.
- ◇ Réduction de la diffusion du trafic sur le réseau.

5.1.9 Quels sont les types des VLANs ?

La segmentation logique peut être effectuée de plusieurs manières, ainsi, il existe trois types de VLAN :

- ◇ Les VLANs de niveau 1 ou VLAN par port (Port-Based VLAN).
- ◇ Les VLANs de niveau 2 ou VLAN MAC (MAC Address-Based VLAN).
- ◇ Les VLANs de niveau 3 ou VLANs d'adresses réseaux (Network Address-Based VLAN)

5.1.9.1 Les VLAN de niveau 1 ou VLAN par port

Les Vlans par port associent un port d'un switch à un numéro de Vlan. Le switch entretien ensuite une table qui lie chaque Vlan au port associé. La configuration est statique, le déplacement d'une station implique son changement de VLAN. Dans la configuration de chaque port, on peut choisir que le port soit :

- ◇ Port Access (ou untagged, non étiqueté) : sur ce port, le switch va envoyer et recevoir uniquement des paquets sans ID précisé. Généralement utilisé pour un périphérique final tel qu'un ordinateur, une imprimante réseau, certains téléphones IP, etc.
- ◇ Port trunk (ou tagged, étiqueté) : sur ce port, tout paquet contient obligatoirement un ID de VLAN bien précis (on parle de norme 802.1q).

La Figure 50 est un exemple d'un VLAN de niveau 1.

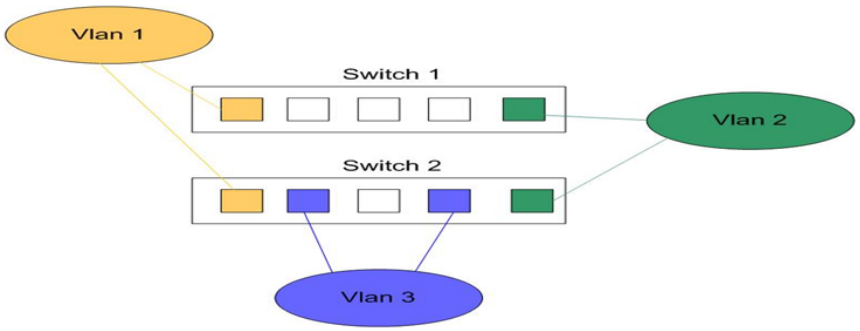


FIGURE 50 – VLAN de niveau 1.

5.1.9.1.1 Répartition de VLANs sur plusieurs équipements Les réseaux locaux sont distribués sur différents équipements via des liaisons logiques appelées trunks. Le trunk est une connexion sur laquelle on transmet le trafic de plusieurs réseaux virtuels. Les trames qui traversent le trunk sont complétées avec un identificateur de réseau local virtuel (VLAN id). Grâce à cette identification, les trames sont conservées dans un même VLAN (ou domaine de diffusion). Les trunks peuvent être utilisés :

- ◇ Entre deux switchs : C'est le mode de distribution des réseaux locaux le plus courant.
- ◇ Entre un switch et un routeur : C'est le mode fonctionnement qui permet d'accéder aux fonctions de routage ; donc à l'interconnexion des réseaux virtuels par routage inter-VLAN.

5.1.9.2 Les VLAN de niveau 2 ou VLAN MAC

Ces VLANs associent les stations par leur adresse MAC. Ce type est beaucoup plus souple que VLAN par port car le réseau est indépendant de la localisation de la station. Cependant, il offre une sécurité moindre que le VLAN par port car il est possible d'usurper une adresse MAC. La Figure 51 est un exemple d'un VLAN de niveau 2.

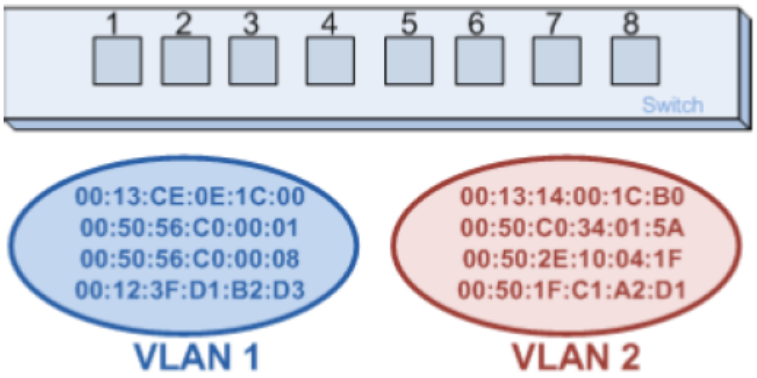


FIGURE 51 – VLAN de niveau 2.

5.1.9.3 Les VLAN de niveau 3 ou VLAN IP

Les Vlans de niveau 3 permettent de regrouper plusieurs machines suivant le sous réseau auquel elles appartiennent. Les utilisateurs d'un VLAN de ce niveau sont affectés automatiquement à un VLAN en fonction de leurs adresses IP. Cependant, nécessite d'utiliser des équipement coûteux assurant la prise en charge des adresses IP. L'usurpation d'adresses IP est plus simple à mettre en œuvre que l'usurpation d'adresses MAC. La Figure 52 est un exemple d'un VLAN de niveau 3.

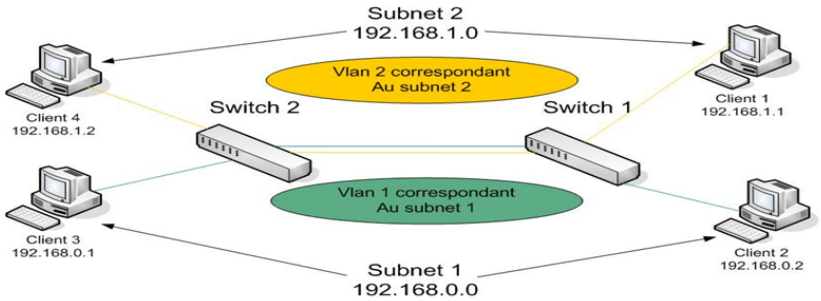


FIGURE 52 – VLAN de niveau 3.

5.2 Conclusion

Nous avons présenté dans ce chapitre le principe de la segmentation des réseaux en domaines de diffusion et de collision dans les réseaux locaux en utilisant les différents équipements d'interconnexion des réseaux et le concept des réseaux locaux privés (VLAN). Cette segmentation apporte beaucoup d'avantages tels que, la réduction du trafic sur le réseau et diminution des collisions, gain en sécurité et contrôle d'accès et enfin, plus de souplesse pour l'administration et la modification des réseaux.

Série d'exercices

TD N°1 Généralités sur les réseaux informatiques

Partie 1 : Généralités et définitions

Exercice 1:

Compléter le paragraphe suivant par la liste des mots suivants:

communication, partager, réseau, d'équipements, informations, logiciels.

Un ……..……informatique est un ensemble ……informatiques (matériels et ……..) reliés entre eux par des moyens de ……permettant d'échanger des ……et de ……..des ressources matérielles et logicielles.

Exercice 2:

Indiquez le type de réseau (LAN /MAN /WAN) pour chacun des cas suivants :

Un réseau qui relie les ordinateurs de votre école	
Un réseau qui relie les ordinateurs d'une société sur la ville d'Oran	
Un réseau qui relie tous les bureaux de la poste sur l'Algérie	
Le réseau Internet	
Un réseau qui relie les ordinateurs de votre maison	

Exercice 3:

Considérer les deux schémas (schéma 1 et schéma 2) suivants

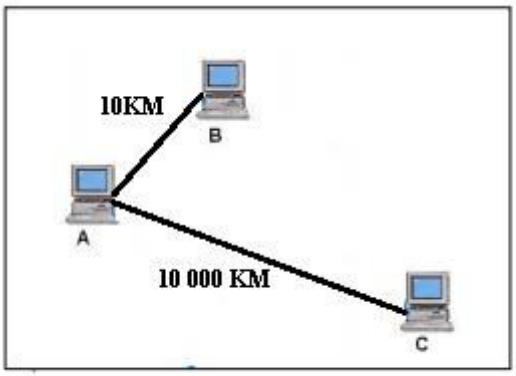


Schéma 1

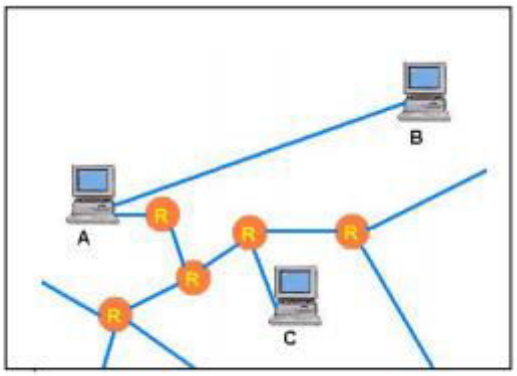


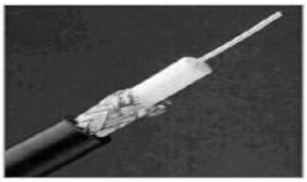
Schéma 2

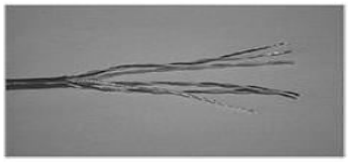
1. Comparer le débit entre l'ordinateur A et l'ordinateur B avec le débit entre A et C.
2. En se basant sur les constatations précédentes, compléter le paragraphe ci-dessous, par les mots suivants : relais, distance, information, courte, moins

Le débit dépend de la ……..et du nombre des ……..intermédiaires qui seront nécessaires à l'acheminement des .....…, plus la distance est ……. et ……il y aura des relais, plus le débit sera fort et inversement.

Partie 2 : Supports de transmission

Identifiez les supports physiques suivants:

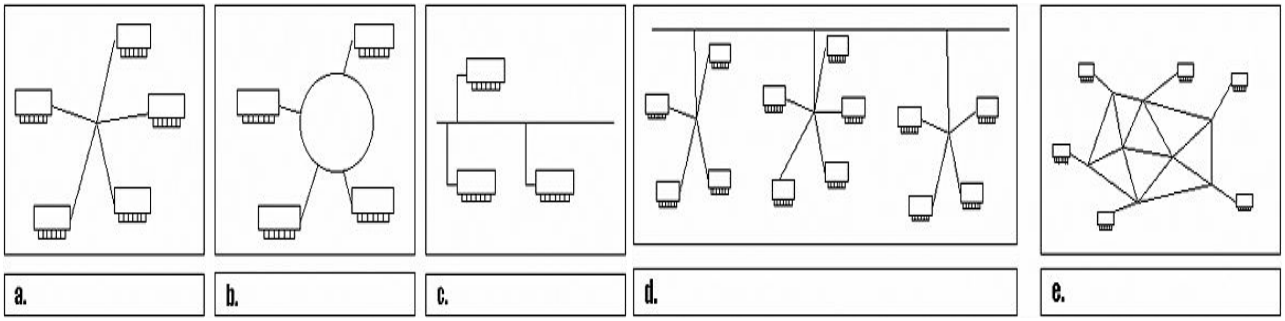




Partie 3 : Topologies et équipements d'interconnexion

Exercice 1:

Précisez quelles topologies sont représentées ci-dessous :



Exercice 2: Soit un réseau d'une entreprise de vente de matériels industriel en ligne ayant la topologie et les équipements suivants :

- Un service administratif, installé dans un bâtiment A, ayant un réseau local en étoile reliant trois ordinateurs Al, A2 et A3 et un serveur (SA) connecté à internet hébergeant le site de l'entreprise.
- Un réseau local en bus pour la gestion des commandes reliant 4 ordinateurs (B1, B2, B3, B4) est situé dans autre bâtiment B, distant de 120m du bâtiment A dans lequel est placé un serveur gestion des commandes en ligne (SB).
- Un serveur de base de données de stocks (SC) est situé dans un troisième bâtiment C, dans lequel le serveur est connecté à 4 postes de travail (C1, C2, C3, C4) par un ancien réseau Token ring pour la gestion des stocks (mise à jour du matériel)
- (SC) est relié aux serveurs (SB) et (SA).
- Un Switch à quatre (04) ports d'entrée/sortie.
- Un routeur à quatre (04) ports d'entrée/sortie, dont l'une sert de connexion à l'internet.
- Des câbles en paires torsadées (TP), des câbles coaxiaux (TX), des MAU (multi station Access Unit).

Représenter l'architecture du réseau d'interconnexion de cette entrepris.

TD N°2 Adressage physique

Exercice 1 :

Pour chaque adresse MAC ci-dessous, indiquez celles qui sont globales, administrées localement, destinées à identifier un équipement et déstinées à identifier un groupe d'équipements:

1. 58:54:ca:fa:4e:f7
2. 55:ca:58:fa:4e:f7
3. ff:ff:ff:ff:ff:ff

Le constructeur Bidule se voit attribuer le numéro OUI 06:11:43 par l'IEEE. Est-ce un numéro valide?

Exercice 2 : Soient les adresses MAC suivantes:

a) 01-00-5E-AB-CD-EF
b) 11-52-AB-9B-DC-12
c) 00–01–4B-B4-A2-EF
d) 00-00-25-47-EF-CD

Ces adresses peuvent-elles appartenir au champ adresse source d'une trame Ethernet ?

Exercice 3 :

Soient les adresses MAC suivantes, précisez celles qui constituent des adresses valides c'est-à-dire qui peuvent être attribuées à une carte réseau. Expliquez pourquoi.

a) 00-A0-B0-F9-H3-11
b) 10-20-30-40-50-60
c) 00–A0–FF-10-G7-99
d) 00-99-00-11-00
e) FF-FF-FF-FF-FF-FF
f) C0-00-10-20-30-72

Exercice 4 :

En vous aidant d'internet, identifier les constructeurs des adresses MAC ci-dessous :

a) 00-01-43-20-41-F4
b) 00-50-F2-02-34-A1
c) 00–01–02-83-BC-31
d) 00-02-B3-72-19-DE
e) 00-04-DC-95-11-28
f) 00-0B-C5-73-8B-C6

TD N°3 Domaines de collision et de diffusion

Exercice 1 :

Examiner les schémas suivants (1-4) qui montrent des exemples de réseaux. Combien de domaines de diffusion et de collision y a-t-ils dans chaque schéma?

Schéma 1 : le réseau suivant comporte deux Switchs (commutateurs), un hub (concentrateur), un MAU (Multistation Access Unit) et un routeur ainsi que trois groupes d'ordinateurs.

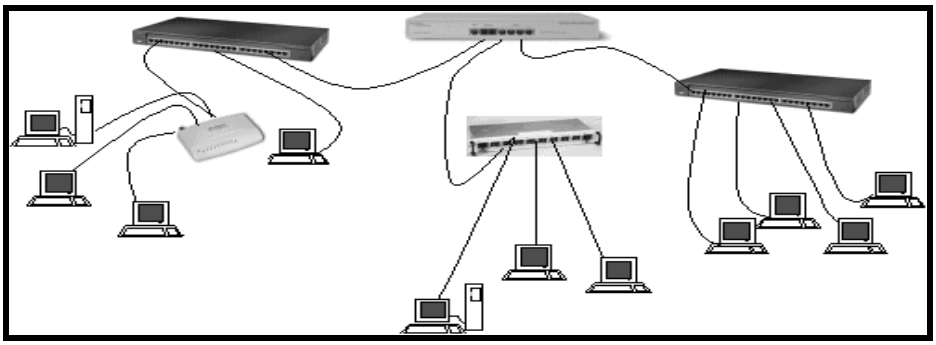


Schéma 2 : le réseau suivant comporte trois ordinateurs, un hub et un commutateur.

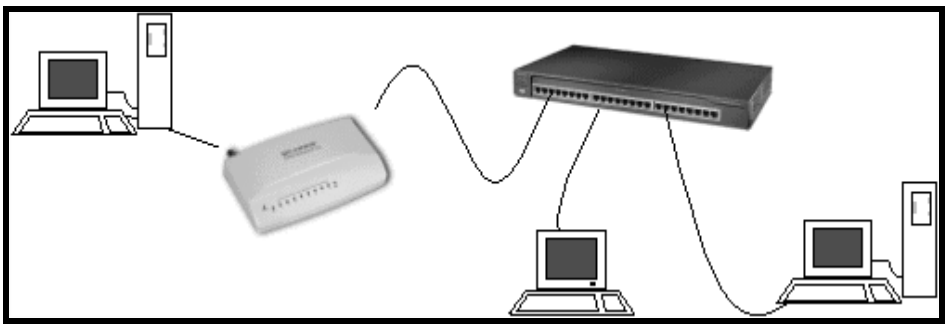


Schéma 3 : le réseau suivant comporte cinq ordinateurs, deux commutateurs et deux routeurs.

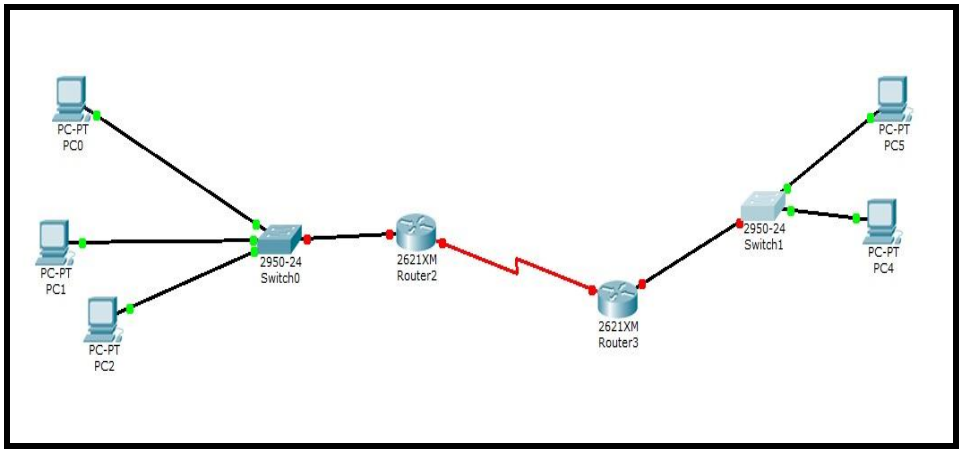
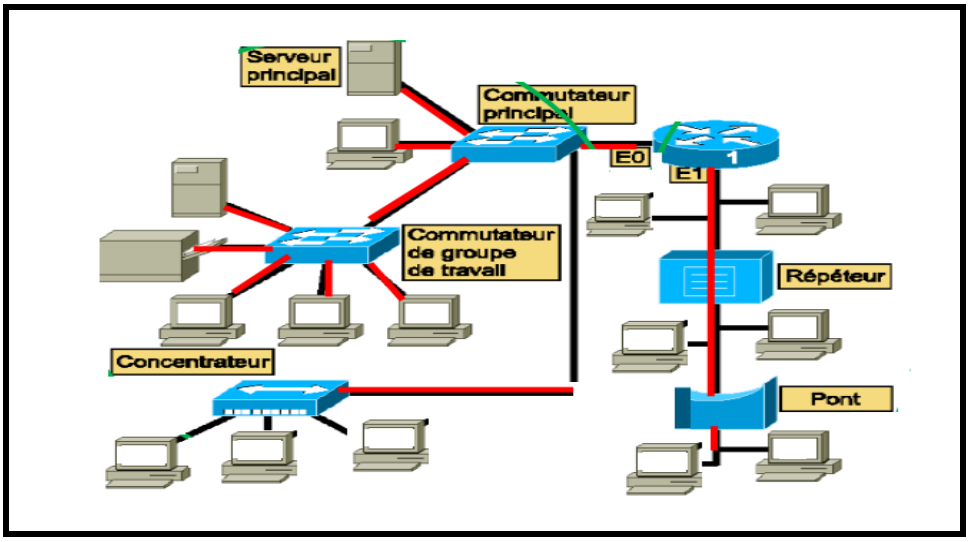
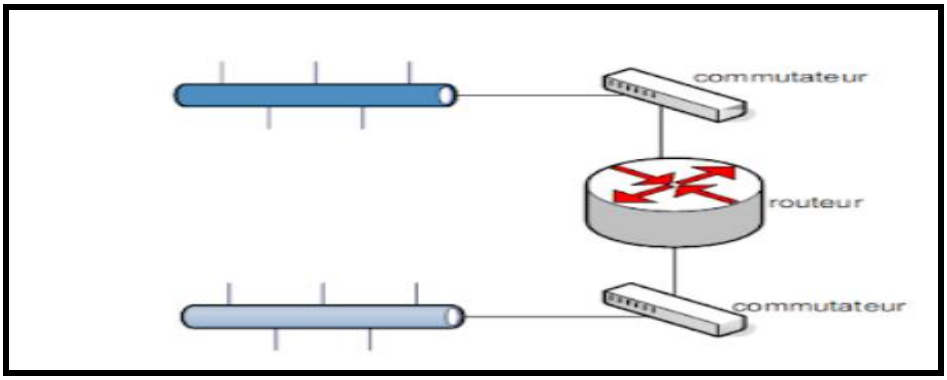


Schéma 4 :

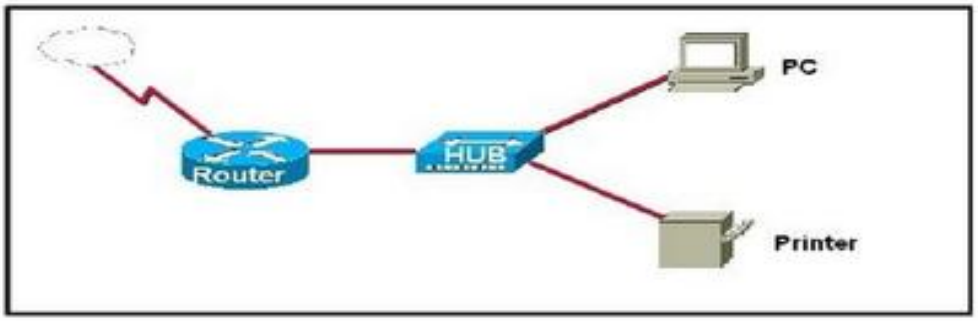


Exercice 2: Soit le réseau suivant :



1. Combien y a-t-il de domaine de diffusion et de collision ?
2. Si on enlève le routeur et qu'on relie les deux commutateurs, Combien y aura-t-il de dc et dd ?

Exercice 3 : Quels sont les équipements du schéma suivant qui doivent disposer d'une adresse MAC ?



1. L'ordinateur et le routeur.
2. Uniquement l'ordinateur.
3. L'ordinateur, le concentrateur et le routeur.
4. L'ordinateur, l'imprimante et le routeur.

TD N°4 Grandeurs caractéristiques d'une voie de transmission

Exercice 1:

Soit une ligne de transmission avec une largeur de la bande passante de 1000 Hz. La rapidité de modulation est de 1200 bauds et les signaux sont de valence 16.

1. Quel est le débit binaire de la ligne ?
2. Quelle est la valeur minimale du rapport S/B afin d'obtenir ce même débit ?
3. On suppose que la ligne présente un rapport S/B afin d'obtenir ce même débit ?
4. On suppose que la ligne présente un rapport S/B de 34 db. Quel est le débit maximum de cette ligne ?

Exercice 2:

Un système de transmission numérique fonctionne à un débit de 9600 bits/s. Sachant qu'on transmet 4 bits par intervalle de temps élémentaire.

1. Quelle est la largeur de bande minimale nécessaire de la voie ?

Exercice 3:

Soit une ligne téléphonique ayant une modulation quadrivalente d'amplitude et bivalente de phase.

1. Déterminer la rapidité de modulation sachant que le débit binaire est de 4800bits/s.
2. Calculer le débit maximum.

Exercice 4:

Pour transmettre des vidéos numériques ayant les caractéristiques suivantes : chaque image est une matrice de 640 X 480 pixels , tel que chaque pixel peut prendre un valeur parmi 32 intensités différentes. La vitesse requise est de 25 images par seconde.

1. Quelle est la vitesse de transmission?
2. Etant donné que le canal possède une bande passante de 4.5 MHz et un rapport S/B de 35 db, peut-on transférer ce signal vidéo sur ce canal ?

Exercice 5:

Un modem fonctionne à 9600 bits/s sur un canal de bande passante de 500 à 2900 Hz. On utilise une modulation de phase à 8 états avec une amplitude bivalente pour chaque état.

1. Calculer la valence du signal modulé.
2. Calculer les rapidités de modulation maximales et effectives.
3. Calculer le rapport signal, bruit limite pour un fonctionnement correct du modem.

Exercice 6:

On veut utiliser la bande 64 KHz – 200 KHz pour assurer un débit de 544 Kbits/s sur le flux montant d'un modem ADSL.

1. Calculer la valence du signal modulé.

Exercice 7:

Le constructeur ALCATEL ER 4820 indique que le type de modulation retenu est une modulation octovalente de phase. Sachant que la rapidité de modulation vaut 1600 bauds. Calculer le débit binaire effectif en bit par seconde.

Exercice 8:

Le constructeur du modem TELSTAT 1030 indique que le type de modulation retenu est une modulation octovalente de phase combinée à une modulation bivalente d'amplitude. Etant donné la rapidité de modulation est de 2400 bauds. Calculer la vitesse de transmission ou débit binaire en bits par seconde.

Exercice 9:

Sachant que le RTC (Réseau Téléphonique Commuté) présente une vitesse de modulation maximale de 6200 bauds, quelle est la vitesse maximale de transmission si l'on utilise une modulation à huit états ?

Exercice 10:

Calculer le temps de transmission et le temps de propagation d'un fichier de 20 KO sur un réseau ETHERNET à 10 Mbits/s et pour des distances de 10 m, 100 m et 1 Km.

.

TD N°5 sur l'adressage IP

Exercice 1 :

a) Trouvez la classe des adresses IP suivantes :

1. 10000000. 00001010. 11011000. 00100111
2. 11101101. 10000011. 00001110. 01011111
3. 01001010. 00011011. 10001111. 00010010
4. 11001001. 11011110. 01000011. 01110101
5. 10000011. 00011101. 00000000. 00000111

b) Pour chaque adresse IP suivante, indiquez les parties Net-ID et Host-ID :

1. 1.102.45.177
2. 196.22.177.13
3. 133.156.55.102
4. 221.252.77.10
5. 123.12.45.77

Exercice 2:

Une machine est configurée avec l'adresse IP **172.128.10.5** et un masque de réseau **255.255.192.0**.

1. Déterminez l'adresse du réseau.
2. Déterminez le nombre d'adresses utilisables.
3. Déterminez l'adresse du broadcast (diffusion) du réseau.
4. Donnez la plage adressable du réseau.
5. Mêmes questions pour l'adresse IP **172.26.17.100** et le masque de réseau **255.255.240.0**, l'adresse IP **193.48.57.163** et le masque de réseau **255.255.255.224** et l'adresse IP **192.168.1.1** et le masque de réseau **255.255.255.0.**

Exercice 3 :

Une société veut utiliser l'adresse IP **192.168.90.0** pour **4** sous réseaux.
Le nombre maximum d'hôtes par sous-réseau étant de **25**, quel masque de sous réseau utiliseriez-vous pour résoudre ce problème ?

Exercice 4 :

Afin de disposer de sous réseaux on utilise le masque de **255.255.240.0** avec une adresse de réseau de **classe B**.

1. Combien d'hôtes pourra-t-il y avoir par sous-réseau ?
2. Quel est le nombre de sous-réseaux disponibles ?

Exercice 5 :

Indiquez pour chacune des plages d'adresses IP suivantes, le réseau et le masque en notation CIDR comme indiqué dans l'exemple :

Plage d'adresses	**notation CIDR**
Ex : 10.0.0.1. -- 10.255.255.254	10.0.0.0 / 8
172.16.80.1 -- 172.16.87.254	
192.168.15.117 -- 192.168.15.118	
172.16.0.1 -- 172.31.255.254	
10.1.64.1 – 10.1.127.254	
210.44.8.81 -- 210.44.8.94	

Exercice 6 :

Une entreprise dispose de l'adresse IP réseau suivante **40.0.0.0**. Elle souhaite segmenter son réseau sous-réseaux. Donnez le plan d'adressage pour le diviser en **20** sous-réseaux selon le tableau suivant :

	Adresse du sous-réseau	**Première adresse IP d'hôte**	**Dernière adresse IP d'hôte**
Le premier Sous-réseau			
Le 2ème			
Le 3ème			
…			
Le dernier			

Conclusion générale

Les réseaux informatiques sont aujourd'hui omniprésents et font partie de notre vie quotidienne. En effet, nous les utilisons pour la réservation de billets et le retrait d'argents dans les banquent et distributeurs automatiques, pour surfer sur le web et envoyer des messages et des mails.

Ce document propose un support pédagogique à destination des étudiants de l'Ecole Supérieure en Génie Electrique et Energétique d'Oran (ESG2E) dans le cadre du module « Informatique ». Il correspond au premier semestre du programme du module « Informatique » enseigné en deuxième année du cycle de spécialité.

Le polycopié est structuré autour de cinq chapitres. Le premier chapitre présente des concepts généraux sur les réseaux informatiques du point de vue: fonctionnement, composants de base, différentes topologies et supports de transmission. Ainsi qu'aux différents équipements d'interconnexion nécessaires à la transmission de données dans un réseau. Nous aborderons par la suite dans le chapitre 2 : l'architecture en couche et modèle TCP/IP cette modélisation en couches permet de définir au départ la division de la problématique générale de communication en plusieurs sous-problèmes qui sont résolus par des couches matérielles et logicielles relativement indépendantes les unes des autres mais qui collaborent pour le bon fonctionnement du réseau. Dans le troisième chapitre les éléments théoriques de base sur lesquels repose la transmission des données, tels que les signaux, la modulation, les grandeurs caractéristiques comme le débit, la valence, la rapidité de modulation, etc. Le chapitre suivant concernera les méthodes déployées pour la gestion des erreurs de transmission. Finalement, le cinquième chapitre présente le principe de la segmentation des réseaux en domaines de diffusion et de collision dans les réseaux locaux en utilisant les différents équipements d'interconnexion des réseaux et le concept des réseaux locaux privés (VLAN).

Le polycopié a comporté également des séries d'exercices de contrôle et d'application des connaissances correspondantes aux éléments introduits dans chaque chapitre.

Bibliographie

[1] Black, Uyless. *Les réseaux*. Pearson, 2011.

[2] Danièle DROMARD, Dominique SERET. *Architecture des réseaux, synthèse des cours et exercices corrigés*. Pearson, 2009.

[3] J F Hérold, O Guillotin, P Anaya. *Informatique industrielleet réseaux en 20 fiches*. Dunod, 2010.

[4] N. Salmi, A. Abdeli. *Réseaux et télétraitements*. Pages Bleues, 2016.

[5] Pujolle, Guy. *Initiation aux réseaux, cours et exercices*. Eyrolles, 2001.

[6] Servin, Claude. *Réseaux et télécoms, Cours et exercices corrigés*. Dunod, 2003.

[7] Stéphane Catloin, Antoine Gallais, Stella Marc-Zwecker Julien Montavont. *Mini manuel des réseauxinformatiques, cours+exos corrigés*. Dunod, 2012.