**CHAPITRE. II. GENERALITE SUR LES RESEAUX**

**INFORMATIQUE**

1. **INTRODUCTION**

Dans l’univers des télécommunications, nous allons nous occuper d’un espace bien défini, celui des communications numériques, c’est à dire des échanges d’informations déjà numérisées, soit d’origine digitale, soit échantillonnées et quantifiées préalablement. Dans cette catégorie d’échange se situent tous les transferts de données existant sous forme binaire ou octet (généralement exprimer en base hexadécimal).

Les réseaux informatiques sont nés du besoin de relier des terminaux distants à un site central puis des ordinateurs entre eux et en fin des machines terminales, telles que des stations de travail ou des serveurs.

Enfin, nous allons parcourir et expliquer les différents concepts de base du réseau informatique tout au long de ce chapitre.

**2**. **DEFINITION DU RESEAU INFORMATIQUE**

Un réseau est un ensemble d'objets interconnectés les uns avec les autres. Il permet de faire circuler des éléments entre chacun de ces objets selon des règles bien définies. Dans le cas où les objets sont des ordinateurs on parle d’un réseau informatique.

Les réseaux informatiques qui permettaient à leur origine de relier des terminaux passifs à de gros ordinateurs centraux autorisent à l'heure actuelle l'interconnexion de tous types, d'ordinateurs que ce soit de gros serveurs, des stations de travail, des ordinateurs personnels ou de simples terminaux graphiques.

**4. HISTORIQUE DES RESEAUX DE COMMUNICATION**

Peu après la seconde guerre mondiale, nous sommes à l'aube de la micro-informatique. Seules les grandes entreprises pouvaient se doter de matériel informatique. Le seul moyen d'échanger des données de station à station était la disquette. Pour un même département, cela ne posait guerre de problèmes. Cependant, la chose devenait plus compliquée lorsqu'il s'agissait d'un bureau situé à un autre étage, ou dans un autre bâtiment. La taille des entreprises croissant au fil du temps, il a fallu envisager un autre mode d'échange des données.

Vers 1960, des ingénieurs, tant du secteur militaire qu'industriel se sont penchés sur ce problème. Le consortium "D.I.X." (Digital, Intel, Xerox) à effectuer des recherches et est parvenu à développer un moyen de communication de poste à poste plus direct. Leur travail, a abouti à la naissance de ce que nous appelons aujourd'hui communément "carte réseau." L'appellation correcte de ce type de matériel est "carte d'interface réseau."

Les réseaux "primitifs" se composaient d'un ordinateur central (mainframe) et de terminaux. Ces stations étaient dépourvues de disques durs et servaient à l'échange pur et simple de caractères avec le poste central. Digital et IBM sont parmi les pionniers avec leur système DECnet, qui constituera un ancêtre de nos réseaux actuels.

Un problème existait néanmoins, chaque fabricant usait de protocoles et de standards propriétaires. Il était donc impossible de faire communiquer des machines de fabricants différents.

La guerre froide couvant, le département américain de la défense (Department of Defense) étudia un moyen de communication fiable et à même de fonctionner en temps de guerre. Ils créèrent le réseau Arpanet (Advanced Research Projects Agency Network.) ARPAnet interconnectait différents points stratégiques par un réseau câblé et reliait le Royaume-Uni par satellite.

C'est aussi la naissance d'un protocole de communication devenu au fil du temps incontournable : TCP/IP. Grâce à ce protocole, les données peuvent atteindre leur destination indépendamment du média. Si un média est hors d'usage, les données sont acheminées malgré tout via un autre.

**5. ARCHITECTURE RESEAUX**

Le réseau permet de connecter des ordinateurs entre eux. Mais les besoins sont très divers, depuis le réseau domestique ou d'une toute petite entreprise jusqu'aux réseaux des grandes sociétés.

Voyons deux approches fondamentalement différentes, encore que l'une puisse facilement évoluer vers l'autre.

* 1. **. LES RESEAUX POINTS A POINTS "PEER TO PEER"**

Cette architecture est en fait un réseau sans serveur constitué de deux ou plusieurs ordinateurs, les ressources sont donc libres de partager ou non.

Les postes de travail sont simplement reliés entre eux et aucune machine ne joue un rôle particulier, chaque poste peut partager ses ressources avec les autres. C'est à l'utilisateur de définir l'accès à ses ressources et il n'y a pas obligatoirement un administrateur attitré.

* 1. **RESEAU CLIENT / SERVEUR**

L'architecture client-serveur s'appuie sur un poste central (serveur) qui envoi des données aux machines clientes. Des programmes qui accèdent au serveur sont appelés programmes clients (client FTP, client mail, etc.).

Les ressources réseau sont centralisées, un ou plusieurs serveurs sont dédiés au partage de ces ressources et en assurant la sécurité. Les postes de travail ne sont en principe que des clients, ils ne partagent pas des ressources, ils utilisent celles qui sont offertes par les serveurs.

Ce type de réseau est évidemment le plus performant et le plus fiable. Vous l'aurez compris, ce n'est pas la solution la plus simple pour un réseau domestique, c'est cependant ce type d'architecture que l'on retrouve sur les réseaux d'entreprise, qui peut parfaitement supporter plusieurs centaines de clients, voire plusieurs milliers.

**6. TYPOLOGIES DE RESEAUX**

On peut distinguer différents types de réseaux selon plusieurs critères tel que (la taille de réseau, sa vitesse de transfert des données et aussi leur situation géographique). Dans les points suivants nous allons nous allons parlé du type de réseau selon leur situation géographique.

## Le PAN (Personal Area Network)

Le PAN permet d’échanger des données entre des appareils proches (généralement dans la même pièce). Pour ce faire, il existe 2 techniques de transmission physique, l’USB et le FireWire. Il est également possible de relier deux appareils via le WPAN (réseau personnel sans fil) avec des technologiques comme l’USB sans fil, le Bluetooth ou le Z-Wave. Il est également possible de relier un réseau PAN vers d’autres réseaux plus grands.

**6.1 Le LAN (Local Area Network) en français Réseau Local :**

Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie (la plus répandue étant Ethernet).

Le LAN permet de transmettre une grande quantité de données rapidement. Celui-ci vous permet de partager des serveurs de fichiers, imprimantes ou encore des applications.  Il est également possible de se connecter via le WLAN (Wireless Local Area Network) ou réseau local sans fil (Wifi).  Bien que les deux solutions soient possibles, l’Ethernet offre plus de sécurité et un débit de données plus important.

**6.2 LE MAN (METROPOLITAIN AREA NETWORK):**

Le MAN interconnecte plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants. Ainsi un MAN permet à deux nœuds distants de communiquer comme s’ils faisaient partie d'un même réseau local.

**6.3 LE WAN (WIDE AREA NETWORK) OU RESEAU ETENDU:**

Le WAN interconnecte plusieurs LAN à travers de grandes distances géographiques. Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons qui augmente avec la distance et peuvent être faibles.

Les WAN fonctionnent grâce à des routeurs qui permettent de "choisir" le trajet le plus approprié pour atteindre un nœud du réseau. Le plus connu des WAN est Internet.

**7. LA TOPOLOGIE DU RESEAU**

La topologie représente la manière dont les équipements sont interconnectés dans le réseau. Nous avons deux sortes de topologie notamment la topologie physique et la topologie logique.

**A) LES TOPOLOGIES PHYSIQUE D’UN RESEAUX :**

Une topologie physique correspond à la disposition physique d’un réseau, mais ne spécifie pas les types de périphérique, les méthodes de connectivité ou les adresses d’un réseau.

Nous avons différents types de topologies physique que nous allons expliquer dans les lignes qui suivent.

* **LA TOPOLOGIE EN BUS OU LINEAIRE**

Dans cette topologie un même câble relie tous les nœuds d’un réseau sans périphérique de connectivité intermédiaire. Les deux extrémités des réseaux en bus sont équipées de résistances de 50 ohms (terminateurs) qui arrêtent les signaux une fois arrivés destination. Sans terminateurs, les signaux d’un réseau en bus continueraient à circuler sans fin ; ce qu’on appelle le rebond de signal.

Un réseau en bus est une architecture de communication où la connexion des matériels est assurée par un bus partagé par tous les utilisateurs.  
Les réseaux de bus permettent de relier simplement de multiples matériels, mais posent des problèmes quand deux machines veulent transmettre des données au même moment sur le bus. Les systèmes qui utilisent une topologie en bus ont normalement un arbitre qui gère l'accès au bus.

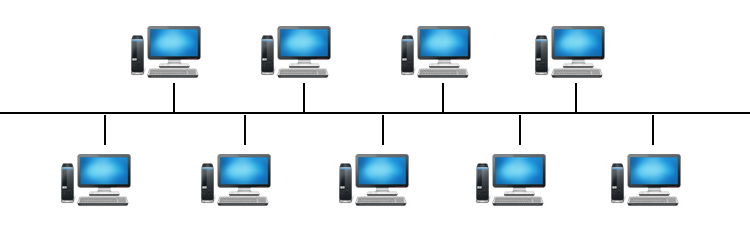


Figure 4 : Topologie bus.

* **LA TOPOLOGIE EN ETOILE**

Dans cette topologie, chaque nœud du réseau est relié à un périphérique central, tel qu’un commutateur (switch). Un même câble de réseau en étoile ne peut relier que deux périphériques, donc un problème de câblage ne touchera jamais plus de deux nœuds. Ceux-ci transmettent des données au commutateur, qui a son tour retransmet les informations au segment de réseau ou le nœud de destination.

Les équipements du réseau sont reliés à un système matériel central (le nœud). Celui-ci a pour rôle d'assurer la communication entre les différents équipements du réseau. Notamment utilisée par les réseaux Ethernet actuels en RJ45, elle concerne maintenant la majorité des réseaux. Lorsque toutes les stations sont connectées à un commutateur, on parle de topologie en étoile. Les nœuds du réseau sont tous reliés à un nœud central.

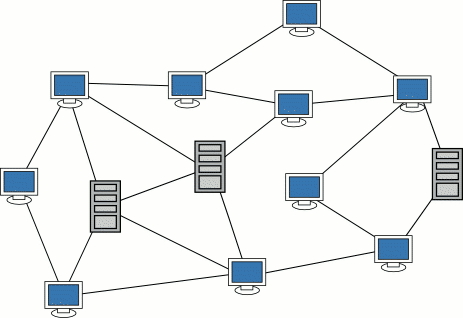
Figure 5. Topologie en étoile

* **LA TOPOLOGIE EN ANNEAU**

Toutes les machines sont reliées entre elles dans une boucle fermée. Les données circulent dans une direction unique, d'une entité à la suivante. Les ordinateurs communiquent chacun à leur tour. Cela ressemble à un bus mais qui serait refermé sur lui-même, le dernier nœud est relié au premier.

Figure 6 : Topologie Anneau.

* **TOPOLOGIE EN MAILLE**



Le réseau maillé est une topologie de réseau qualifiant les réseaux filaires ou non dont tous les hôtes sont connectés pair à pair sans hiérarchie centrale, formant ainsi une structure en forme de filet. Par conséquent, chaque nœud doit recevoir, envoyer et relayer les données. Cela évite d'avoir des points sensibles, qui en cas de panne, isolent une partie du réseau.

Si un hôte est hors service, ses voisins passeront par une autre route.  
Les réseaux maillés utilisent plusieurs chemins de transferts entre les différents nœuds. Cette méthode garantit le transfert des données en cas de panne d'un nœud. Le réseau Internet est basé sur une topologie maillée sur le réseau étendu (WAN), elle garantit la stabilité en cas de panne d'un nœud.

B) LA TOPOLOGIE LOGIQUE

La topologie logique détermine la disposition logique des équipements dans le réseau.

Nous avons trois sortes de topologies logiques dont :

* La topologie Ethernet (IEEE 802.3)

Dans cette topologie chaque nœud possède une adresse unique, les stations de travail n’ont pas un certain ordre pour utiliser le média. C’est une topologie à collision et crée la latence.

Le protocole CSMA/CD permet de faire la mise à l’écoute des équipements avant d’émettre ou de recevoir dans le réseau. Elle est actuellement la topologie la plus utilisé parce qu’elle coûte moins chère et est facile à déployer.

* La topologie FDDI (Fiber Distributed Data Interface)

Elle est une technologie d’accès au réseau sur des lignes fibre optique. Il s’agit d’une paire d’anneau, l’une dite primaire pour l’envoie des données et l’autres dite secondaire pour la détection des erreurs.

* La topologie Token Ring

Elle repose sur la methode d’accès au réseau basé sur les principes de la communications tour à tour, chaque ordinateur a la possibilité d’émettre dans le réseau à travers un jeton électronique et ceci se fait en boucle. Il n’y a pas de collision dans cette topologie.

**8. LE MODELE DE REFERENCE OSI :**

Au début des années 70, chaque constructeur a développé sa propre solution réseau autour d’architecture et de protocole privés et il s’est vite avéré qu’il serait impossible d’interconnecter ces différents réseaux si une norme internationale n’était pas établie.

Cette norme établie par l’internationale standard organisation (ISO) est la norme open system interconnexion (OSI, interconnexion de systèmes ouverts).

Un système ouvert est un ordinateur, un terminal, un réseau, n’importe quel équipement respectant cette norme et donc apte à échanger des informations avec d’autres équipement hétérogènes et issus de constructeurs différents.

Le premier objectif de la norme OSI a été de définir un modèle de toute architecture de réseau base sur découpage en sept couches chacun de ces couches correspondant à une fonctionnalité particulière d’un réseau.

Les couches 1, 2,3 et 4 sont dites basses et les couches 5,6 et 7 sont dites hautes.

Figure 7 : Modèle OSI.

**8.1.1 LA COUCHE PHYSIQUE :**

Cette couche définit les caractéristiques techniques, électriques, fonctionnelles et procédures nécessaires à l’activation et à la désactivation des connexions physiques destinées à la transmission de bits entres deux entités de la couche liaisons de données.

La couche physique s’occupe de la transmission des bits de façon brute sur un canal de communication. Cette couche doit garantir la parfaite transmission des données (un bit 1 envoyé doit bien être reçu comme bit valant 1). Concrètement, cette couche doit normaliser les caractéristiques électriques (un bit 1 doit être représenté par une tension de 5 V, par exemple), les caractéristiques mécaniques (forme des connecteurs, de la topologie…), les caractéristiques fonctionnelles des circuits de données et les procédures d’établissement, de maintien et de libération du circuit de données.

L’unité d’information typique de cette couche est le bit, représenté par une certaine différence de potentiel.

**8.1.2 LA COUCHE LIAISON DES DONNEES :**

Cette couche définit les moyens fonctionnels et procéduraux nécessaires à l’activation et à l’établissement ainsi qu’au maintien et à la libération des connexions de liaisons de données entre les entités du réseau.

Cette couche détecte et corrige, quand cela est possible, les erreurs de la coche physique et signale à la couche réseau les erreurs irrécupérables. L’unité d’information de la couche liaison de données est la trame qui est composées de quelques centaines à quelques milliers d’octets maximum.

**8.1.3 LA COUCHE RESEAU :**

Cette couche assure toutes les fonctionnalités de services entre les entités du réseau, c’est à dire : l’adressage, le routage, le contrôle de flux, la détection et la correction d’erreurs non résolues par la couche liaison pour préparer le travail de la couche transport.

C’est la couche qui permet de gérer le sous-réseau, i.e. le routage des paquets sur ce sous-réseau et l’interconnexion des différents sous-réseaux entre eux. Au moment de sa conception, il faut bien déterminer le mécanisme de routage et de calcul des tables de routage (tables statiques ou dynamiques…). L’unité d’information de la couche réseau est le paquet.

**8.1.4 LA COUCHE TRANSPORT :**

Cette douche définit un transfert de données entre les entités en les déchargeant des détails d’exécution (contrôle entre l’OSI et le support de transmission).

Son rôle est d’optimiser l’utilisation des services de réseau disponibles afin d’assurer à moindre coût les performances requises par la couche session.

Cette couche est responsable du bon acheminement des messages complets au destinataire. Le rôle principal de la couche transport est de prendre les messages de la couche session, de les découper s’il le faut en unités plus petites et de les passer à la couche réseau, tout en s’assurant que les morceaux arrivent correctement de l’autre côté. Cette couche effectue donc aussi le réassemblage du message à la réception des morceaux. Un des tous derniers rôles à évoquer est le contrôle de flux.

C’est l’une des couches les plus importantes, car c’est elle qui fournit le service de base à l’utilisateur, et c’est par ailleurs elle qui gère l’ensemble du processus de connexion, avec toutes les contraintes qui y sont liées. L’unité d’information de la couche transport est le message.

**8.1.5 LA COUCHE SESSION :**

Cette couche fournit aux entités de la couche présentation les moyens d’organiser et de synchroniser les dialogues et les échanges de données. Il s’agit de la gestion d’accès, de sécurité et d’identification des services.

Cette couche organise et synchronise les échanges entre tâches distantes. Elle réalise le lien entre les adresses logiques et les adresses physiques des tâches réparties. Elle établit également une liaison entre deux programmes d’application devant coopérer et commande leur dialogue (qui doit parler, qui parle…). Dans ce dernier cas, ce service d’organisation s’appelle la gestion du jeton. La couche session permet aussi d’insérer des points de reprise dans le flot de données de manière à pouvoir reprendre le dialogue après une panne.

**8.1.6 LA COUCHE PRESENTATION :**

Cette couche assure la transparence du format des données à la couche application.

Cette couche s’intéresse à la syntaxe et à la sémantique des données transmises : c’est elle qui traite l’information de manière à la rendre compatible entre tâches communicantes. Elle va assurer l’indépendance entre l’utilisateur et le transport de l’information.

Typiquement, cette couche peut convertir les données, les reformater, les crypter et les compresser.

**8.1.7 LA COUCHE APPLICATION :**

Cette couche assure aux processus d’application le moyen d’accès à l’environnement OSI et fournit tous les services directement utilisables par l’application (transfert e données, allocation de ressources, intégrité et cohérence des informations, synchronisation des applications).

Cette couche est le point de contact entre l’utilisateur et le réseau. C’est donc elle qui va apporter à l’utilisateur les services de base offerts par le réseau, comme par exemple le transfert de fichier, la messagerie…

TCP/IP désigne communément une architecture réseau, mais cet acronyme désigne en fait 2 protocoles étroitement liés, un protocole de transport TCP ([Transmission Control Protocol](http://www.frameip.com/entete-tcp/)) qu’on utilise par-dessus un protocole réseau IP ([Internet Protocol](http://www.frameip.com/entete-ip/)). Ce qu’on entend par « modèle TCPIP », c’est en fait une architecture réseau en 4 couches dans laquelle les protocoles TCP et IP jouent un rôle prédominant, car ils en constituent l’implémentation la plus courante. Par abus de langage, TCP/IP peut donc désigner deux choses : le modèle TCP/IP et la suite de deux protocoles TCP et IP.

Le modèle TCP/IP, comme nous le verrons plus bas, s’est progressivement imposé comme modèle de référence en lieu et place du [modèle OSI](http://www.frameip.com/osi/). Cela tient tout simplement à son histoire. En effet, contrairement au modèle OSI, le modèle TCP/IP est né d’une implémentation ; la normalisation est venue ensuite. Cet historique fait toute la particularité de ce modèle, ses avantages et ses inconvénients.

L’origine du modèle TCPIP remonte au réseau ARPANET. ARPANET est un réseau de télécommunication conçu par l’ARPA (Advanced Research Projects Agency), l’agence de recherche du ministère américain de la défense (le DoD : Department of Defense). Outre la possibilité de connecter des réseaux hétérogènes, ce réseau devait résister à une éventuelle guerre nucléaire, contrairement au réseau téléphonique habituellement utilisé pour les télécommunications mais considéré trop vulnérable. Il a alors été convenu qu’ARPANET utiliserait la technologie de commutation par paquet (mode datagramme), une technologie émergeante promettante. C’est donc dans cet objectif et ce choix technique que les protocoles TCP et IP furent inventés en 1974. L’ARPA signa alors plusieurs contrats avec les constructeurs (BBN principalement) et l’université de Berkeley qui développait un Unix pour imposer ce standard, ce qui fut fait.

Figure 9 : Model TCP/IP

**9.2.1 COUCHE APPLICATION :**

Contrairement au modèle OSI, c’est la couche immédiatement supérieure à la couche transport, tout simplement parce que les couches présentation et session sont apparues inutiles. On s’est en effet aperçu avec l’usage que les logiciels réseau n’utilisent que très rarement ces 2 couches, et finalement, le modèle OSI dépouillé de ces 2 couches ressemble fortement au modèle TCP/IP.

Cette couche contient tous les protocoles de haut niveau, comme par exemple Telnet, TFTP (trivial File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), HTTP (HyperText Transfer Protocol). Le point important pour cette couche est le choix du protocole de transport à utiliser. Par exemple, TFTP (surtout utilisé sur réseaux locaux) utilisera UDP, car on part du principe que les liaisons physiques sont suffisamment fiables et les temps de transmission suffisamment courts pour qu’il n’y ait pas d’inversion de paquets à l’arrivée. Ce choix rend TFTP plus rapide que le protocole FTP qui utilise TCP. A l’inverse, SMTP utilise TCP, car pour la remise du courrier électronique, on veut que tous les messages parviennent intégralement et sans erreurs. Les applications interagissent avec les protocoles de la couche Transport pour envoyer ou recevoir des données.

Figure 10 : Les protocoles de la couche application.

**9.2.2 LA COUCHE TRANSPORT :**

Son rôle est le même que celui de la couche transport du modèle OSI : permettre à des entités paires de soutenir une conversation. Officiellement, cette couche n’a que deux implémentations : le [protocole TCP](http://www.frameip.com/entete-tcp/) (Transmission Control Protocol) et le [protocole UDP](http://www.frameip.com/entete-udp/) (User Datagram Protocol). TCP est un protocole fiable, orienté connexion, qui permet l’acheminement sans erreur de paquets issus d’une machine d’un internet à une autre machine du même internet. Son rôle est de fragmenter le message à transmettre de manière à pouvoir le faire passer sur la couche internet. A l’inverse, sur la machine destination, TCP replace dans l’ordre les fragments transmis sur la couche internet pour reconstruire le message initial. TCP s’occupe également du contrôle de flux de la connexion.

UDP est en revanche un protocole plus simple que TCP : il est non fiable et sans connexion. Son utilisation présuppose que l’on n’a pas besoin ni du contrôle de flux, ni de la conservation de l’ordre de remise des paquets. Par exemple, on l’utilise lorsque la couche application se charge de la remise en ordre des messages. On se souvient que dans le modèle OSI, plusieurs couches ont à charge la vérification de l’ordre de remise des messages. C’est là un avantage du modèle TCP/IP sur le modèle OSI, mais nous y reviendrons plus tard. Une autre utilisation d’UDP : la transmission de la voix. En effet, l’inversion de 2 phonèmes ne gêne en rien la compréhension du message final. De manière plus générale, UDP intervient lorsque le temps de remise des paquets est prédominant.

Chargé de fournir un moyen de communication de bout en bout entre 2 programmes d'application. Agi en mode connecté et en mode non connecté.

Elle divise le flux de données venant des applications en paquets, transmis avec l'adresse destination IP au niveau IP.

Figure 11 : Les protocoles de la couche transport.

**9.2.3 LA COUCHE INTERNET :**

Cette couche est la clé de voûte de l’architecture. Cette couche réalise l’interconnexion des réseaux (hétérogènes) distants sans connexion. Son rôle est de permettre l’injection de paquets dans n’importe quel réseau et l’acheminement de ces paquets indépendamment les uns des autres jusqu’à destination. Comme aucune connexion n’est établie au préalable, les paquets peuvent arriver dans le désordre ; le contrôle de l’ordre de remise est éventuellement la tâche des couches supérieures.

Du fait du rôle imminent de cette couche dans l’acheminement des paquets, le point critique de cette couche est le [routage](http://www.frameip.com/routage/). C’est en ce sens que l’on peut se permettre de comparer cette couche avec la couche réseau du modèle OSI.

La couche internet possède une implémentation officielle : le [protocole IP](http://www.frameip.com/entete-ip/)(Internet Protocol).

Remarquons que le nom de la couche (« internet ») est écrit avec un i minuscule, pour la simple et bonne raison que le mot internet est pris ici au sens large (littéralement, « interconnexion de réseaux »), même si l’Internet (avec un grand I) utilise cette couche.

Figure 12 : Les protocoles de la couche internet.

**9.2.4 LA COUCHE HOTE RESEAU :**

Cette couche est assez étrange. En effet, elle semble regrouper es couches physique et liaison de données du modèle OSI. En fait, cette couche n’a pas vraiment été spécifiée ; la seule contrainte de cette couche, c’est de permettre un hôte d’envoyer des paquets IP sur le réseau. L’implémentation de cette couche est laissée libre. De manière plus concrète, cette implémentation est typique de la technologie utilisée sur le réseau local. Par exemple, beaucoup de réseaux locaux utilisent Ethernet ; Ethernet est une implémentation de la couche hôte-réseau.

Assure la transmission d'un datagramme venant de la couche IP en l'encapsulant dans une trame physique et en transmettant cette dernière sur un réseau physique.

Figure 13 : Les protocoles de la couche accès réseau.

**10. PERIPHERIQUES D’INTERCONNEXION :**

L’interconnexion des réseaux c’est la possibilité de faire dialoguer plusieurs sous réseaux initialement isolés, par l’intermédiaire de périphériques spécifiques (récepteur, concentrateur, pont, routeur, modem), ils servent aussi à interconnecter les ordinateurs d’une organisation, d’un campus, d’un établissement scolaire, d’une entreprise. Il est parfois indispensable de les relier.

Cette liaison peut être réalisée avec des équipements spécifiques aux types de réseau, et selon la distance et le besoin, dans cette partie de notre projet nous allons définir en brève ces équipements ou en vas accentuer la définition du routeur comme suit :

**10.1. LES MULTIPLEXEURS :**

Les formes de transmission qui permet à plusieurs signaux de voyager simultanément sur un même media s’appelle transmission multiplex ou multiplexage. Pour accommoder plusieurs signaux sur le même support est logiquement séparé en plusieurs canaux donc un multiplexeur sert à transiter sur une seule et même ligne de liaison, dite voie haute vitesse, des communications appartenant à plusieurs paires d'équipements émetteurs et récepteurs. Chaque émetteur (respectivement récepteur) est raccordé à un multiplexeur (respectivement démultiplexeur) par une liaison dite voie basse vitesse. Plusieurs techniques de multiplexage sont possibles :

Figure 14 : les multiplexeurs.

**10.2 LES CONCENTRATEURS (HUBS) :**

Servent à relier entre elles toutes les parties d'un même réseau physique, généralement tous les ordinateurs sont reliés à un Hub, sauf dans le cas d'un câblage coaxial où le Hub est inutile. Lorsqu'une information arrive sur un Hub, elle est rediffusée vers toutes les destinations possibles à partir de celui-ci, c'est à dire vers toutes ses prises.

Les concentrateurs connectent plusieurs équipements du réseau informatique. Un concentrateur sert également de répéteur, en ce sens qu’il amplifie les signaux, qui se détériorent après avoir parcouru de longues distances sur les câbles de connexion. Le concentrateur est le plus simple de la famille des équipements de connexion réseau, car il connecte des composants LAN ayant des protocoles identiques.

Figure 15 : Les hubs.

**10.3 LES COMMUTATEURS (SWITCHES) :**

Le commutateur (ou Switch) est un système assurant l'interconnexion de stations ou de segments d'un LAN en leur attribuant l'intégralité de la bande passante, à l'inverse du concentrateur qui la partage. Les commutateurs ont donc été introduits pour augmenter la bande passante globale d’un réseau d’entreprise et sont une évolution des concentrateurs Ethernet (ou HUB).

Les commutateurs jouent généralement un rôle plus intelligent que les concentrateurs. Un commutateur est un dispositif multiport qui améliore l’efficacité du réseau. Le commutateur gère des informations de routage limitées sur les nœuds du réseau interne et permet des connexions à des systèmes tels que les concentrateurs ou les routeurs. Les brins des réseaux locaux sont généralement connectés à l’aide de commutateurs. En général, les commutateurs peuvent lire les adresses matérielles des paquets entrants afin de les transmettre à la destination appropriée.

Figure 16 : Les switch.

**10.4 LES PONTS (BRIDGES) :**

Ils servent à relier entre eux deux réseaux différents d'un point de vue physique. De plus ils filtrent les informations et ne laissent passer que celles qui doivent effectivement aller d'un réseau vers l'autre. Ils peuvent être utilisés pour augmenter les distances de câblage en cas d'affaiblissement prématuré du signal.

Le rôle fondamental des ponts dans l’architecture réseau est de stocker et de transférer les trames entre les différents segments qu’ils relient. Ils utilisent les adresses MAC (contrôle d’accès au support) des équipements pour le transfert des trames. En examinant l’adresse MAC des appareils connectés à chaque segment, les ponts peuvent transmettre les données ou les empêcher de traverser. Les ponts peuvent également être utilisés pour connecter deux réseaux locaux physiques en un réseau local logique plus grand.

Figure 17 : Les ponts.

**10.5 LES REPETEURS (REPEATER) :**

Sont des dispositifs permettant d'étendre la distance de câblage d'un réseau local. Leur rôle consiste à amplifier et à répéter les signaux qui leurs parviennent. Il existe également des répéteurs qui en plus régénèrent les signaux. Ceci réduit le bruit et la distorsion. Le répéteur intervient au niveau 1 du modèle OSI.

Un répéteur est un appareil électronique qui amplifie le signal qu’il reçoit. Vous pouvez considérer un répéteur comme un appareil qui reçoit un signal et le retransmet à un niveau plus élevé ou à une puissance supérieure, afin qu’il puisse couvrir de plus longues distances, plus de 100 mètres pour les câbles LAN standard. Les répéteurs opèrent sur la couche Physique.

## 10.6 POINT D’ACCES

Même si un point d’accès peut techniquement comporter une connexion câblée ou sans fil, il s’agit généralement d’un dispositif sans fil. Un point d’accès fonctionne au niveau de la deuxième couche OSI, la couche Liaison de données, et il peut fonctionner soit comme un pont reliant un réseau câblé standard à des appareils sans fil ou comme un routeur transmettant des données d’un point d’accès à un autre.

Les points d’accès sans fil (WAP) se composent d’un émetteur et d’un récepteur, qui permettent de créer un réseau local sans fil (WLAN). Les points d’accès sont généralement des équipements réseau distincts dotés d’une antenne, d’un émetteur et d’un adaptateur intégrés. Les points d’accès utilisent le mode réseau d’infrastructure sans fil pour fournir un point de connexion entre les réseaux locaux sans fil (WLAN) et un réseau local Ethernet câblé. Ils disposent également de plusieurs ports, ce qui vous permet

**10.7 LES PASSERELLES (GATEWAY) :**

Sont des dispositifs permettant d'interconnecter des architectures de réseaux différentes. Elles offrent donc la conversion de tous les protocoles, au travers des 7 couches du modèle OSI. L'objectif étant de disposer d'une architecture de réseau évolutive, la tendance actuelle est d'interconnecter les réseaux par des routeurs, d'autant plus que le prix de ceux-ci est en baisse.

Ainsi, les passerelles connectent deux ou plusieurs réseaux autonomes, chacun ayant ses propres algorithmes de routage, protocoles, topologie, service de noms de domaine, procédures et politiques d’administration réseau.

## 10.8 MODEM

Les modems (modulateurs-démodulateurs) servent à transmettre des signaux numériques via des lignes téléphoniques analogiques. Les signaux numériques sont donc convertis par le modem en signaux analogiques de différentes fréquences et transmis à un autre modem au lieu de réception. Le modem récepteur effectue la transformation inverse et fournit une sortie numérique au dispositif qui y est connecté, généralement un ordinateur. Les données numériques sont habituellement transférées vers/depuis le modem via une liaison série et une interface standard RS-232. De nombreuses compagnies téléphoniques offrent des services DSL et de nombreux câblo-opérateurs utilisent des modems comme terminaux finaux pour l’identification et la reconnaissance des utilisateurs individuels. Les modems opèrent à la fois sur les couches Physique et Liaison de données.

**10.9 LES ROUTEURS (ROUTERS) :**

Les routeurs sont des appareils universels qui interconnectent deux ou plusieurs réseaux hétérogènes. Ils sont généralement dédiés à des ordinateurs spécialisés et dotés d’interfaces réseau entrée et sortie séparées pour chaque réseau connecté. Les routeurs et les passerelles constituant la colonne vertébrale des grands réseaux informatiques comme Internet, ils possèdent des caractéristiques spéciales qui leur donnent la souplesse et la capacité de s’adapter aux différents systèmes d’adressage réseau et tailles de trame en segmentant les gros paquets en plus petits, adaptés aux nouveaux composants réseau. Chaque interface de routeur possède son propre protocole de résolution d’adresses (ARP), sa propre adresse LAN (adresse de carte réseau) et sa propre adresse IP (protocole Internet). Le routeur, grâce à une table de routage, connaît les itinéraires qu’un paquet peut prendre de sa source à sa destination. La table de routage, comme pour le pont et le commutateur, se développe de manière dynamique. Dès réception d’un paquet, le routeur supprime son en-tête et son *trailer*, puis analyse l’en-tête IP en déterminant les adresses source et destination et le type de données, et en notant l’heure de réception. Il met également à jour la table de routage avec de nouvelles adresses qui n’y figurent pas déjà. L’en-tête IP et les informations d’heure d’arrivée sont entrées dans la table de routage. Les routeurs opèrent normalement au niveau de la couche Réseau du modèle OSI.

Les routeurs contribuent à transmettre des paquets vers leurs destinations en traçant un chemin dans l’océan des équipements réseau interconnectés, à l’aide de différentes topologies de réseau. Les routeurs sont des appareils intelligents qui stockent des informations sur les réseaux auxquels ils sont connectés. La plupart des routeurs peuvent être configurés de manière à fonctionner comme pare-feu à filtrage de paquets et utilisent des listes de contrôle des accès (ACL). Les routeurs, conjointement avec une unité de service de canal/unité de service de données (CSU/DSU), servent également à traduire le tramage LAN en tramage WAN. Ceci est nécessaire car les réseaux locaux (LAN) et les réseaux étendus (WAN) utilisent des protocoles différents. De tels routeurs sont appelés routeurs frontières. Ils assurent la connexion externe d’un réseau local à un réseau étendu, et ils fonctionnent à la frontière de votre réseau.

Les routeurs servent également à scinder les réseaux internes en deux ou plusieurs sous-réseaux. Il est également possible de connecter des routeurs en interne à d’autres routeurs, pour créer des zones qui opèrent indépendamment les unes des autres. Les routeurs établissent la communication en gérant des tables sur les destinations et les connexions locales. Un routeur contient des informations sur les systèmes qui y sont connectés et sur la destination des requêtes à envoyer si celle-ci n’est pas connue. Les routeurs communiquent généralement les informations de routage et autres en utilisant l’un des trois protocoles standard : le protocole d’informations de routage (RIP), le protocole de passerelle frontière (BGP) ou le chemin le plus court ouvert en premier (OSPF).

11. ADRESSAGE

L’adressage est l’opération d’identification des équipements dans le réseau. Il existe deux manières d’identifier un équipement dans le réseau, nous citons : l’adressage physique (Adresse Mac) et l’adresse Logique (Adresse IP)

**L’adresse physique ou adresse MAC**

Chaque appareil qui possède une possibilité de raccordement à un réseau informatique possède une adresse unique déterminé lors de sa fabrication.

Cet identifiant unique s'appelle l'adresse MAC (Media Access Control) et se présente sous la forme d'une suite de 6 octets (donc 48 bits) en général noté en hexadécimal.

L’adresse MAC de notre matériel est donc : **34-48-ED-01-14-D0**

**Structure d’une adresse MAC :**

|  |  |
| --- | --- |
| * Les 3 premiers octets sont l’**OUI** (Organizationally Unique Identifier) : il s’agit d’un nombre de 24 bits assigné par l'IEEE (Institute of Electrical and Electronics Engineers). Ce numéro identifie le fabricant. * Les 3 octets de poids faible correspondent à un identifiant fixé par le fabricant afin que chaque appareil soitunique. |  |

**L’adresse IP**

L’adresse IP (Internet Protocol) est une adresse « logique » affectée à une machine manuellement par l’administrateur réseau ou automatiquement par un serveur DHCP (Dynamic Host Configuration Protocol). Cette adresse est modifiable. Ce sera cette adresse IP qui servira pour tous les échanges au sein du réseau.

***Le format IPV4***

Une adresse IPV4 est constituée de quatre champs dont chacun représente un octet et séparé par un point. Ce qui revient à dire que ceci est codé sur de 32 bits. Pour faciliter la lecture et la manipulation de cette adresse on la représente plutôt en notation décimale. La valeur maximale d’un champ est 255.

Par xemple : 192.168.2.6

Un adresse IPV4 est composée d’un identifiant réseau (**NetID**) et d’un identifiant équipement ou hôte (**HostID**).

Une adresse IP est dite :

* Adresse hôte ou adresse utilisable si le HostId est différent de 0 et de 255.
* Adresse réseau si le HostId est égal à 0.
* Adresse de diffusion ou broadcast : si le HostId est égal à 255.

Il existe au final cinq classes d'adresses IP, chaque classe est identifiée par une lettre allant de A à E.

Ces différentes classes ont chacune leurs spécificités quant à la répartition du nombre d'octets servant à identifier le réseau ou les ordinateurs connectés à ce réseau

* Une adresse IP de classe A dispose d'une partie NetID comportant uniquement un seul octet.
* Une adresse IP de classe B dispose d'une partie NetID comportant deux octets.
* Une adresse IP de classe C dispose d'une partie NetID comportant trois octets.
* Les adresses IP de classes D et E correspondent à des adresses IP particulières.

 Cela donne :

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Classe** | **Bits de départ** | **Début** | **Fin** | **Notation CIDR** | **Masque de sous-réseau par défaut** |
| **Classe A** | 0 | 0.0.0.0 | 126.255.255.255 (127 est réservé) | /8 | 255.0.0.0 |
| **Classe B** | 10 | 128.0.0.0 | 191.255.255.255 | /16 | 255.255.0.0 |
| **Classe C** | 110 | 192.0.0.0 | 223.255.255.255 | /24 | 255.255.255.0 |
| **Classe D** (multicast) | 1110 | 224.0.0.0 | 239.255.255.255 |  | 255.255.255.255 |
| **Classe E** (réservée) | 1111 | **240**.0.0.0 | 255.255.255.255 |  | Non défini |

**Masques de sous réseau**  
Un sous-réseau est une subdivision logique d'un réseau de taille plus importante. Le masque de sous-réseau permet de distinguer la partie de l'adresse réseau ou NetId avec l’adresse de l’hôte ou .

***Exemple*** : adresse 192.168.1.13 et masque 255.255.255.0

Le masque de sous réseau va nous permettre, à l’aide de la fonction logique **ET**, de récupérer l’adresse de notre matériel débarrassé de la partie commune :

Une forme plus courte est connue sous le nom de « notation CIDR » (Classless Inter-Domain Routing). Elle donne le numéro du réseau suivi par un slash et le nombre de bits à 1 dans la notation binaire du masque de sous-réseau. Le masque 255.255.255.0, équivalent en binaire à 11111111.11111111.11111111.00000000, sera donc représenté par /24 (24 bits à la valeur 1, suivis de 8 bits 0).

La notation 192.168.1.13/24 désigne donc l'adresse IP 192.168.1.13 avec le masque 255.255.255.0, et signifie que les 24 premiers bits de l'adresse sont dédiés à l'adresse du sous-réseau (192.168.1) et le reste à l'adresse de l'ordinateur hôte à l'intérieur du sous-réseau (ici 13).

**Le format IPV6**

Le nombre d'adresses IP disponibles avec le protocole IPv4, environ 4 milliards, n'est plus suffisant pour répondre à la demande croissante notamment avec l’arrivée des objets connectés. C'est pourquoi un nouveau protocole internet a été créé : IPv6

L'adressage se fait sur 16 octets (16\*8=128 bits), ce qui représente 2128 adresses possibles (contre 232 pour l'IPv4).

La notation décimale employée pour les adresses IPv4 est abandonnée au profit d'une écriture hexadécimale, où les 8 groupes de 2 octets (soit 16 bits par groupe) sont séparés par un signe deux-points.

***Exemple et règles d’écriture :***

   2001:0db8:0000:85a3:0000:0000:ac1f:8001

La notation complète ci-dessus comprend exactement 39 caractères (**32 chiffres hexa et 7 deux-points**).

***Simplification d’écriture :***

Il est permis d'omettre de 1 à 3 chiffres zéros non significatifs dans chaque groupe de 4 chiffres hexadécimaux. Ainsi, l'adresse IPv6 ci-dessus est équivalente à :  
2001 :db8:0:85a3:0:0:ac1f:8001

De plus, une unique suite d’un ou plusieurs groupes consécutifs de 16 bits tous nuls peut être omise, en conservant toutefois les signes deux-points de chaque côté de la suite de chiffres omise, c'est-à-dire une paire de deux points « : ». Ainsi, l'adresse IPv6 ci-dessus peut être abrégée en :  
2001 :db8:0:85a3::ac1f:8001

I.7. SUPPORT DE TRANSMISSION Les supports de transmission sont des lignes de liaisons ou moyen auquel on fait recours pour l’interconnexion des équipements, parmi les supports de transmission, nous avons ceux qui sont logiques (immatériels) et d’autres physiques (matériels) mais nous mettrons en premier lieu un accent sur le support physique et en second lieu le support logique. I.7.1. CARACTERISTIQUES Quelle que soit la nature du support, le signal désigne le courant, la lumière ou l’onde électromagnétique transmis. Certaines caractéristiques des supports (bande passante, sensibilité, aux bruits, limites des débits possibles) en perturbant la transmission. Leur connaissance est nécessaire pour fabriquer de « bons » signaux, c’est-à-dire les mieux adaptés aux supports utilisés. ➢ DEBIT Le débit est l’une des caractéristiques de support de transmission qui détermine la quantité des données qui peuvent être transmise pendant un temps dans un support de transmission. ➢ BANDE PASSANTE 18 Les supports de transmission ont une bande passante limitée. Certains signaux s’y propagent correctement (ils sont affaiblis mais reconnaissables à l’autre extrémité), alors que d’autre ne les traversent pas (ils sont tellement affaiblis ou déformés qu’on ne les reconnaît plus à la sortie). Intuitivement, plus un support a une bande passante large, plus il transporte d’informations par unité de temps. ➢ PORTEE La portée est un élément important dans un support de transmission, qui sépare deux entités qui s’échangent les données. I.8. FAMILLES DE SUPPORTS DE TRANSMISSION I.8.1. LES SUPPORTS MATERIELS I.8.1.1. Le câble coaxial C’est un câble qui est entouré par un isolant, il est constitué de deux conducteurs de même axe, et il n’est plus utilisé dans le réseau local, les plus utilisés de ces câbles sont : câble 50ohm, de type Ethernet et câble 75 ohm de CATV (câble de télévision) Fig.I.15. Câble coaxial I.8.1.2. Le câble à paire torsadée Une paire torsadée est une ligne symétrique formée de deux fils conducteurs enroulés en hélice l’un autour de l’autre. Cette configuration a pour but principal de limiter la sensibilité aux interférences et la diaphonie dans les câbles multi paires. ❖ Blindé Le câble à paire torsadée blindée (STP) est doté d'un revêtement en maille tressée supplémentaire ou d'une feuille de métal qui enveloppe chaque jeu de conducteurs isolés. Le boîtier métallique intercepte la pénétration de bruit électromagnétique. Cela peut également éliminer un phénomène appelé diaphonie, qui est l'effet indésirable d'un circuit (ou canal) sur un autre circuit (ou canal). 19 Fig. 16. Câble à paire torsadée blindé. ❖ Non blindé Le câble à paire torsadée non blindée (UTP) est le type de support de télécommunication le plus répandu actuellement. Sa gamme de fréquences convient à la transmission de données et à la voix. Par conséquent, ils sont le plus souvent utilisés dans les systèmes téléphoniques. Une paire torsadée est constituée de deux conducteurs isolés (généralement en cuivre) dans une configuration torsadée. Les bandes de couleur sont utilisées dans les isolants plastiques pour l'identification. En outre, les couleurs identifient également les conducteurs spécifiques d'un câble et indiquent les fils qui appartiennent par paires et leur relation avec les autres paires d'un faisceau plus grand7. Fig.I.17. Câble à paire torsadée non blindé. I.8.1.3. Le guide d’onde Un guide d’onde est un système physique qui sert à guider les ondes électromagnétiques ou les ondes acoustiques, pour les maintenir dans un milieu particulier, sur certaine distance 7 https://fr.gadget-info.com/difference-between-utp, consulté le 13/03/2022 à 14h47 20 Fig. I.18. Le guide d’onde. I.8.2. LES SUPPORTS IMMATERIELS La transmission sans fil s’impose donc comme la réponse à cette nécessité vitale. Le sans-fil peut même présenter certains avantages pour le raccordement des équipements fixes. Les technologies sans fils utilisent comme support des ondes électromagnétiques. L’émission et la réception de ces ondes se font par des antennes intégrées dans toute carte sans fil. I.8.2.1 Faisceau hertzien Un faisceau hertzien est un système de transmission de signaux aujourd'hui principalement numériques monodirectionnel ou bidirectionnel et généralement permanent, entre deux sites géographiques fixes. Il exploite le support d'ondes radioélectriques, par des fréquences porteuses allant de 1 à 86 GHz (gamme des micro-ondes), focalisées et concentrées grâce à des antennes directives. Ces émissions sont notamment sensibles aux obstacles et masquages (relief, végétation, bâtiments, etc.), aux précipitations, aux conditions de réfractivité de l'atmosphère, aux perturbations électromagnétiques et présentent une sensibilité assez forte aux phénomènes de réflexion (pour les signaux analogiques mais la modulation numérique peut, au moins en partie, compenser le taux d'erreur de transmission dû à ces nuisances). À cause des limites de distance géographique et des contraintes de « visibilité », le trajet hertzien entre deux équipements d'extrémité est souvent découpé en plusieurs tronçons, communément appelés « bonds », à l'aide de stations relais (exemple : la tour hertzienne du Vigen). Dans des conditions optimales (profil dégagé, conditions géo climatiques favorables, faible débit, etc.), un bond hertzien peut dépasser 100 km.

**10. CONCLUSION :**

Dans ce chapitre, nous avons vu que les réseaux et Internet ont modifié nos façons de communiquer, d’apprendre, ou encore de travailler et de nous divertir.

Les réseaux peuvent être de différentes tailles :

* Cela va des réseaux de base (deux ordinateurs), aux réseaux les plus complexes (des millions de périphériques).
* Internet est le plus grand réseau existant. En réalité, le terme « Internet » signifie « réseau de réseaux ».
* Internet fournit des services qui nous permettent de communiquer avec la famille, les amis et les collègues.

L’infrastructure réseau est la plate-forme qui prend en charge le réseau. Elle fournit le canal stable et fiable à travers lequel nos communications peuvent s’établir. Ce dernier est constitué de composants réseau tels que les périphériques finaux, les équipements intermédiaires et les supports de transmission.

Dans ce chapitre, nous avons traité des connaissances générales sur les réseaux qu’il faut acquérir, afin de pouvoir installer une sécurité, qu’on va développer dans les chapitres suivants.

Enfin, de ce chapitre On doit être en mesure de :

 • Différencier les différents types de réseaux et leurs topologies.

 • Les deux model de logique de télécommunication ISO et TCP/IP.

 • Connaitre les différents périphériques d’interconnexion.

 • Maitre l’accent sur le routeur, ses fonctions et ses composants.