

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Mohammed Seddik Benyahia - Jijel



Faculté des Sciences Exactes et Informatique

Département d'Informatique

Polycopié de cours

Réseaux de communication

Spécialité : 2^{ème} année Licence Informatique

Préparé par

Dr. Manel KHELIFI



Année scolaire **2020-2021**

Avant propos

Ce cours est destiné aux étudiants de la deuxième année de licence (L2) en informatique. A travers ce support de cours, les étudiants pourront acquérir les notions de base en réseaux informatiques et ainsi, approfondir leurs connaissances sur les architectures des systèmes de communication et leurs caractéristiques. Afin de concrétiser et de rendre pratique les différentes notions abordées, une série d'exercices est proposée en annexe.

Ce support de cours est organisé en six chapitres comme suit :

Le premier chapitre initie les étudiants aux réseaux de communication en présentant des généralités sur ces réseaux avec une description de leurs architectures, technologies, caractéristiques ainsi que les différentes classifications qui en découlent.

Dans le deuxième chapitre, nous abordons le paradigme de la normalisation dans les réseaux, en exposant les modèles et les normes de référence existants, à savoir le modèle de référence OSI et TCP. Le troisième chapitre est consacré à l'étude détaillée des supports de communication et des équipements de réseau. Le quatrième chapitre porte sur l'étude des techniques utilisées pour transférer les informations, en l'occurrence, les méthodes permettant le codage et la modulation du signal. Dans le cinquième chapitre, une étude approfondie de la couche liaison de données est réalisée où nous exposons les principaux mécanismes servant à contrôler et à corriger les informations en cas d'erreur. Le sixième chapitre présente l'architecture TCP/IP, en particulier la description détaillée des protocoles IP, TCP et UDP. Enfin, ce support se termine par une série d'exercices.

Il convient de noter que ce support de cours est le fruit de cinq années consécutives d'enseignement depuis 2017. Le contenu de ce document est en constante évolution, et donc toutes remarques et/ou commentaires visant à améliorer la qualité de ce document sont les bienvenus.

Table des matières

Tables des matières

Liste des Figures

Chapitre 1 Introduction aux réseaux

1.1 Introduction.....	3
1.2 Chronologie de développement des réseaux et des télécommunications	3
1.3 Concepts préliminaires	5
1.4 Motivation.....	5
1.5 Classification d'un réseau.....	6
1.5.1 Selon la distance (la portée).....	6
1.5.2 Selon la Topologie d'un réseau.....	8
1.5.3 Selon le mode de commutation.....	10
1.6 Conclusion	11

Chapitre 2 La normalisation et architecture en couches

2.1 Introduction	12
2.2 Pourquoi la normalisation ?.....	12
2.3 Les modèles d'architectures réseaux.....	13
2.3.1 Le Modèle de référence OSI.....	13
2.3.2 Le modèle TCP/IP	16
2.4 Modèle en couches	17
2.4.1 Les unités de données et communication entre les couches	18
2.4.2 Les Services	20
2.4.3 L'encapsulation des données	21
2.5 Conclusion	22

Chapitre 3 Les équipements d'interconnexion et de réseautage

3.1 Introduction	23
3.2 Média de transmission ou Câblage	23
3.2.1 Le câble coaxial	23
3.2.2 La paire torsadée	24
3.2.3 La Fibre Optique.....	25

3.3 Les équipements d'interconnexion	25
3.3.1 Les Répéteurs.....	26
3.3.2 Concentrateurs / Hubs	26
3.3.3 Les Ponts.....	27
3.3.4 Les Commutateurs / Switch	27
3.3.5 Les Routeurs	28
3.3.6 Coupe-feux (pare-feu)	28
3.3.7 Passerelle (Gateway)	29
3.4 Exemples de réseaux existants : Ethernet et Token Ring	29
3.5 Conclusion	30

Chapitre 4 Transmission physique de l'information

4.1 Introduction.....	31
4.2 Principe de la transmission.....	31
4.3 Transformations sur les signaux.....	32
4.3.1 Type de liaison.....	33
4.3.2 Type de communication de la liaison	34
4.3.3 Mode de liaison	35
4.3.4 Les modes de synchronisation des signaux	36
4.3.5 Les méthodes de transmission.....	37
4.4 Le Codage des signaux	37
4.5 La Modulation des signaux	38
4.6 Le Multiplexage	40
4.7 Les phénomènes caractérisant les supports de transmission.....	41
4.8 Les Grandeurs de transmission	41
4.9 Conclusion	43

Chapitre 5 Fiabilisation de la transmission

5.1 Introduction.....	44
5.2 Mécanismes de détection et de correction d'erreurs	44
5.2.1 Détection d'erreurs par parité.....	45
5.2.2 La détection d'erreurs par CRC	46
5.2.3 Codes auto-correcteurs: Le code de Hamming.....	48

5.2.4 Les mécanismes de correction par retransmission	50
5.3 Le protocole de liaison de données HDLC (HDLC: High Data Level Control).....	51
5.4 Conclusion	52

Chapitre 6 L'architecture TCP/IP

6.1 Introduction	53
6.2 Le modèle TCP/IP	53
6.3 Le Protocole IP	55
6.3.1 Principe	55
6.3.2 Format du datagramme IP	55
6.3.3 La fragmentation des datagrammes IP	56
6.3.4 L'adressage IP	58
6.3.5 Le Routage	61
6.4 Le Protocole TCP.....	63
6.4.1 Principe	64
6.4.2 Le format d'un segment TCP	65
6.4.3 Fiabilité des transferts	65
6.5 Le protocole UDP	66
6.5.1 Format de l'en-tête UDP.....	66
6.6 Les protocoles de la couche Application	67
6.8 Conclusion	68

Bibliographie

Annexe Série d'Exercices (TD et Sujets d'examen)

Liste des figures

Figure 1.1 Catégories de réseaux selon la distance	6
Figure 1.2 Type de réseaux	7
Figure 1.3 Exemples des LANs	7
Figure 1.4 Topologie en Bus	9
Figure 1.5 Topologie en Etoile	9
Figure 1.6 Topologie en Anneau	10
Figure 1.7 Différentes topologies (arbre, maillage complet/incomplet)	10
Figure 2.1 Le Modèle OSI	14
Figure 2.2 Le Modèle TCP/IP	16
Figure 2.3 Communication entre couches	18
Figure 2.4 La communication horizontale dans un modèle OSI	19
Figure 2.5 La communication verticales dans un modèle OSI	20
Figure 2.6 Service (Primitives de service)	21
Figure 2.7 L'encapsulation des données	22
Figure 3.1. Interconnexion de réseaux	23
Figure 3.2 Les équipements réseau	26
Figure 3.3 Schéma d'utilisation d'un répéteur	26
Figure 3.4 Schéma d'utilisation d'un Hub	27
Figure 3.5 Schéma d'utilisation d'un Pont	27
Figure 3.6 Schéma d'utilisation d'un switch	28
Figure 3.7 Schéma d'utilisation d'un routeur	28
Figure 3.8 Ethernet et Token Ring	29
Figure 4.1 Signal numérique	32
Figure 4.2 Signal analogique	32
Figure 4.3 Schéma d'un système de transmission	32
Figure 4.4 Circuit de données	33
Figure 4.5 Liaison série	34
Figure 4.6 Liaison parallèle	34
Figure 4.7 Mode simplex	34

Figure 4.8 Mode duplex	35
Figure 4.9 Mode full duplex	35
Figure 4.10 La modulation (Transmission large bande)	37
Figure 4.11 Exemples de codage	38
Figure 4.12 Modulation de fréquence	39
Figure 4.13 La modulation d'amplitude	39
Figure 4.14 La modulation de phase	39
Figure 4.15 Le multiplexage fréquentiel	40
Figure 4.16 Le multiplexage temporel	40
Figure 5.1 Send & Wait	50
Figure 5.2 Rejet systématique	51
Figure 5.3 Rejet Sélectif	51
Figure 6.1 La pile protocolaire TCP/IP	53
Figure 6.2 Les protocoles TCP/IP	54
Figure 6.3 L'entête IP	56
Figure 6.4 Exemple de MTU	57
Figure 6.5 Exemple de routage	61
Figure 6.6 La table de routage	62
Figure 6.8 L'entête TCP	51

Chapitre 1

Introduction aux réseaux

1.1 Introduction

Un **réseau informatique** constitue une composante essentielle pour assurer la communication entre deux ou plusieurs dispositifs électroniques. De manière générale, un réseau informatique permet la transmission et l'échange de données à distance. A l'origine, ces communications étaient destinées exclusivement au transfert de données informatiques, tandis qu'aujourd'hui on tend vers des réseaux intégrant aussi bien les données que la parole et la vidéo.

Ce chapitre est destiné à familiariser les étudiants avec le vocabulaire des réseaux informatiques tout en les initiant à leurs différentes caractéristiques. Ainsi, nous précisons les concepts de base de ces réseaux en évoquant leurs avantages, et leurs différentes architectures et structurations. Une classification synoptique détaillant les différents types de réseaux, leurs topologies ainsi que leurs modes de communications est aussi donnée.

1.2 Chronologie de développement des réseaux et des télécommunications

Depuis 1940, le développement des réseaux et des télécommunications est en constante évolution. Les dates suivantes méritent en effet d'être évoquées:

- **1940**

En 1940, fut la première communication à distance réalisée par George Stibitz de Bell Labs. Ils réussissent à communiquer par téléscripteur à partir du Dartmouth College, New Hampshire, et faire fonctionner à distance une machine à calculer à relais située à New York.

- **1957**

La mise en orbite du satellite Spoutnik par l'URSS a conduit les Américains à créer une agence au sein du département de la défense appelée ARPA (Advanced Research Projects Agency) ayant pour but d'établir une suprématie américaine dans le domaine de la science et de la technologie à des fins militaires.

- **1960**

C'est dans le cadre du système de surveillance aérienne SAGE (Semi-Automatic Ground Environment) en 1960, que l'on installe le premier réseau informatique réel. Ainsi, plusieurs radars positionnés aux confins des frontières géographiques stratégiques se partagent la tâche de créer une carte complète du ciel en temps réel. Celle-ci étant centralisée par quarante énormes ordinateurs reliés par des lignes téléphoniques (Breton et Proulx, 1989).

- **1962**
La compagnie American Airlines est devenue en 1962 la première compagnie aérienne commerciale au monde à mettre en place un système de réservation informatisé. Il s'agissait du premier grand réseau informatique commercial, SABRE, installé par IBM.
- **1969**
ARPAnet (Advanced Research Projects Agency network) représente le premier réseau informatique destiné à la recherche. Initialement, ce réseau a été conçu par le ministère de la Défense des États-Unis pour examiner le mode de fonctionnement des réseaux informatiques d'une part, et pour permettre aux chercheurs d'échanger des informations d'autre part. Les échanges se font par deux ordinateurs, chacun ayant une adresse, qui partagent des informations en utilisant un protocole appelé Internet Protocol (IP) et qui peuvent ainsi communiquer entre eux. Par ailleurs, ARPAnet prévoit la redirection de ces échanges vers d'autres ordinateurs du réseau en cas de rupture de communication. Le réseau peut ainsi demeurer opérationnel malgré la défaillance de l'un des nœuds.
- **1973**
Lancement officiel du projet de raccordement international à ARPANET. Or, le Collège universitaire de Londres (Angleterre) et le Royal Radar Establishment (Norvège) se connectent à ARPANET.
- **1978**
La mise en œuvre du vidéotex (ou vidéographie) est une technologie de transmission d'informations textuelles ou graphiques contenues sur ordinateur, vers des écrans de télévision, sous forme interactive (vidéotex) ou non (télétexte). Ce sont les Anglais et les Français qui furent à l'origine de la mise en route de cette technologie dans leurs projets Prestel et Minitel.
- **1980**
Le début de la décennie 1980 est marqué par la prolifération de toute une génération de machines individuelles dans les universités américaines, remplaçant les gros ordinateurs. Ces machines sont pilotées par UNIX et peuvent communiquer en réseau. Dès lors, il y a une multitude de petites machines individuelles connectées au réseau ARPAnet.
- **1990**
Début 1990, la grande toile (World Wide Web, WWW) est née. Elle a été lancée par le Centre d'études et de recherches nucléaires, le CERN, basé à Genève en Suisse, afin de permettre aux chercheurs de communiquer plus rapidement des informations textuelles, y compris les images fixes ou animées et les sonorités. Le succès de ce nouveau mode de transmission des informations s'est rapidement imposé dans le monde entier par le biais de logiciels de navigation hypertextuelle facilitant l'accès tels que Mosaic. Ce dernier a été mis au point au National Center for Supercomputing Applications (NCSA) de l'université de l'Illinois par un groupe d'étudiants.
- **1991**
Le Congrès américain vote en 1991 un budget de 400 millions de dollars pour relier les chercheurs ensemble et permettre aux écoles américaines d'être connectées à Internet. Il est également décidé d'ouvrir l'Internet à la commercialisation. Cette idée est lancée en vue de créer une véritable autoroute informatique. Ainsi Internet connaîtra un essor fulgurant non seulement aux États-Unis mais aussi dans le monde entier.
- **1994**
L'année 1994 est sans doute l'année d'Internet au sens large. Elle a connu une fulgurante expansion avec l'arrivée massive des entreprises sur le World Wide Web (WWW) et ce, à l'aide d'interfaces graphiques comme Internet Explorer, Mosaic ou Netscape.

1.3 Concepts préliminaires

- **Réseau informatique:** Un réseau est en général le résultat de la connexion de plusieurs ordinateurs (ou de périphériques) autonomes, distants et situés dans un certain domaine géographique. Cela permet aux utilisateurs et aux applications qui fonctionnent sur ces derniers d'échanger différents types d'informations.
- **Téléinformatique:** est la composition de **télécommunication** et **informatique**. C'est une science qui combine la communication à distance et l'informatique en associant les difficultés liées au traitement des données à celles du transport de l'information.
- **Station de travail** : une station de travail est tout dispositif capable d'envoyer des données vers les réseaux.
- **Nœud** : C'est une station de travail, une imprimante, un serveur ou toute entité pouvant être adressée par un numéro unique.
- **Serveur** : Dépositaire centrale d'une fonction spécifique : service de base de données, de calcul, de fichier, mail, ...
- **Topologie** : Décrit l'organisation physique et logique d'un réseau. L'organisation physique concerne la façon dont les machines sont connectés (Bus, Anneau, Étoile.). La topologie logique montre comment les informations circulent sur les réseaux (diffusion ou point à point).
- **Un protocole** est un ensemble de règles destinées à une tâche de communication particulière. Deux ordinateurs doivent utiliser le même protocole pour pouvoir communiquer entre eux. En d'autres termes, ils doivent parler le même langage pour se comprendre. Cependant, dans une architecture en couches cela signifie qu'ils fournissent le service que la couche est censée fournir

1.4 Motivations

Les réseaux informatiques ont surgi suite au besoin de connecter des équipements distants à une unité centrale. L'évolution des besoins ne se limite plus à relier les dispositifs des grands instituts et sociétés mais vise à connecter tous les objets usuels aux réseaux informatiques (notamment Internet ; internet des objets). Un réseau informatique présente de nombreux avantages tels que:

- **Réduire les coûts** : par exemple le partage d'une seule imprimante pour plusieurs ordinateurs.
- **Partage des ressources:** le partage des applications et des fichiers
- **Augmenter la fiabilité:** dupliquer les données et les traitements sur plusieurs machines. Dans ce cas, si une machine tombe en panne une autre prendra la relève.

- **Fournir un puissant média de communication**: la communication entre personnes et donc l'interaction avec les utilisateurs connectés, messagerie électronique, conférences électroniques, etc. Ce qui permet une communication et organisation plus efficace.

- **L'accès facile et rapide à l'information** : le transfert de la parole, de la vidéo et des données (réseaux à intégration des services multimédia) et donc l'accès aux données à temps utile.

1.5 Classification d'un réseau

Plusieurs critères peuvent être distingués pour classer les réseaux :

- ✓ Taille ou la distance: PAN, LAN, MAN, WAN, etc.
- ✓ Topologie: bus, étoile, anneau, maillée, etc.
- ✓ Le mode de d'acheminement: commutation de circuit, commutation de messages (données) et commutation de paquets.

1.5.1 Selon la distance (la portée)

Les réseaux informatiques peuvent être répartis selon la distance (la portée) en plusieurs classes comme on peut voir dans le tableau ci-dessous ; voir aussi la figure 1.1.

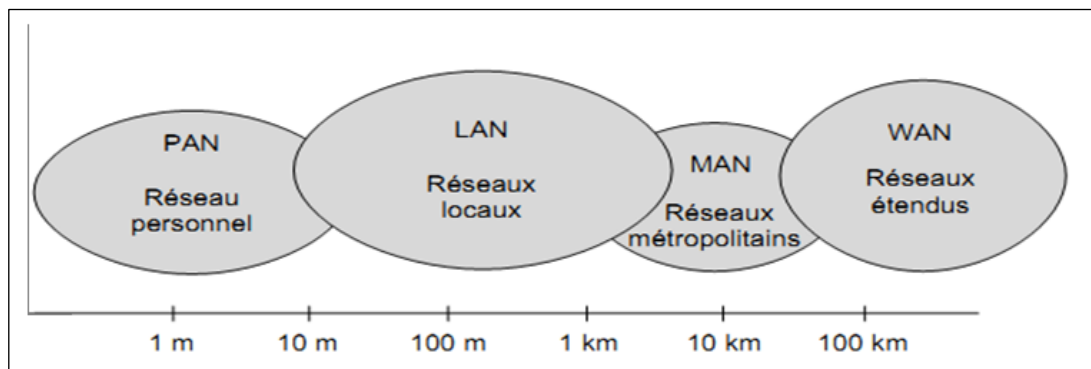


Figure 1.1 Catégories de réseaux selon la distance

PAN	Espace réduit	Quelques mètres
LAN	Immeuble, Salle	Dizaine de m jusqu'à 1 km
MAN	Ville, Campus	Dizaine de km jusqu'à 100 km
WAN	Continent, région	Plus de 100Km
Internet	La terre entière	

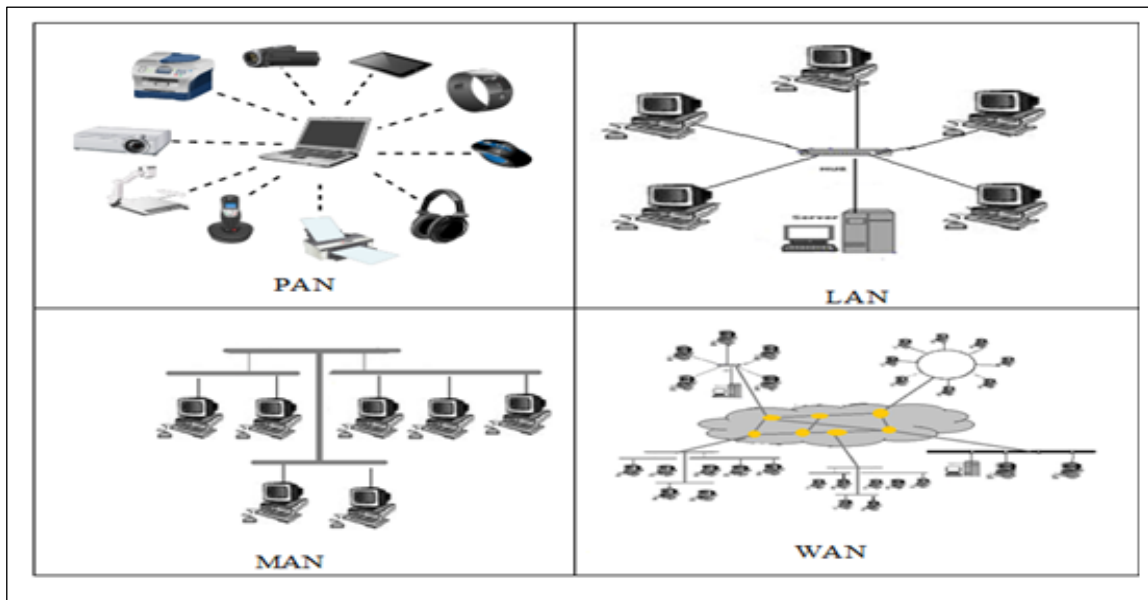


Figure 1.2 Type de réseaux

- **Réseau PAN (Personal Area Network)**
 - Interconnecte sur quelques mètres (souvent par des liaisons sans fil) des équipements personnels tels que les téléphones portables, PDA, oreillettes, etc.
 - Il représente la plus petite taille qu'un réseau peut avoir.
- **Réseau LAN (Local Area Network) ou encore appelé réseau local**
 - Un réseau local est d'étendue limitée à une circonscription géographique réduite (bâtiment, campus...).
 - Ces réseaux destinés au partage local de ressources informatiques (matérielles ou logicielles). Généralement ils sont constitués d'ordinateurs et de périphériques reliés entre eux et implantés dans une même entreprise à caractère **privé**.
 - Ils ne dépassent pas la centaine de machines et ne desservent jamais au-delà du kilomètre. Ils offrent des débits élevés de 10 à 100 Mbit/s.
 - Les LANs peuvent fonctionner selon deux modes : **Peer to peer** ou **clients/serveur**, et Principalement on peut distinguer deux types de LAN : Ethernet et en anneau.

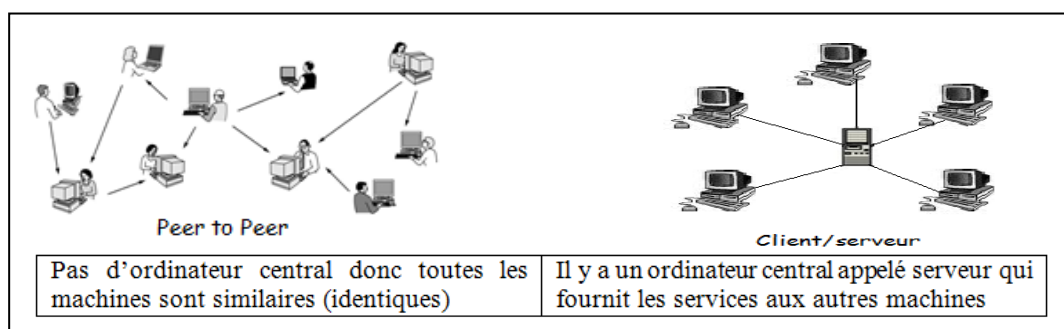


Figure 1.3 Exemples des LANs

- **Réseau MAN (Metropolitan Area Network)** ou Réseau Métropolitain
 - Ce type de réseau s'étend de 1 à 100 kilomètres et peut compter de 2 à 1000 abonnés
 - Il est utilisé pour relier des réseaux de type LAN sans que la vitesse de transfert ne soit affectée.
 - Il interconnecte plusieurs lieux situés dans une même ville, par exemple les différents sites d'une université ou d'une administration, chacun possédant son propre réseau local et à des débits importants (de 1 à 100 Mbits/s.).
 - Un MAN Peut être privé ou public et utilise un ou deux câbles de transmission sans avoir besoin d'éléments de commutation (routage).
- **Réseau WAN (Wide Area Network)** ou réseau étendu ou large portée
 - C'est un réseau étendu qui assure la transmission des données numériques sur des distances à l'échelle d'un pays, ou de la planète entière
 - Les WANs fonctionnent grâce à des routeurs; équipements d'interconnexion qui permettent de choisir le chemin le plus approprié pour atteindre un nœud du réseau.
 - Les WANs peuvent être des réseaux terrestres (essentiellement de la fibre optique), ou hertziens (comme les réseaux satellitaires).
 - Les débits offerts sont très variables de quelques kbit/s à quelques Mbit/s.

Remarque : On peut dire qu'un réseau WAN est un ensemble de réseaux LANs reliés par des routeurs.
- **Internet (réseau des réseaux)** avec la contrainte d'utilisation des protocoles TCP/ IP.

1.5.2 Selon la Topologie d'un réseau

La topologie d'un réseau appelée aussi la structure du réseau, indique comment le réseau doit être conçu et organisé au niveau physique ainsi qu'au niveau logique.

✓ Le niveau physique

- Un réseau informatique est constitué d'ordinateurs reliés entre eux grâce à du matériel (câblage, cartes réseaux, ainsi que d'autres équipements permettant d'assurer la bonne circulation des données).
- L'arrangement physique de ces éléments est appelé Topologie physique.

✓ Le niveau logique

- Elle correspond à la façon avec laquelle les données transitent dans les câbles
- Les protocoles de communication.
- Les programmes (applications) communicants.

Exemple de topologies

Il existe de nombreuses topologies possibles. En outre, il est également possible de combiner les différentes topologies pour former des topologies hybrides. Parmi les plus importantes topologies, on peut citer :

- **La topologie en bus** : c'est une topologie ancienne et très peu utilisée de nos jours. Elle repose sur le rattachement de chaque ordinateur du réseau à un câble principal appelé **Bus**. Hormis sa simplicité, cette structure présente de nombreux inconvénients et faiblesses en termes de performances et de vulnérabilité aux pannes matérielles ; Si un câble est hors service, l'ensemble du réseau ne fonctionne plus.

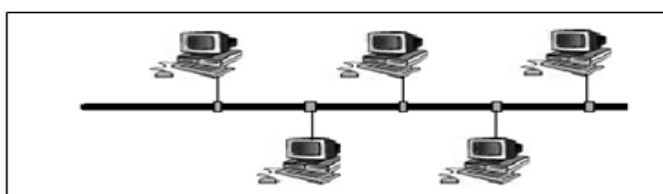


Figure 1.4 Topologie en Bus

- **La topologie en étoile** : C'est de loin la topologie la plus utilisée aujourd'hui. Elle consiste à connecter chaque ordinateur du réseau individuellement (au moyen d'un câble ou d'une connexion sans fil) à une partie centrale (exemple : hub, switch). Elle permet d'offrir de meilleures performances, flexibilité, sécurité et une vulnérabilité aux défaillances techniques.

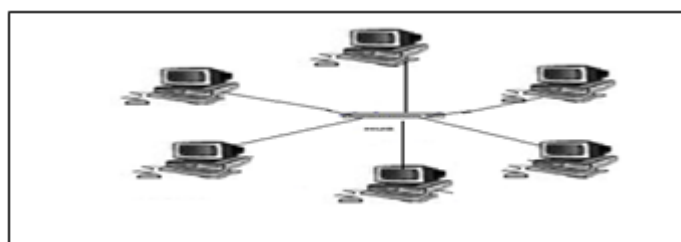


Figure 1.5 Topologie en Etoile

- **La topologie en Anneau** : dans ce type de topologie, chaque station est reliée à la suivante de manière circulaire. Ce type de liaison permet des débits de données élevés et convient aux longues distances. Le transfert d'informations se fait dans un seul sens afin d'éviter les collisions. En outre, ces dernières sont écartées par une gestion basée sur le respect des droits d'accès au support. Toutefois, l'anneau est vulnérable à la

rupture de la liaison. Ainsi, une autre boucle de secours est ajoutée pour éviter toute défaillance du réseau en cas de destruction des câbles.

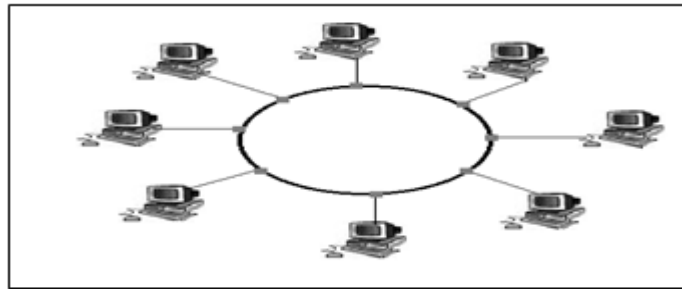


Figure 1.6 Topologie en Anneau

Autres topologies:

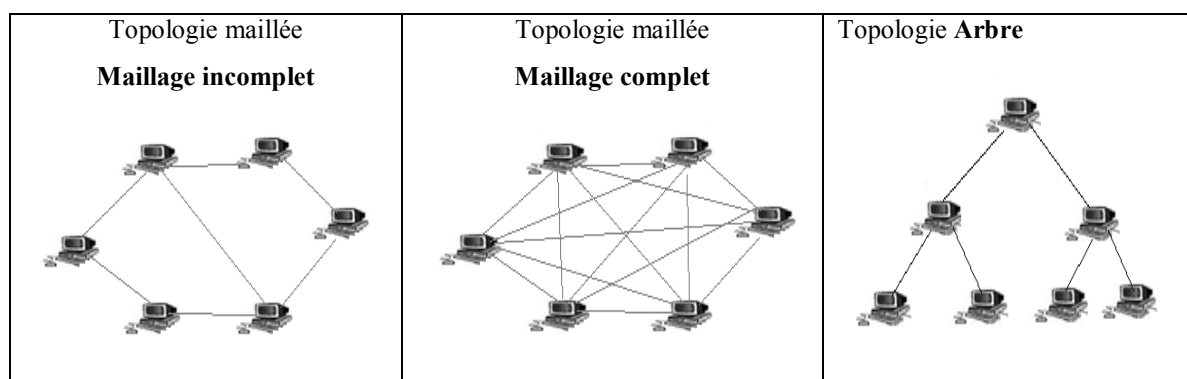


Figure 1.7 Différentes topologies (arbre, maillage complet/incomplet)

1.5.3 Selon le mode de commutation

La commutation rassemble toutes les techniques qui réalisent la mise en relation de deux utilisateurs quelconques. Elle décrit les modalités d'acheminement de l'information dans un réseau de nœuds reliés entre eux. Il existe plusieurs techniques de commutation comme par exemple:

- Commutation de circuits → Réseaux téléphoniques
- Commutation de messages → eMail
- Commutation de paquets → Internet

- Commutation de circuit

- Un lien physique est établi par juxtaposition de différents supports physiques afin de constituer une liaison de bout en bout entre une source et une destination (exemple : le Réseau Téléphonique Commuté (RTC)).

- Commutation de messages

- Consiste à envoyer un message de l'émetteur jusqu'au récepteur en passant de nœud de commutation en nœud de commutation.
- Chaque nœud attend d'avoir reçu complètement le message avant de le réexpédier au nœud suivant
- Cette technique nécessite de prévoir de grandes zones tampon dans chaque nœud du réseau

- Commutation de paquets

- Un message émis est découpé en paquets et par la suite chaque paquet est commuté à travers le réseau comme dans le cas des messages
- Les paquets sont envoyés indépendamment les uns des autres
- Ils n'arrivent pas dans l'ordre initial, soit parce qu'ils ont emprunté des routes différentes, soit parce que l'un d'eux a dû être réémis suite à une erreur de transmission.

Un réseau à commutation par paquets peut offrir différents services

- ✓ **Service sans connexion** : *Service non fiable, sans garantie de délivrance, de l'ordre de réception ou des délais*
 - Chaque paquet est acheminé indépendamment des autres
 - Chaque paquet contient les adresses source et destinataire
- ✓ **Service orienté connexion** : *Service fiable*
 - Lors de l'établissement, des paramètres comme la vitesse de transmission, la taille des paquets, la numérotation des paquets, etc. peuvent être négociés.

1.6 Conclusion

L'intérêt pour les réseaux de communication ne cesse de croître et leurs différentes utilisations possibles démontrent la diversité de leurs applications. Dans ce chapitre, nous avons présenté les fondements et les notions de base d'un réseau de communication ainsi que ses caractéristiques. Nous avons également passé en revue les différentes classifications proposées pour ces réseaux.

Le chapitre suivant sera consacré à l'étude détaillée du concept de la normalisation dans les réseaux et plus précisément nous étudierons le modèle OSI et ses différentes couches.

Chapitre 2

La normalisation et architecture en couches

2.1 Introduction

Les composants électroniques et les technologies de communication utilisés pour créer les réseaux informatiques sont nombreux et variés. En fait, la prolifération des modalités des réseaux est principalement liée à la diversité des utilisations et des exigences des applications, qui requièrent des solutions différentes. L'inconvénient de cette situation est qu'il y a différentes technologies, types de systèmes et de protocoles à comprendre et à manier ensemble. Or, les réseaux informatiques doivent permettre aux différents utilisateurs et applications de coopérer sans avoir à tenir compte de l'hétérogénéité des équipements électroniques et des processus de transmission (topologie, méthode d'accès, caractéristiques des équipements, caractéristiques des supports, etc.). Cela est possible grâce à une démarche de normalisation ou de standardisation.

Dans ce chapitre, nous allons présenter les normes spécifiant les réseaux en détaillant leurs principes et modèles.

2.2 Pourquoi la normalisation ?

A l'aube des années 70, les constructeurs ont développé leur propre solution réseau basée sur une architecture et des équipements privés comme SNA d'IBM, DSA de Bull, TCP/IP du DoD, etc. Chaque réseau utilise ses propres spécifications et implémentations pour échanger les données. Cependant, afin de profiter de la technologie réseau, les sociétés avaient besoin d'interconnecter leurs réseaux. Néanmoins, il a été constaté qu'il serait impossible d'interconnecter ces différents réseaux hétérogènes sans établir une norme internationale. Par conséquent, une normalisation de ces architectures était requise. Cependant, la normalisation permet de :

- Résoudre le problème de l'incompatibilité des équipements matériels et garantir leur interconnexion.
- Aider les fournisseurs et les constructeurs à créer des réseaux compatibles et interopérables.

- La décomposition de l'ensemble complexe du réseau en entités simples et fonctionnellement homogènes; les couches.

Les organismes de normalisation les plus connus sont :

- **ISO** : International Standardisation Organisation.
- **IEEE** : Institute of Electrical and Electronics Engineers.
- **UIT_T** : Union Internationale de Télécommunication section Télécommunication (ex.: CCITT).
- **ANSI** : American National Standards Institute.
- **AFNOR** : Association Française de Normalisation.
- **IAB** : Internet Activitie vjhyjhjiyhn jy b èys Board.

2.3 Les modèles d'architectures réseaux

Deux types d'architectures sont mises au point par l'industrie. La première émane de la norme ISO et se nomme OSI (Open System Interconnexion). Quant à la seconde, elle est appelée TCP/IP. Il est à noter qu'une troisième structure très récente qui provient de l'UIT-T (Union Internationale des Télécommunications). Ce modèle de référence constitue la version adaptée du modèle OSI pour intégrer les réseaux à haut débit.

2.3.1 Le Modèle de référence OSI

En 1978, l'Organisation internationale de normalisation (ISO) l'Organisation internationale de normalisation (ISO) a développé une architecture qui permettrait aux dispositifs de différents fabricants de fonctionner ensemble pour communiquer avec différents systèmes d'exploitation. En 1984, l'architecture ISO est devenue une norme internationale connue sous le nom de modèle de référence **Open Systems Interconnection (OSI)**. Cette architecture détermine comment le matériel, les logiciels, les topologies et les protocoles existent et fonctionnent sur un réseau.

Le modèle OSI **est basé sur sept (07) couches**, comme le montre la figure 2.1. Chaque couche ajoute des fonctionnalités à la couche précédente et communique avec les couches supérieures et inférieures. Étant donné que chaque couche du modèle OSI gère une partie différente du processus de communication, le processus de résolution des incidents et défaillances est un plus simple car il fournit des spécifications sur la façon dont les éléments doivent fonctionner.

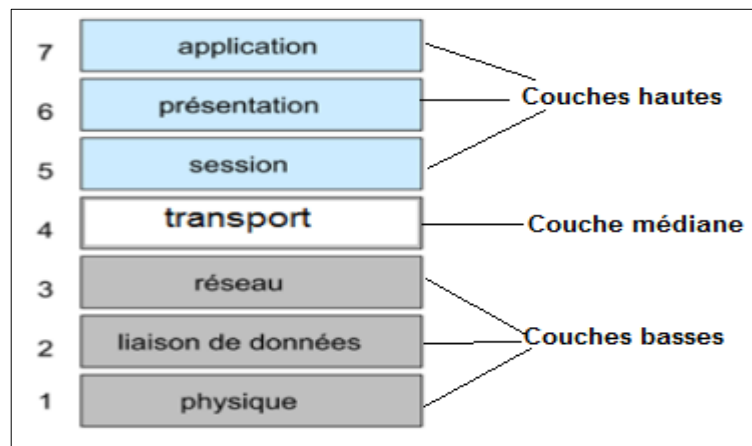


Figure 2.1 Le Modèle OSI

- ✓ Les couches hautes sont orientées transmission de données :
 - rendent un service d'accès.
 - comportent les fonctions de traitement sur les données transportées.
- ✓ Les couches basses sont orientées applications :
 - rendent un service de transport.
 - comportent les fonctions de transmission de données.
- ✓ La couche transport est une couche médiane.
- ✓ Analogie du modèle OSI avec un échange humain :
 - Je souhaite parler → la couche application (7).
 - On doit utiliser la même langue → la couche présentation (6).
 - On commence par se dire bonjour → la couche session (5).
 - On s'assure que l'autre a bien reçu le message → la couche transport (4).
 - Chemin emprunté par le son → la couche réseau (3).
 - Préparation à l'envoi (air, téléphone) → la couche liaison de donnée (2).
 - Le son se propage dans la ligne téléphonique → la couche physique (1).

➤ Rôle des 7 couches du modèle OSI

• La couche physique

Elle assure le transport de l'information. Au fait, un grand nombre de techniques de transmission gérées par des méthodes en général uniformisées sont possibles. L'unité d'information utilisée à ce niveau est **le bit**. Alors cette couche permet :

- La spécification des connecteurs
- La détermination des caractéristiques électriques des circuits
- La définition des procédures d'utilisation des connexions physiques

- **La couche liaison de données**

Elle est responsable de l'acheminement sans erreurs de blocs d'informations sur les liaisons des données. Elle supervise le fonctionnement de la transmission et définit la topologie du réseau, l'accès au réseau, la livraison ordonnée des données. L'unité de données utilisée à ce niveau est la **Trame (Frame)**. Globalement cette couche assure:

- Le contrôle de flux.
- Le contrôle d'erreur.

- **La couche réseau**

Elle s'occupe de la transmission des données d'un ordinateur à l'autre, même s'il se trouve sur un réseau distant est responsable. Ces données peuvent traverser plusieurs nœuds intermédiaires selon une politique bien définie (le routage). L'unité de données utilisée à ce niveau est le **Paquet (Packet)**. Ses principales fonctions sont :

- Adressage
- Routage
- Contrôle de congestion et d'erreurs.

- **La couche transport**

Elle se charge de la transmission de bout en bout des informations sur le réseau. Dans ce niveau, l'unité de données utilisée est le **message**.

Cette couche est à la liaison entre les couches orientées transmission, qui sont les couches inférieures (1, 2, 3) et les couches orientées traitement de l'information, qui sont les couches supérieures (5, 6, 7). Ses fonctionnalités sont:

- La reprise sur erreur
- Le contrôle de flux
- L'optimisation

- **La couche session**

Elle est responsable de la synchronisation et du séquençage du dialogue et des paquets dans une connexion réseau. Cette couche est également chargée de s'assurer que la connexion est maintenue jusqu'à la fin de la transmission, et que les mesures de sécurité appropriées sont prises pendant une "session". Cette couche est utilisée par la couche présentation située au-dessus d'elle, et utilise la couche transport située en dessous. Elle a pour tâches :

- L'organisation du dialogue.
- La synchronisation du dialogue.
- L'établissement et libération d'une session.

• La couche présentation

Elle est responsable de la mise en forme (convertir, structurer) les données échangées par les applications. Elle est donc responsable de la présentation des informations d'une manière qui convient aux applications ou aux utilisateurs qui les traitent. Cela est pour avoir une compatibilité entre les différents équipements raccordés au réseau. Elle englobe :

- La traduction des données.
- La compression.
- Le cryptage.

• La couche application

Elle est responsable de l'accès des applications au réseau. Elle fournit ainsi à l'utilisateur des services pour réaliser une application répartie et pour accéder à l'environnement réseau. Les services de cette couche sont beaucoup plus variés que les services des couches inférieures, car toute la gamme des possibilités d'applications et de tâches est disponible ici. Exemples d'applications réseaux:

- Interrogation de BD.
- Transfert de fichiers.
- La messagerie électronique.
- Le partage des ressources distantes.

2.3.2 Le modèle TCP/IP

Les protocoles TCP/IP doivent leur nom à deux de leurs principaux protocoles : le protocole de contrôle de transmission (TCP) et le protocole Internet (IP). Ce modèle combine en une seule couche les différents paramètres liés à l'application et considère que les données sont correctement préparées pour la couche suivante. En outre, il comprend également la couche session et la couche présentation et traite les protocoles de haut niveau, les questions de représentation, le code et le contrôle du dialogue.

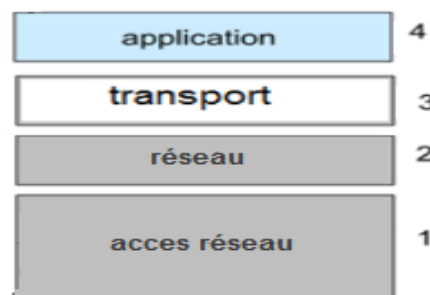


Figure 2.2 Le ModèleTCP/IP

Ce modèle sera étudié en détail dans le chapitre 6. Toutefois, on va résumer brièvement, dans la suite de ce paragraphe, les principales fonctionnalités de ses couches.

- **La couche accès réseau**

- Cette couche combine les fonctions des deux couches les plus basses du modèle OSI à savoir la couche physique et la couche liaison de données.
- Elle assure la livraison des données aux différents systèmes connectés au réseau.

- **La couche réseau**

- Cette couche assure toutes les fonctions nécessaires à un paquet IP pour parvenir au destinataire.
- Elle inclut des détails sur les technologies et les méthodes de communication pour router les paquets IP.

Assure une abstraction aux détails des couches physiques et de liaison de données du modèle OSI ; groupés dans la même couche appelée accès réseau

- **La couche transport**

- Cette couche est responsable de la qualité du service, y compris la fiabilité, le contrôle du flux et la correction des erreurs.
- Détermine l'application à laquelle les paquets doivent être livrés.
- En fonction du mode de transport des données de bout en bout, on distingue deux protocoles : TCP (Transmission Control Protocol) et UDP (User Datagram Protocol).
- Le protocole TCP constitue un excellent moyen de créer des communications réseau souples, fiables, à faible taux d'erreur et ordonnées.
- Le protocole UDP est une extension du protocole IP où aucun contrôle n'est fourni.

- **La couche application**

- Elle regroupe les couches session, présentation et application du modèle OSI.
- C'est la couche la plus riche en termes de nombre d'applications réseau et de services associés.

2.4 Modèle en couches

Les éléments qui composent un réseau sont très différents selon l'application d'où ils proviennent et les informations qui en découlent. Or, l'organisation de ces équipements informatiques très variés reliés en réseau repose sur une structuration en couches. Cette organisation en couches permet de :

- Réduire la complexité du système en le découpant en plusieurs entités (couches).
- Uniformiser les interfaces afin de simplifier le contrôle du flux échangé.

- Faciliter la conception et l'implémentation modulaire ainsi que les tests et les vérifications des erreurs.
- Assurer l'interopérabilité des technologies en offrant une certaine abstraction à leurs détails, ce qui rend les réseaux plus portables et flexibles.
- Simplifier l'enseignement et l'apprentissage du réseau.

2.4.1 Les unités de données et communication entre les couches

Sur n'importe quel équipement d'un réseau, différentes fonctions logicielles et matérielles peuvent fonctionner simultanément. Par exemple, les sept couches du modèle de référence OSI sont utilisées pour répartir les différentes fonctions nécessaires à la réalisation du réseau. En général, tous les éléments composant un réseau fonctionnent ensemble afin de mettre en œuvre ses services (voir figure 2.3) :

- Il est nécessaire que les couches puissent **communiquer verticalement** entre **les couches adjacentes situées** sur **un même hôte** donné (service).
- Aussi, pourvoir communiquer **horizontalement** avec **les couches homologues** d'un **autre hôte** (protocole).
- Le mécanisme de communication entre les couches adjacentes s'appelle **une interface** ; L'interface entre les couches se réfère typiquement au processus par lequel les données sont transmises entre la **couche N** et **la couche N-1** ou **la couche N+1** (SAP).

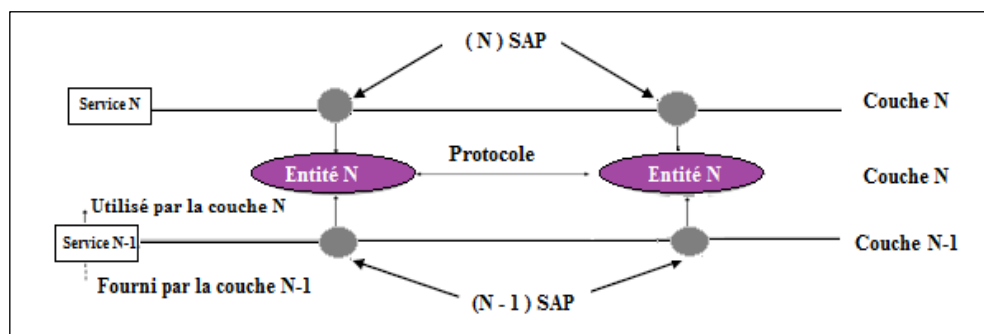


Figure 2.3 Communication entre couches

a. Communication Horizontale (Protocole)

- Chaque couche du modèle de référence OSI a un ensemble de tâches générales dont elle est responsable.
- Sur chaque réseau, les dispositifs matériels et les logiciels fonctionnent sur différentes couches du modèle.

- Les fonctions exécutant une tâche particulière sur la machine " Hôte A" sont conçues pour communiquer avec des programmes similaires ou complémentaires qui fonctionnent sur la machine " Hôte B" ; (voir figure 2.4).
- Cette communication est logique (virtuelle)
- Aucun message ne passe directement d'une entité à son homologue.
- Ces éléments du réseau sont contraints de parler le même "langage" pour se comprendre: ils recourent à un protocole.
- Un protocole est un ensemble de règles ou de procédures qui définissent la communication entre des éléments logiciels ou matériels fonctionnant sur la même couche de dispositifs de réseau.

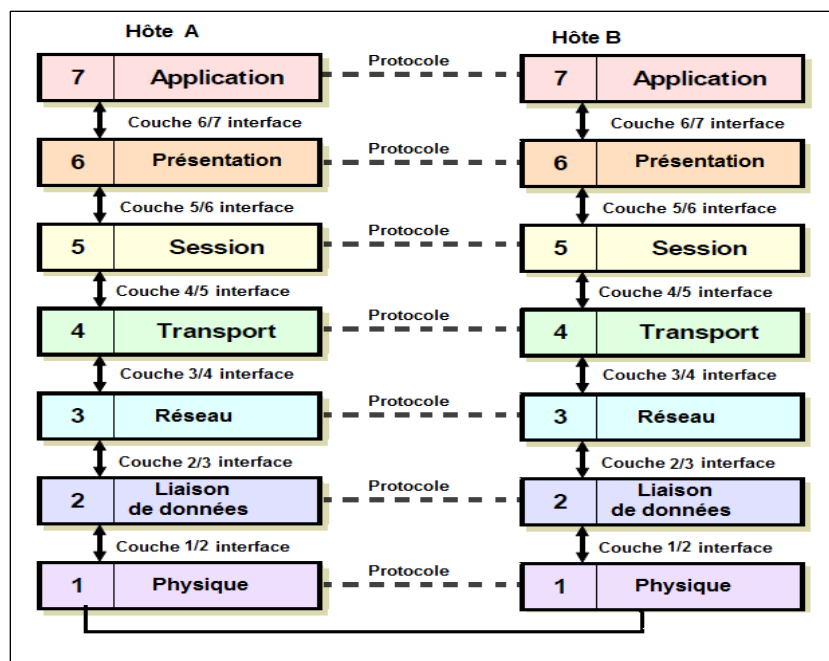


Figure 2.4 La communication horizontale dans un modèle OSI

b. Communication Verticale (Service)

- Représente le chemin réel emprunté par les données qui traversent les différentes couches.
- La communication verticale se fait de haut en bas de la pile des protocoles à chaque fois que des données sont envoyées à travers le réseau, et aussi, à chaque fois qu'elles sont reçues ; voir figure 2.5.
- Chaque couche réalise un service bien défini
 - Une couche est le fournisseur de service pour la couche immédiatement supérieure
 - Une couche est l'utilisateur de service de la couche immédiatement inférieure.

- Les couches supérieures regroupent les données et les envoient aux couches inférieures pour qu'elles soient envoyées sur le réseau.
- Au niveau le plus bas, Le support physique véhicule les données sur le réseau
- Au niveau de la réception, le processus est inversé: les données remontant jusqu'aux couches supérieures sur le terminal de destination.

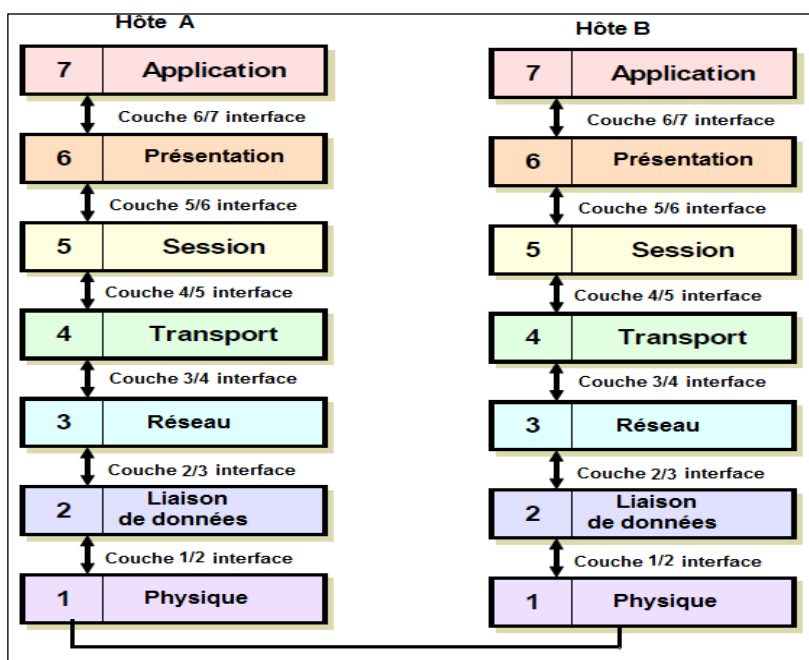


Figure 2.5 La communication verticales dans un modèle OSI

c. Point d'accès au service SAP (Service Access Point)

- L'échange de données et de primitives entre ces couches se fait par l'intermédiaire des points d'accès de service (*SAP Service Access Point*).
- Chaque SAP est identifié par un numéro unique. On peut trouver d'autres dénominations pour les SAP comme : port, porte et socket ...etc.
- Il assure la connexion entre deux entités de couches adjacentes.
- Une entité peut être connectée à plusieurs entités des couches adjacentes.
- Lors de la communication, l'entité doit préciser l'entité destinatrice.

2.4.2 Les Services

- Le service fourni par une couche quelconque est exprimé sous la forme d'une primitive de service avec les données à transférer en tant que paramètre.
- Une primitive de service est une demande de service fondamentale faite entre les protocoles. Par exemple, la couche N+1 peut se trouver au-dessus de la couche N. Si N+1 souhaite invoquer un

service de N, elle peut émettre une primitive de service sous la forme de **N. Demande de connexion à N**.

- Les primitives de service sont généralement utilisées pour transférer des données entre les différents processus d'un ordinateur.

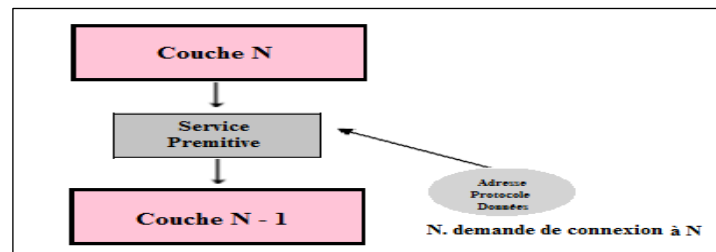


Figure 2.6 Service (Primitives de service)

2.4.3 L'encapsulation des données

- L'échange de données entre deux points terminaux d'un réseau traverse les différentes couches : la couche N de la machine source communique avec sa couche homologue N de la couche de destination

- Les règles et conventions utilisées sont appelées Protocole de couche N.

- Les données traversent toutes les couches (Application,..., physique).

- Chaque couche ajoute aux données des informations relatives au protocole, i.e. son propre ensemble de fonctions spécifiques : il s'agit de l'**en-tête**, puis les transmettre ;

- **L'en-tête**: est l'ensemble d'informations qui garantissent la transmission.

- A chaque niveau, le paquet de données change d'aspect, car on lui ajoute un en-tête, ainsi les appellations changent suivant les couches :

- Le paquet de données est appelé **message** au niveau de la **couche application**.
- Le message est ensuite encapsulé sous forme de **segment** dans la **couche transport**.
- Le segment une fois encapsulé dans la **couche réseau** prend le nom de **datagramme**.
- Enfin, on parle de **trame** au niveau de la **couche accès réseau**.

- Les données sont encapsulées ; l'**Encapsulation** : est le processus de conditionnement des données consistant à ajouter un en-tête de protocole déterminé avant que les données ne soient transmises à la couche inférieure.

- A la destination, l'opération est effectuée à rebours ; le protocole de chaque couche de destination rétablit la forme originale des informations : lors du passage dans chaque couche, l'en-tête est lu, puis supprimer, donc le message est dans son état originel à la réception.

La figure 2.7 résume les étapes de ce processus d'encapsulation.

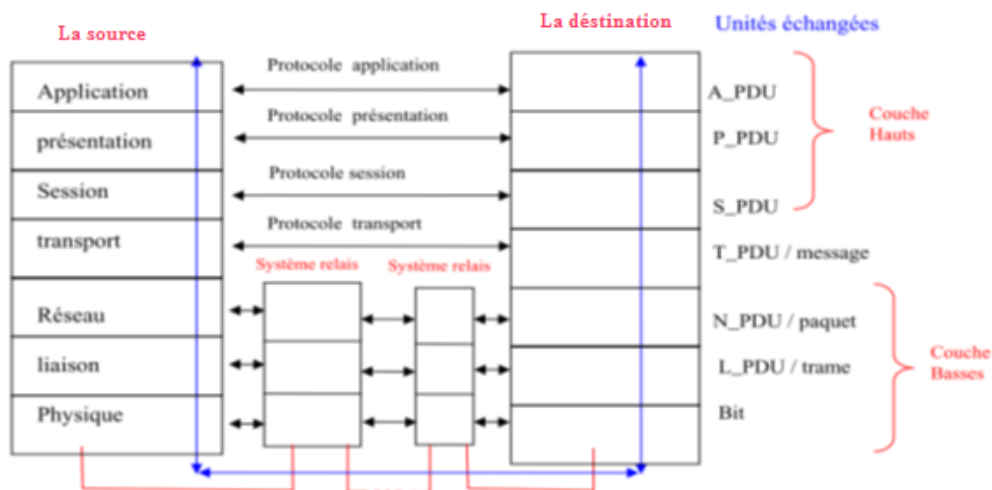


Figure 2.7 L'encapsulation des données

PDU : DU échangées entre entités paires

Data Unit (DU): Les entités échangent les informations sous forme d'unités de données

2.5 Conclusion

Dans ce chapitre, nous avons introduit les principaux piliers des Normes de réseau, à savoir les modèles OSI et TCP/IP. Par ailleurs, nous avons présenté les aspects fonctionnels de ces modèles ainsi que leurs volets et caractéristiques. Nous avons également exposé les principes directeurs de la structuration en couches et de ses divers éléments.

Dans le chapitre suivant, nous présentons en détail les différents équipements d'interconnexion et de réseau, où nous allons énumérer leurs principes de fonctionnement et caractéristiques.

Chapitre 3

Les équipements d'interconnexion et de réseautage

3.1 Introduction

Un réseau local est utilisé pour interconnecter les différents appareils d'une société. Cependant, la plupart des sociétés possèdent plusieurs réseaux locaux et il est donc parfois nécessaire de les relier entre eux. Ainsi, l'interconnexion regroupe les spécificités de chaque réseau et offre un service commun à tous les équipements, faisant apparaître tous ces réseaux hétérogènes comme un seul réseau (voir figure 3.1).

Dans ce qui suit, nous allons mettre l'action sur les éléments nécessaires à la mise en œuvre d'une connexion de réseaux. Pour ce faire, nous présentons tout d'abord les différentes technologies et équipements utilisés dans la transmission de données et l'interconnexion de réseaux. Par la suite, nous détaillons les dispositifs réseaux et enfin, nous présentons un exemple de réseaux existant. Il est à noter que nous présentons dans ce cours qu'un sous ensemble d'exemple de type de réseaux locaux.

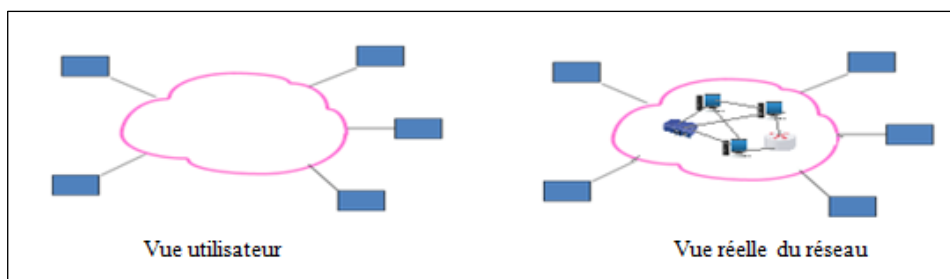


Figure 3.1. Interconnexion de réseaux

3.2 Média de transmission ou Câblage

- Pour relier les différentes entités d'un réseau, plusieurs supports physiques de transmission peuvent être utilisés. En outre, ces supports sont utilisés aussi pour la transmission et la gestion des signaux.
- Ils sont classés en fonction de la gamme de fréquences qu'ils sont capables de tenir.
- Ils reposent sur la propriété de conductivité électrique des métaux (cuivre, bronze,...).

Il existe de nombreux types de câbles, mais on distingue généralement:

- **Le câble de type coaxial**
- **La paire torsadée**
- **La fibre optique**

Il faut noter que d'autres techniques de liaison sont aussi disponibles telles que :

- **CPL (courants Porteurs en Ligne)** utilisant des lignes d'alimentation électriques. Ces techniques sont réservées le plus souvent aux réseaux domestiques (indoor).
- **Les ondes électromagnétiques (liaisons RF , Radio Frequency)** permettent de réaliser des réseaux sans fils comme les réseaux sans fils locaux ou WLAN (Wireless Local Area Network), et ce en utilisant les techniques de Wi-Fi (Wireless Fidelity), UWB, LoraWAN, Bluetooth, Zigbee, ect.

3.2.1 Le câble coaxial

C'est le type de câble le moins cher. Il est constitué par un câble de cuivre rigide placé au cœur d'un tube en plastique épais, lui-même recouvert d'une feuille de métal assurant sa protection contre les perturbations électriques extérieures. Grâce à cette isolation et ce blindage, le câble coaxial peut atteindre des taux de transmission de données acceptable. Le câble coaxial est assez courant dans les systèmes de télévision par câble.

3.2.2 La paire torsadée

Le câble à paires torsadées servait à l'origine aux lignes téléphoniques. C'est le support le plus utilisé à l'intérieur des immeubles. Deux types peuvent être distingués :

- Le câble à paire torsadée **non blindée** (UTP).
- Le câble à paire torsadée **blindée** (STP).

- **La paire torsadée non blindée (UTP : Unshielded Twisted Pair)** est composée de 2, 4, 6 ou 8 fils torsadés deux par deux. Ces fils ne sont protégés que par une gaine plastique isolante. Il s'agit du support le plus répandu dans les réseaux informatiques, avec des connecteurs au format RJ45.

- **La paire torsadée blindée (STP : Shielded Twisted Pair)** : La STP est une UTP renforcée par une feuille ou une natte métallique de protection, outre la gaine isolante, en vue de mieux résister aux perturbations extérieures.

Avec **le blindage**, il est possible de diminuer les interférences (mélange de signaux électriques provenant de plusieurs lignes,...). Il peut être apposé sur la totalité du câble mais il peut aussi être appliqué de manière isolée sur chacune des paires qui le composent. Si le blindage est appliqué à l'ensemble, on parle **d'écrantage** et la feuille métallique formant le blindage est appelée **écran**.

3.2.3 La Fibre Optique

Une fibre optique est un support fin et flexible qui conduit des impulsions de lumière. Chaque impulsion représentant un bit. Une seule fibre optique peut supporter d'énormes débits binaires, jusqu'à des dizaines ou même des centaines de gigabits par seconde. Elle est aussi insensible aux parasites électriques. C'est donc un meilleur support que la paire torsadée ou le câble coaxiale. Une fibre optique est dite **monomode** si le taux de réfraction du signal qu'elle transporte est minimal. Moins le diamètre de la fibre est important, plus la réfraction est faible et plus la distance que le signal peut parcourir sans devoir être régénéré est grande.

La fibre optique est un câble possédant de nombreux avantages

- ✓ Légèreté
- ✓ Immunité au bruit
- ✓ Permet des débits de l'ordre de 100 Mbits/s à 1 Gbits/s
- ✓ Largeur de bande de quelques dizaines de mégahertz à plusieurs gigahertz.
- ✓ Elle est très adaptée à la connexion entre les réseaux de distribution (connexion centrale entre plusieurs immeubles, appelée épine dorsale) car il permet des connexions sur de longues distances.
- ✓ C'est un câble très sécurisé car il est extrêmement difficile de le mettre sur écoute.

Cependant, malgré sa souplesse mécanique, la fibre optique n'est pas adaptée aux connexions d'un réseau local car son installation est problématique et son coût est élevé (c'est pourquoi la paire torsadée est préférée pour les petites liaisons).

3.3 Les équipements d'interconnexion

Les longueurs des segments d'un réseau local sont limitées en raison des contraintes physiques et du domaine de collision. Il est souvent nécessaire d'augmenter cette portée. Cela peut être réalisé au moyen d'un certain nombre de dispositifs d'interconnexion, allant des répéteurs aux passerelles comme illustré sur la figure 3.2. Ci-dessous les équipements les plus utilisés :

- **Le répéteur** : agit au niveau de la couche physique.
- **Le pont** : assure une conversion jusqu'au niveau liaison de données.
- **Le commutateur** : gère l'aiguillage des blocs d'information.
- **Le routeur** : traduit les protocoles de la couche réseau.
- **La passerelle** : intervient à partir de la couche 4.
- **Les Coupe-feux ou FireWall.**
- **Les Gateways.**

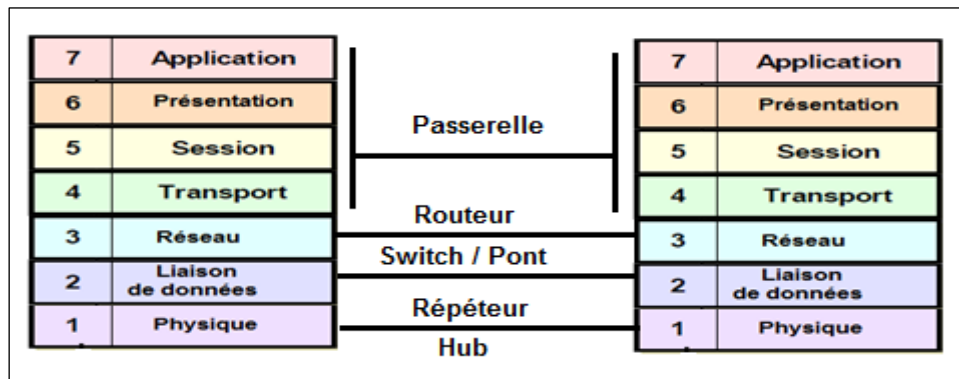


Figure 3.2 Les équipements réseau

3.3.1 Les Répéteurs

Le répéteur est un équipement électronique employé pour amplifier un signal numérique et prolonger la distance maximale entre deux noeuds d'un réseau. Il fonctionne au niveau **Physique (bit)**. Il a pour fonctions:

- La répétition des bits d'un segment à l'autre en reliant deux segments de câbles sur un même réseau et permet ainsi de s'affranchir des limitations de distances imposées par les normes
- La régénération du signal pour compenser l'affaiblissement du signal.
- Changer de média (passer d'un câble coaxial à une paire torsadée, etc.).
- Il a un port d'entrée et un port de sortie (le signal entrant étant répété et amplifié).
- Il ne modifie pas le débit d'un réseau.

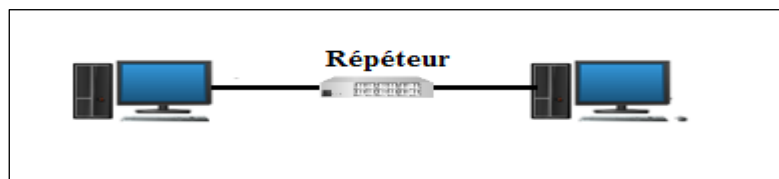


Figure 3.3 Schéma d'utilisation d'un répéteur

Limitations

- ✓ Les répéteurs ne peuvent être utilisés que sur les mêmes types de segments. Par exemple, Ethernet- Ethernet ou Token Ring-Token Ring.
- ✓ Pas de conversion de signaux (Optique → électrique)

3.3.2 Concentrateurs / Hubs

Un concentrateur (ou Hub) est un répéteur multiport. Sa fonction est aussi de régénérer, resynchroniser et propager le signal reçu entre plusieurs machines. Son **niveau d'utilisation** est la **couche physique**. Il a une fonction de répéteur, mais aussi :

- Permet de mixer différents médias (paire torsadée, fibre optique, ...).

- Utiliser une topologie physique en étoile.
- Les concentrateurs sont appelés aussi "concentrateurs" car ils centralisent le signal pour le répéter sur tous ses ports. La trame qui arrive sur l'un des ports d'un hub est immédiatement répétée sur tous les ports de ce hub.

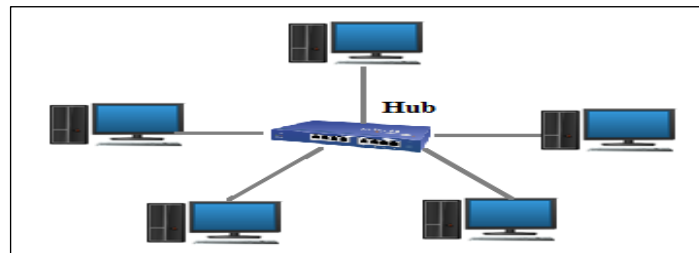


Figure 3.4 Schéma d'utilisation d'un Hub

3.3.3 Les Ponts

Aussi appelé Bridge, il intervient au niveau de la **liaison de données** sur les trames. Il fournit les services des répéteurs, avec l'ajout de :

- Permet de segmenter le réseau en sous-réseaux indépendants.
- Capable de convertir des trames de formats différents (ex : Ethernet à Token Ring).
- Dispositif actif filtrant (collision):
 - permet de diminuer la charge du réseau : amélioration des performances.
 - Sécurisation des échanges entre segments
- Les ponts sont des répéteurs filtrants. Le pont laisse passer les trames qui correspondent au sous-réseau qu'ils protègent.

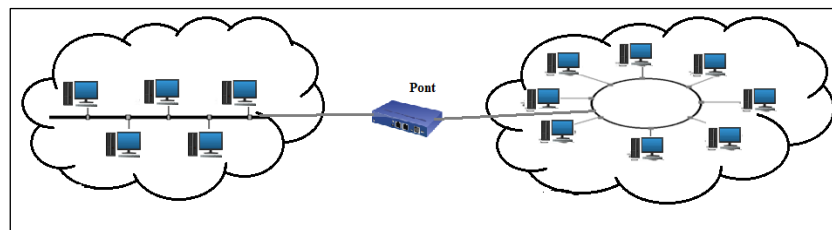


Figure 3.5 Schéma d'utilisation d'un Pont

3.3.4 Les Commutateurs / Switch

C'est un pont multiport qui assure les mêmes fonctions qu'un pont mais, en utilisant des ports dédiés pour filtrer le trafic et l'acheminer uniquement vers son destinataire. Il agit au niveau 2 **Liaison de données** du modèle OSI.

- Peut gérer simultanément plusieurs communications (liaisons).

- ✓ Les switchs sont des hubs intelligents qui, au lieu de répliquer bêtement les trames reçues à toutes les stations (plus précisément, tous ses ports), ils les acheminent à la station qui convient (le port lui correspondant plus exactement).

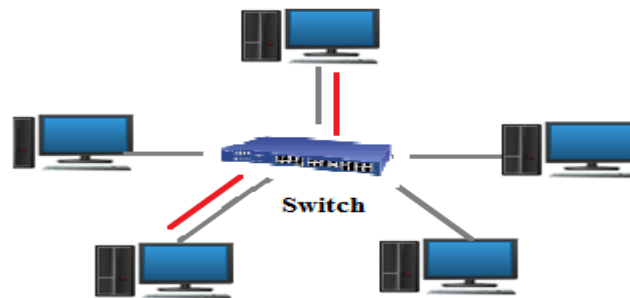


Figure 3.6 Schéma d'utilisation d'un switch

3.3.5 Les Routeurs

Un routeur est un dispositif doté de plusieurs interfaces réseau. Chaque interface est connectée à un réseau. Il assure le routage des paquets d'un réseau à l'autre et fournit des fonctions de contrôle et de filtrage du trafic. Il opère **au niveau réseau** (couche 3 du modèle OSI), en utilisant des adresses logiques.

- ✓ Il est totalement indépendant des couches physiques/de liaison et il permet donc d'interconnecter des réseaux physiques de nature hétérogène.
- ✓ Permet des interconnexions à travers des réseaux longues distances, comme vers plusieurs sous-réseaux.

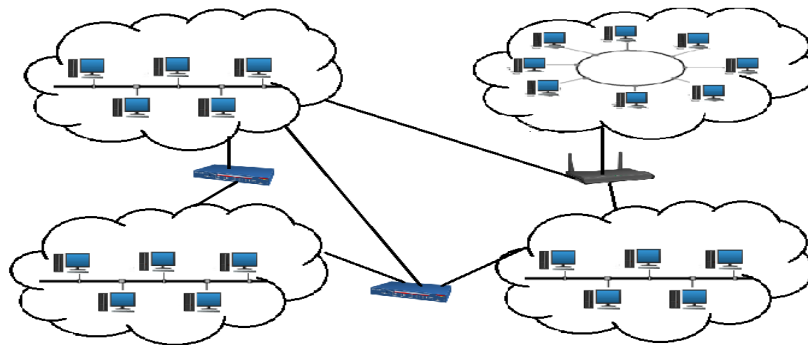


Figure 3.7 Schéma d'utilisation d'un routeur

3.3.6 Coupe-feux (pare-feu)

Également appelé pare-feu, ce dispositif est un routeur disposant de fonctionnalités étendues. Il assure une sécurité accrue (Access Control List). Il est placé sur la façade d'accès externe afin de protéger les réseaux internes ;

- ✓ Vérifie si les règles de sécurité (définies par un administrateur) permettent le transfert de paquets vers le destinataire
- ✓ Filtrage des requêtes FTP, HTTP, et autres services.
- ✓ Prévention contre les chevaux de Troie ou virus par filtrage e-mail, etc.
- ✓ Vérification et enregistrement de tous les échanges.

3.3.7 Passerelle (Gateway)

Une passerelle est une interface qui relie des réseaux de types hétérogènes. Elle fonctionne au niveau de la couche transport et supérieure (4 et sup). Si le réseau ne reconnaît pas la destination de l'information, il la transmet à une passerelle par défaut.

Exemples : les messageries d'entreprise, serveurs de fichiers et d'impression, etc.

- ✓ Deux types de passerelles sont disponibles:
 - **Une passerelle de transport**: raccorde les flux de données d'un protocole de couche de transport.
 - **Une passerelle d'application**: relier deux parties distinctes d'une application distribuée dans le monde entier.

3.4 Exemples de réseaux existants : Ethernet et Token Ring

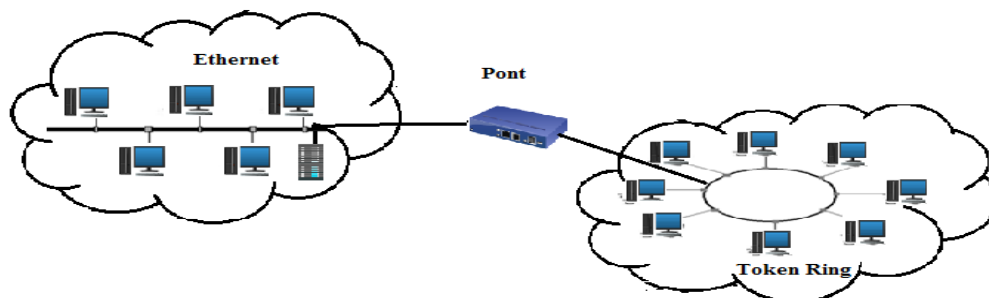


Figure 3.8 Ethernet et Token Ring

Le Réseau local Ethernet

- ✓ Tous les ordinateurs d'un réseau Ethernet sont connectés à la même ligne de transmission et la communication se fait à l'aide d'un protocole appelé CSMA/CD (Carrier Sense Multiple Access with Collision Detect).
- ✓ Ce protocole permet un accès multiple avec détection de porteuse (Carrier Sense) et détection de collision.
- ✓ Toute station souhaitant émettre se charge de contrôler que rien ne circule sur le réseau.
- ✓ Autrement, elle attend que ce dernier soit libre de tout trafic. La vitesse de ce réseau est de 10 MBPS.

Le Réseau Token Ring (Anneau à jeton)

- ✓ Token Ring est né dans les années 1970 sous l'impulsion d'IBM. Bien que les réseaux locaux d'aujourd'hui utilisent de plus en plus la technologie Ethernet, il reste utilisé.
- ✓ Il s'agit d'un réseau local utilisant la technologie Token Ring dont le principe repose sur le fait de disposer les machines en anneau, en les dotant chacune d'une interface avec un canal entrant et sortant, et en utilisant le mode d'accès par jeton.

- ✓ Ce jeton circule autour de l'anneau.
- ✓ La station qui a le jeton émet des données qui font le tour de l'anneau.
- ✓ À leur retour, les données sont éliminées par la station qui les a envoyées.
- ✓ Un réseau local Token Ring ne doit avoir qu'une longueur très limitée, afin de réduire le délai de propagation sur l'ensemble de l'anneau.

3.5 Conclusion

Ce chapitre a été axé sur la présentation des médias de transmission utilisés pour relier les réseaux, ainsi que les équipements réseau pour les interconnecter. En outre, nous avons mis l'accent sur les différents réseaux locaux.

Le chapitre suivant sera consacré sur l'étude détaillée de la couche physique en examinant les principales techniques utilisées pour transférer les informations, de codage et de modulation.

Chapitre 4

Transmission physique de l'information

4.1 Introduction

Les réseaux de communication assurent le transfert d'informations d'un système source vers un système de destination. Les informations sont véhiculées sur les supports de communication sous forme de signaux. Les informations échangées sont généralement sous forme texte, image fixe, son, images animées et données informatiques. Cependant, il faut trouver une bonne transformation de l'information de signal de sorte que le média de communication soit capable de le propager correctement. Par conséquent, les informations échangées sont codées sous une forme *binnaire*, donc le système utilisé est le *système binnaire*. Aussi, pour garantir le succès des communications, la source et la destination doivent utiliser une méthode de transmission des données convenue mutuellement.

Dans ce chapitre, nous allons présenter les principales techniques utilisées pour transférer les informations dans un réseau de communication. Pour ce faire, nous allons dresser un aperçu général sur la nature du signal avant de passer en revue les techniques de codage et de modulation et les différents phénomènes susceptibles de l'affecter.

4.2 Principe de la transmission

Un signal correspond à la variation d'une grandeur physique en fonction du temps afin de représenter physiquement l'information. Cette variation peut être continue ou discrète. Ainsi, deux types de signaux sont utilisés pour la transmission de l'information sous forme de bits:

- **Signal numérique (Digital)**
- **Signal Analogique.**

✓ **Signal numérique**

- Un signal **Discret**.
- Nombre d'états fini.

- Affaiblissement.
- Courte distance.
- Adapté aux réseaux LANs (transmission en bande de base).

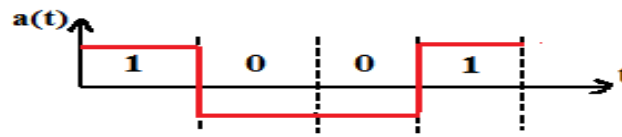


Figure 4.1 Signal numérique

✓ Signal analogique

- Un signal Continu (nombre d'état infini).
- Moins sensible au problème d'affaiblissement.
- Longue distance
- Adapté aux réseaux WANs (transmission en large bande).

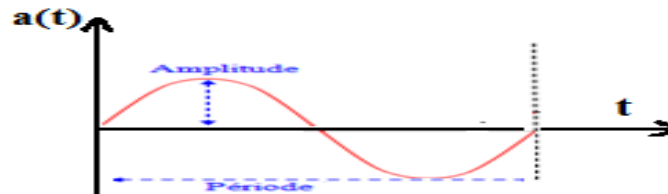


Figure 4.2 Signal analogique

$$a(t) = A \sin(wt + \varphi)$$

$a(t)$: amplitude en fonction de temps. A : amplitude max. $w=2\pi f$ (pulsion).

f : fréquence en Hz. (Fréquence : nombre de période par seconde).

φ : décalage par rapport à l'origine.

t : temps en seconde.

4.3 Transformations sur les signaux

La transmission physique de l'information (figure ci-dessous 4.3) comporte le transcodage et/ou la modulation de signaux électriques pour obtenir des signaux adaptés aux caractéristiques des supports de transmission.

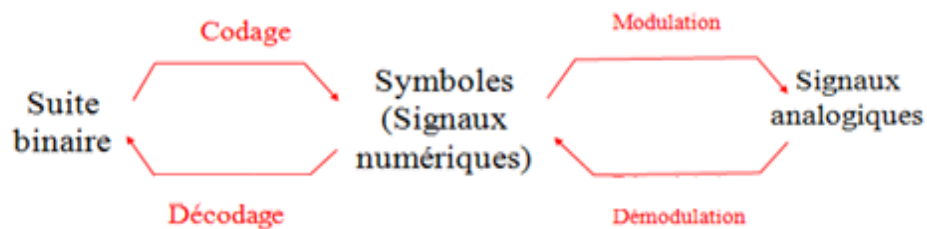


Figure 4.3 Schéma d'un système de transmission

Le composant qui adaptera le signal numérique en fonction des caractéristiques du support ou du réseau (il peut être le modem ou un autre équipement) est appelé *Équipement Terminal de Circuit de Données* (ETCD).

On désigne généralement sous le nom de *circuit de données* (voir la figure 4.4) l'ensemble constitué par le support et les ETCDs utilisés pour adapter le signal transmettant ses informations. Par conséquent, à travers un circuit de données, la transformation du signal est totalement intégrée.

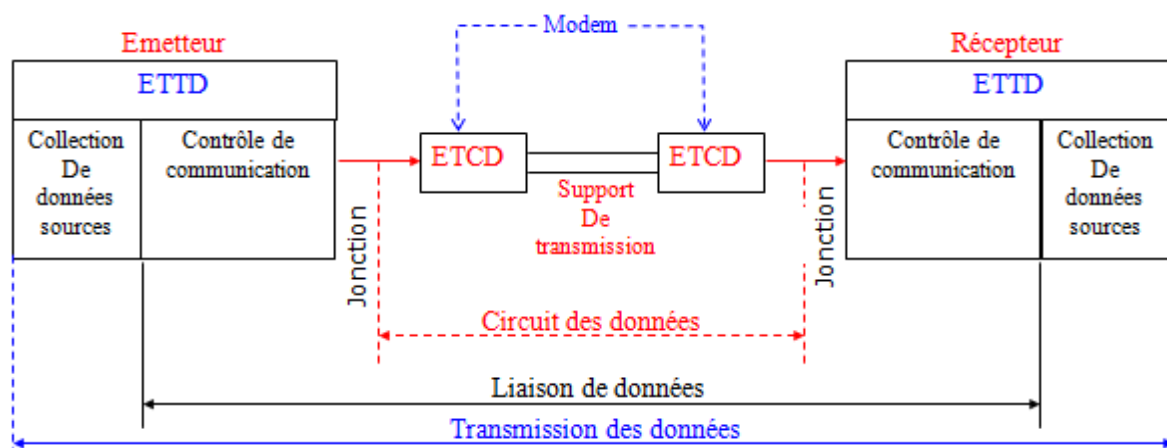


Figure 4.4 Circuit de données

ETTD : Equipement Terminal de Traitement de Donnée
ETCD : Equipement Terminal de Communication de Donnée
Jonction : interface ETTD _ ETCD

On peut résumer les caractéristiques essentielles des systèmes de transmission dans les points suivants:

- ✓ **Type de liaison**
- ✓ **Direction du flux des signaux**
- ✓ **Mode de liaison**
- ✓ **Modes de synchronisation des signaux**
- ✓ **Méthode de transmission**

4.3.1 Type de liaison

La communication des informations (suite de bits) comprend l'envoi de plusieurs bits organisés en mots. Ces bits peuvent être envoyés en mode série ou en mode parallèle.

- a. **Liaison série** : consiste à la transmission bit par bit les uns derrières les autres sur une même ligne (un seul fil) comme illustré sur la figure 4.5.



Figure 4.5 Liaison série

- b. **Liaison parallèle** : consiste à la transmission des bits d'un même mot en même temps sur plusieurs lings (plusieurs fils).

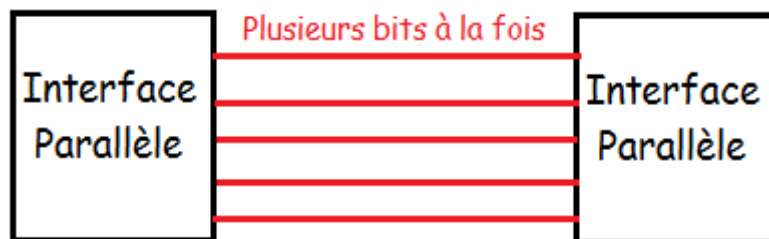


Figure 4.6 Liaison parallèle

4.3.2 Type de communication de la liaison

Les échanges d'informations entre deux systèmes de communication peuvent être organisés selon plusieurs modes : simplex, half-duplex et full-duplex.

- a. **Simplex** : un canal simplex est **unidirectionnel**. Il permet aux données de circuler dans une seule direction, comme le montre la figure 4.7 ci-dessous.

Exemple : radio / télévision

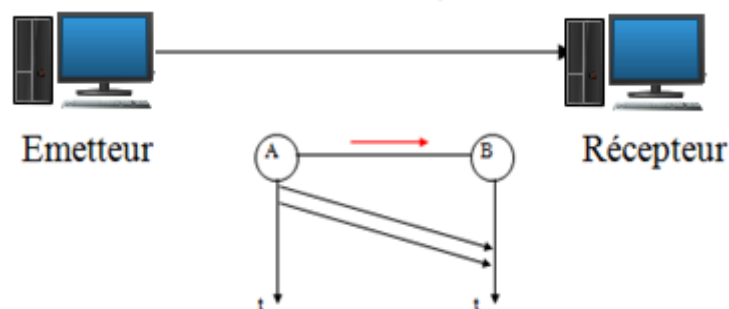


Figure 4.7 Mode simplex

- b. Half Duplex** : La transmission half-duplex nous permet d'assurer une communication simplex dans les deux directions sur un seul canal (directionnelle à l'alternat) ;

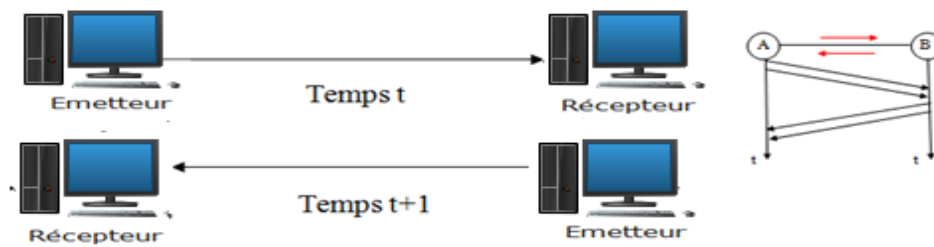


Figure 4.8 Mode duplex

- c. Full Duplex** : c'est une communication simultanément en deux sens (directionnelle) (voir figure 4.8);

Exemple : téléphone

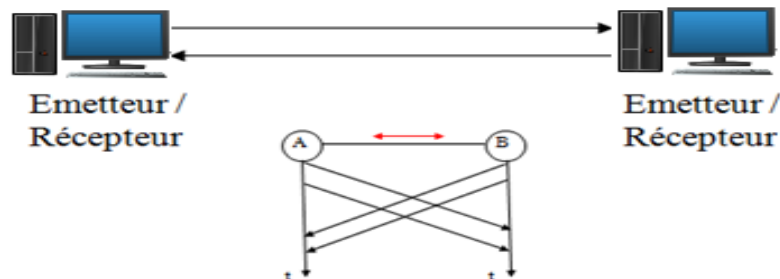


Figure 4.9 Mode full duplex

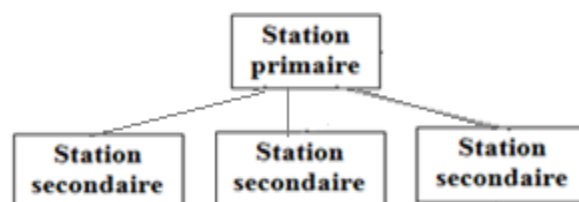
4.3.3 Mode de liaison

- a. Liaison point à point**: les différents équipements sont reliés en couples avec des liens dédiés ; Exemple : le lien entre un ordinateur et un terminal

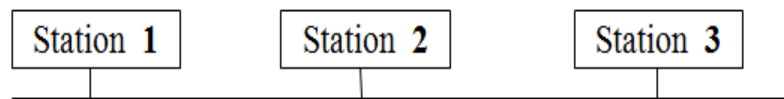


- b. Liaison Multipoint (à diffusion)**: Le support est partagé par plusieurs nœuds, auquel le contrôle d'accès devient indispensable pour éviter les problèmes relatifs aux droits d'accès. Deux modes de contrôle d'accès sont disponibles :

- Mode maître/esclave



○ Mode égal à égal (P2P)



4.3.4 Les modes de synchronisation des signaux

La synchronisation entre l'émetteur et le récepteur permet la délimitation des données (les bits, les caractères, les blocs de données). Il existe 3 types de méthodes de synchronisation.

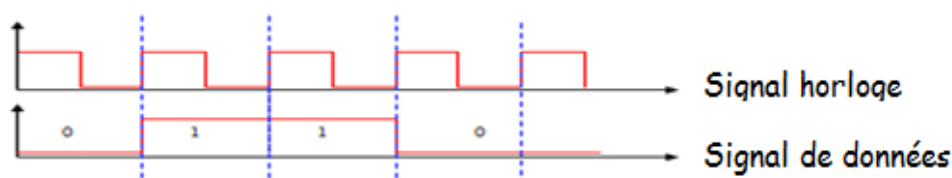
- a. **La transmission asynchrone:** La source produit des caractères à des instants aléatoires (Exemple : frappe des caractères sur le clavier). Chaque caractère émis est précédé d'un moment élémentaire appelé bit start et suivi par un moment élémentaire de fin appelé bit stop.

Exemple



- b. **La transmission synchrone par fil:** Un fil particulier appelé fil de synchronisation relie les deux horloges des deux équipements communicants et on aura la transmission des différents bits les uns à la suite des autres à chaque période d'horloge.

Exemple



- c. **La transmission synchrone par déduction:** La séquence de synchronisation est déduite du flux binaire reçu, permettant ainsi de synchroniser la totalité des données

Exemple

Synchronisation 1 0	Commande 1 0	Données >= 0 0	FCS 2 0	Synchronisation 1 0
------------------------	-----------------	-------------------	------------	------------------------

4.3.5 Les méthodes de transmission

Il y a deux méthodes de transmission : La transmission en bande de base et la transmission à large bande.

a. La transmission en bande de base

Elle consiste à transmettre l'information sous sa forme **numérique** (figure 4.9). Compte tenu du phénomène d'affaiblissement des signaux numériques (avec la distance). Avec ce mode, le délai de transmission est limité à une distance maximale théorique de 50 km (en pratique 30 km). Pour les réseaux locaux, cette technique est la plus répandue. L'idée de base de cette méthode repose sur le **codage en bande de base** en transformant **une séquence binaire** en **une séquence numérique**, afin d'adapter le signal sur le support. L'opération inverse est appelée **décodage**. L'équipement qui se charge de cette opération est appelée **ERBDB** (Emetteur Récepteur en Bande De Base).

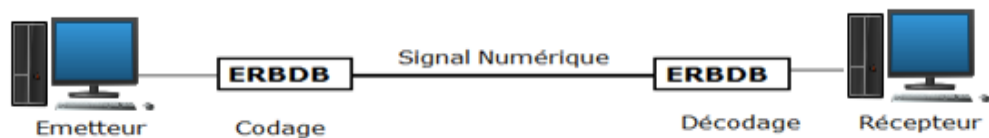


Figure 4.9 Le codage (Transmission en bande de base)

b. La transmission en large bande

Elle se base sur la **transformation** des **signaux numériques** en **signaux analogiques** pouvant être transmis sur une longue distance (figure 4.10). L'opération de base de cette technique est appelée **Modulation**. L'opération inverse est **la Démodulation**. L'équipement qui se charge de cette opération est le **Modem**. Cette méthode est adaptée aux réseaux WANs qui s'étendent sur des longues distances.



Figure 4.10 La modulation (Transmission large bande)

4.4 Le Codage des signaux

Le **codage** permet de transformer **une séquence binaire** (bits) en une séquence de symboles codés (**signaux numériques**) ; le plus souvent binaires ou ternaires (trois niveaux). Quant au **décodeur**, il effectue l'opération inverse. Le **but du codage** est **d'adapter les bits** à transmettre **aux spécificités** du mode de transmission.

Les Codes usuels en bande de base:

1. Les codes à deux niveaux	2. Les codes à trois niveaux	3. Les codes en Blocs
<ul style="list-style-type: none"> - NRZ - NRZI - Biphase Manchester - Biphase Différentiel - Miller 	<ul style="list-style-type: none"> - RZ - Bipolaire - Bipolaire d'ordre 2 	<ul style="list-style-type: none"> -nB / mB -nB / mT

Exemple : Comme illustré sur la figure 4.11, on va coder la suite suivante 11000101 avec les codages Biphase Manchester, Biphase différentiel, RZ et bipolaire.

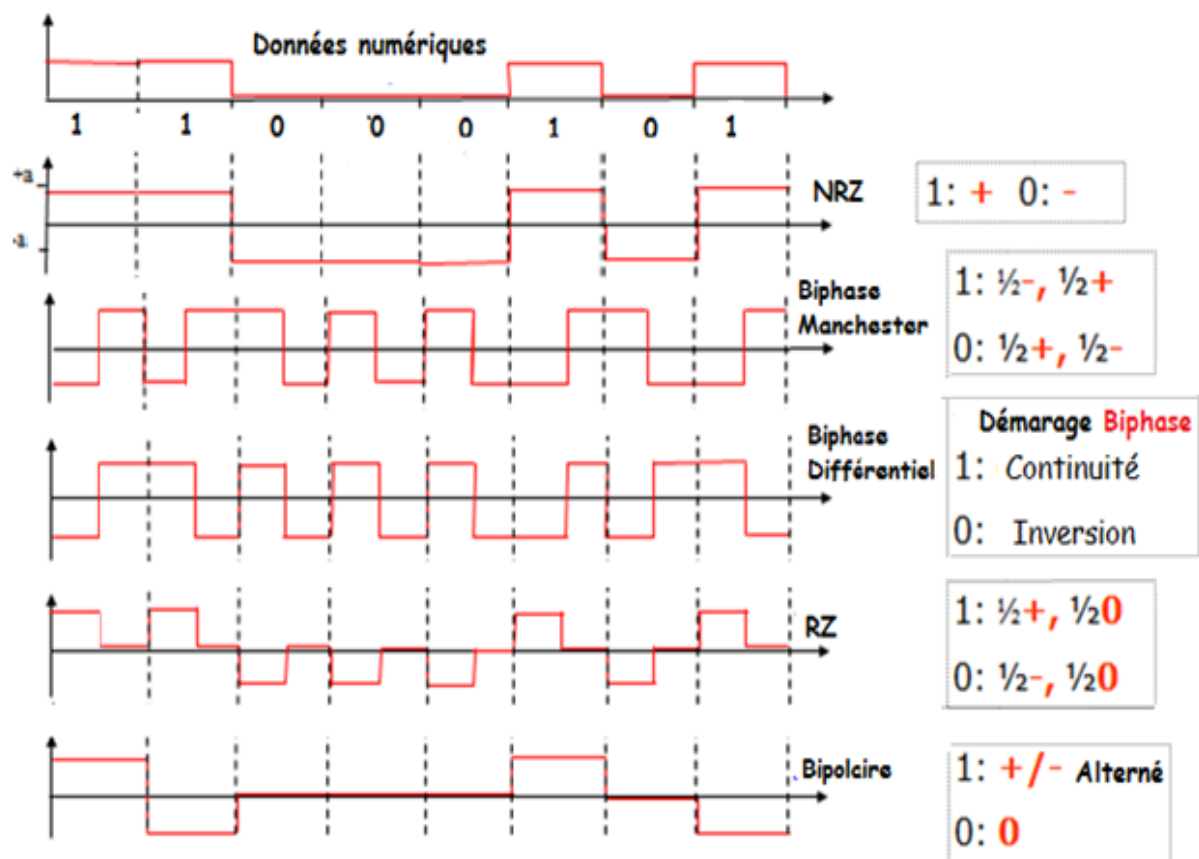


Figure 4.11 Exemples de codage

4.5 La Modulation des signaux

La modulation consiste à transformer les **signaux numériques** en **signaux analogique**. Le principe général consiste à modifier l'un des paramètres d'un signal de base (appelé la porteuse). Ce dernier est un signal sinusoïdal de la forme : $S(t) = A_0 \sin(\omega_0 t + \phi_0)$. C'est une opération réalisée par un **modem**. Il existe **3** techniques de modulation.

- a. **La modulation de fréquence** : consiste à utiliser deux fréquences différentes une pour représenter " 1 " l'autre pour représenter " 0 "

Exemple : Sur la figure 4.12, la modulation du signal 0110.

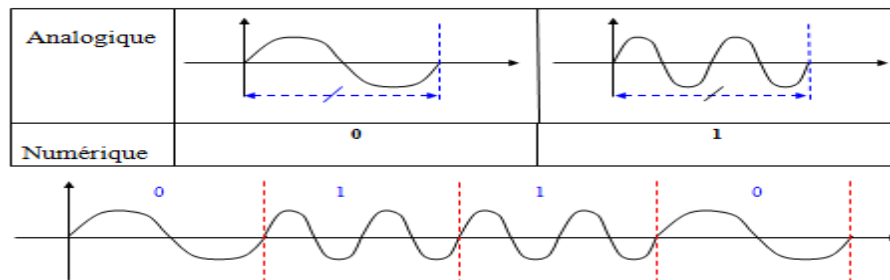


Figure 4.12 Modulation de fréquence

- b. **La modulation d'amplitude**: consiste à utiliser deux amplitudes une pour " 1 " et l'autre pour " 0 ".

Exemple : On peut voir sur la figure 4.13 la modulation du signal 10011.

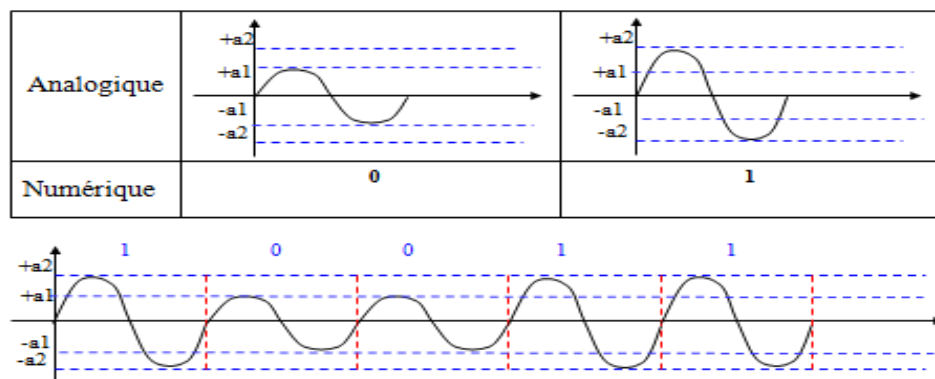


Figure 4.13 La modulation d'amplitude

- c. **La modulation de phase** : consiste à utiliser deux phases, une pour " 1 " et l'autre pour " 0 "

Exemple : sur la figure 4.14 la modulation du signal 10011.

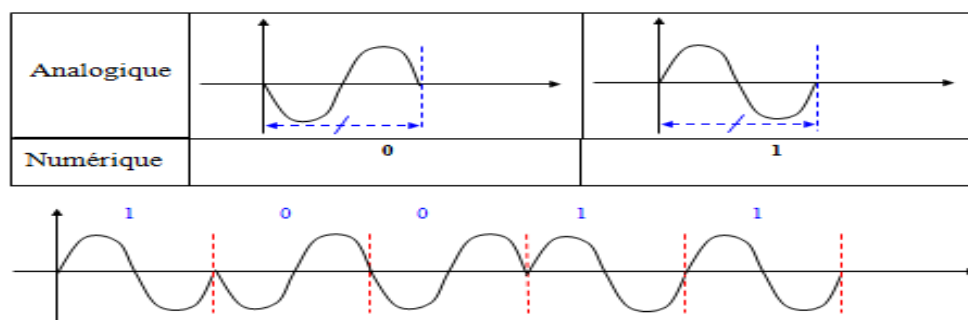


Figure 4.14 La modulation de phase

4.6 Le Multiplexage

Il s'agit de partager un canal entre plusieurs lignes. Si plusieurs voies de données sont requises entre deux sites, il est plus économique d'utiliser **une seule ligne partagée** qui permettra de transmettre tous les messages des différents équipements plutôt que d'utiliser plusieurs lignes point à point. Deux techniques de multiplexage peuvent être distinguées : **le multiplexage fréquentiel** et **le multiplexage temporel**.

a. Le multiplexage fréquentiel (FDM : Frequency Division Multiplexing)

Cette technique revient à diviser la bande passante en sous-bandes (canaux) qui seront exploitées simultanément. En d'autres termes, l'échange d'informations s'effectue simultanément entre les équipements car chaque sous-bande est attribuée à un canal afin d'éviter le problème des interférences (figure 4.15). Elle est essentiellement utilisée dans la transmission analogique.

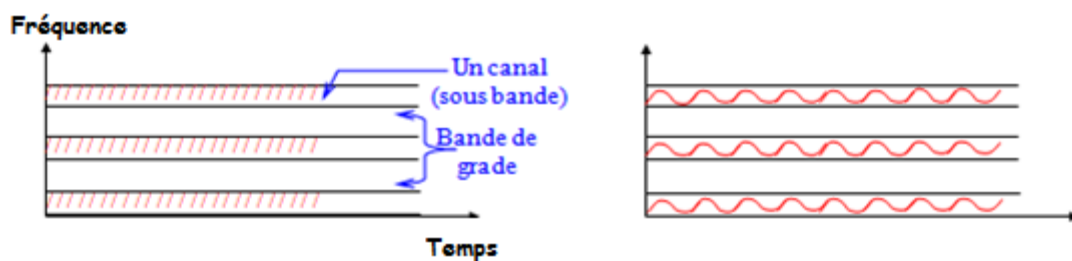


Figure 4.15 Le multiplexage fréquentiel

b. Le multiplexage temporel (TDM : Time Division Multiplexing)

Il consiste à répartir dans le temps le canal entre plusieurs transmissions, et à chaque transmission est attribué un intervalle de temps appelé IT : (Interval Time) (figure 4.16). Il est principalement utilisé dans les transmissions numériques.

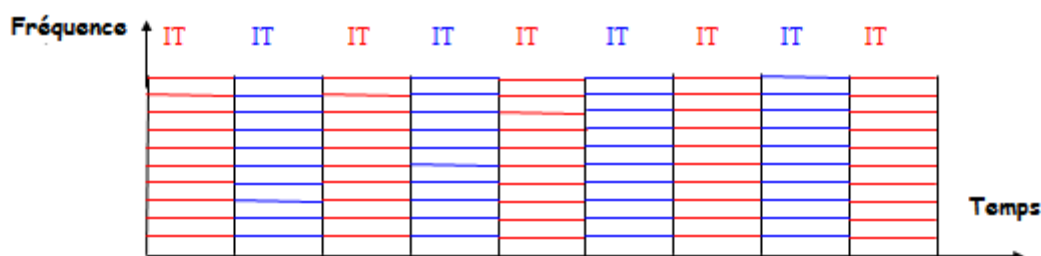


Figure 4.16 Le multiplexage temporel

4.7 Les phénomènes caractérisant les supports de transmission

a. L'atténuation : transformation de l'amplitude du signal qui varie en fonction de la fréquence. L'atténuation du signal est mesurée en termes de perte de signal par unité de longueur du câble, généralement en dB/km. Lorsque le signal se propage sur un canal de communication, son amplitude diminue car le support physique résiste au flux d'énergie électromagnétique. Ainsi, la résistance de certains matériaux des conducteurs fait qu'une partie de l'énergie électrique du signal est convertie en énergie thermique lors de la progression du signal le long du câble, ce qui entraîne une diminution continue du signal électrique.

b. Le déphasage : déformation de la phase du signal. Au fait, la quantité d'informations qu'un canal peut transmettre sur une période donnée est déterminée par sa capacité à gérer le taux de changement du signal, c'est-à-dire sa fréquence.

c. Les bruits ou phénomènes de perturbation : Le bruit est un signal perturbateur, ayant une nature aléatoire, qui s'ajoute au signal et provoque des anomalies et des erreurs de transmission. Le bruit peut provenir

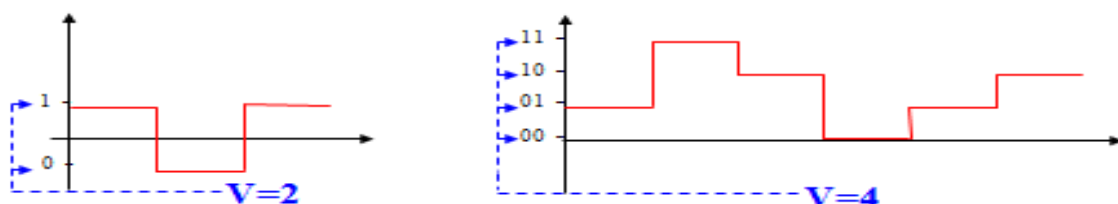
- du support lui-même, il est alors appelé **bruit blanc** qui se résume en agitation thermique (chaleur).
- de l'environnement du support, et est appelé **bruit impulsif** qui est dû à des organes électromécaniques

Il existe aussi d'autres types de bruit comme :

- **diaphonie** : couplage parasite entre lignes voisines.
- **écho** : réflexion du signal.

4.8 Les Grandeurs de transmission

- **Le moment élémentaire** : Laps de temps relatif à une représentation binaire (en **seconde**).
- **La Rapidité (vitesse) de modulation** : c'est le nombre de moments élémentaires par second. Elle se mesure en **bauds**.
- **La Valence** : c'est le nombre d'états significatifs (voir la figure ci-dessous.)



- **La Bande passante** : C'est une caractéristique de la voie de transmission. Elle représente les fréquences supportées, l'unité de mesure est le **Hertz (Hz)**, calculée selon la formule suivante :

$$B = F_{\max} - F_{\min}$$

Remarque

$$\begin{aligned} 1 \text{ KHz} &= 10^3 \text{ Hz} \\ 1 \text{ MHz} &= 10^6 \text{ Hz} \\ 1 \text{ GHz} &= 10^9 \text{ Hz} \end{aligned}$$

- **Le Débit binaire** (vitesse de transmission) : C'est le nombre de bits transmis par seconde. L'unité de mesure est le **bps (b/s)**.

Remarque

$$\begin{aligned} 1 \text{ Kb/s} &= 10^3 \text{ b/s} \\ 1 \text{ Mb/s} &= 10^6 \text{ b/s} \\ 1 \text{ Gb/s} &= 10^9 \text{ b/s} \end{aligned}$$

- **Relation de Nyquist** : C'est une relation qui ne tient pas compte du bruit sur la ligne donnée par la formule ci-dessous :

$$\begin{aligned} D &= R * \log_2 (v) \\ R &= 2 * B \end{aligned}$$

- D : Débit (b/s)
- R : Rapidité de modulation (baude)
- B : Bande passante (Hz)
- V : Valence

Théorème de Shannon : C'est une relation de maximisation qui tient compte du bruit sur la ligne obtenue comme suit:

$$D = B * \log_2 (1 + \frac{S}{N})$$

- D : Débit (b/s),
- B : Bande passante (Hz)
- S/N : rapport signal sur bruit (en valeur).

Remarque : S/N est le rapport du signal sur bruit qui se mesure en décibels (**dB**) mais dans la relation de Shannon il est utilisé en valeur. La relation entre les 2 est la suivante:

$$\frac{S}{N}_{\text{dB}} = 10 \text{ Log}_{10} (S/N)_{\text{(valeur)}}$$

- **Temps de Transfert (Tr)**: temps nécessaire pour que le message émis à travers le réseau soit reçu complètement par l'équipement récepteur calculé comme suit :

$$Tr = Tt + Tp$$

- Tr: Temps de transfert (s)
- Tt: Temps de transmission (s)
- Tp: Temps de propagation (s)

- **Temps de propagation (T_p)**: c'est le temps nécessaire pour que le signal parcourt le support d'un point à l'autre de la liaison. Il dépend de plusieurs paramètres (Nature du support, Distance, Fréquence du signal). Il est calculé selon la formule suivante :

$$T_p = L / V_p$$

- T_p : Temps de propagation (s).
- L : Distance (m).
- V_p : Vitesse de propagation (m/s).

Remarque: le T_p est souvent négligeable sur liaison terrestre. Par contre, il peut devenir important pour les liaisons satellitaires.

- **Temps de transmission (T_t)**: c'est le temps nécessaire pour que le message soit envoyé totalement sur la ligne. Il dépend du débit du canal et il est obtenu comme suit :

$$T_t = \text{Taille} / D$$

- T_t : Temps de transmission (s)
- Taille: Taille du message (bits)
- D : Débit (b/s)

4.9 Conclusion

Dans ce chapitre, nous avons présenté la couche physique en détaillant ses différents principes de communication et les grandes lignes directrices en matière de transmission du signal. Nous avons également passé en revue les différentes méthodes permettant le codage et la modulation du signal ainsi que les différents phénomènes susceptibles de l'affecter.

Le chapitre suivant fera l'objet d'une étude approfondie de la couche liaison de données où nous aborderons les principales techniques utilisées pour transférer et contrôler les informations dans un réseau de communication, ainsi que les corriger en cas d'erreur.

Chapitre 5

Fiabilisation de la transmission

5.1 Introduction

Les circuits de communication de données sont souvent soumis au bruit et différents phénomènes, en particulier lorsque les équipements sont situés dans un environnement industriel où les nuisances électriques sont élevées. Par exemple, le rayonnement électromagnétique émanant des équipements adjacents ou l'induction émise par les câbles. Par conséquent, les données reçues de la couche physique peuvent contenir des erreurs, ce qui rend le processus de transmission peu fiable. Or, pour assurer une communication fiable des données, il faut vérifier l'exactitude de chaque message de données.

Ce chapitre sera consacré à l'étude détaillée de la couche liaison de données, avec un focus sur les différents mécanismes et techniques de détection des erreurs et celles utilisées pour leur correction. Par ailleurs, les méthodes de transmission propres à cette couche seront également présentées, en mettant l'accent sur le protocole HDLC.

5.2 Mécanismes de détection et de correction d'erreurs

Les phénomènes perturbateurs peuvent entraîner des erreurs de transmission en inversant les bits de l'information transmise. Une liaison est caractérisée par son taux d'erreurs T_e appelé aussi **BER (Bit Error Rate)** donné comme suit :

$$T_e = \frac{\text{nombre bits erronés}}{\text{nombre bits total}}$$

Exemple

Info :transmise : 1110001100111100

Info. reçue : 1110101100101100

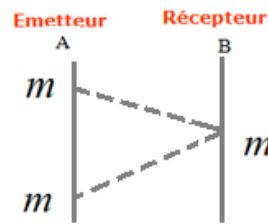


$$T_e = 2/16 = 12.5\%$$

T_e varie pratiquement entre 10^{-4} et 10^{-9} . Au fait, plusieurs mécanismes sont utilisés pour détecter et éventuellement corriger les erreurs de transmission à savoir la détection par echo, par répétition, par code de parité, CRC et Hamming.

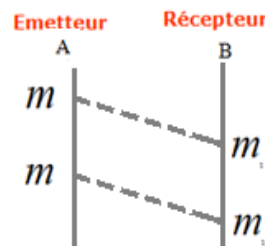
- ✓ **La détection par écho** : le récepteur renvoie le message reçu. Si le message est différent de celui émis alors il y a erreur et le message doit être retransmis.

Si $m = m_1$ Alors
 Pas d'erreur
 Sinon
 Erreur
 Retransmission
 Fin Si



- ✓ **La détection par répétition** : chaque message émis est suivi par sa réplique. Si les deux messages sont différents, le récepteur demande une retransmission.

Si $m_1 = m_2$ Alors
 Pas d'erreur
 Sinon
 Erreur
 Demande de retransmission
 Fin Si



- ✓ **La détection d'erreurs par code** : consiste à ajouter à l'information initiale une information supplémentaire qui permet de détecter l'erreur. Exemples : **parité**, **CRC**.
- ✓ **La détection et la correction d'erreurs par code** : utilisation des codes auto correcteurs. Exemple : **Hamming**.

Dans ce qui suit, les détails des trois méthodes de détection par parité, par CRC et l'auto-correcteur de Hamming et par retransmission seront présentés.

5.2.1 Détection d'erreurs par parité

Cette technique utilise une redondance de un bit par caractère. On peut distinguer deux sortes de parité :

- **Parité paire** : rendre le nombre des 1 paire

Exemple :

1	0	1	1	0	1	1	1
0	1	0	0	1	0	0	0

- **Parité impaire** : rendre le nombre des 1 impaire

Exemple :

1	1	0	1	1	1	0	0
0	0	1	1	0	0	0	1

Utilisation de la parité: Dans le cas de la **transmission asynchrone**, la parité utilisée est appelée

VRC. Mais dans le cas des **transmissions synchrones** le VRC ne suffit pas, il est complété par le **LRC**. Sachant que :

VRC : Vertical Redundancy Check (vérification par redondance verticale).

LRC : Longitudinal Redundancy Check (vérification par redondance Longitudinale).

La Forme d'un message est :

Caractère transmis	VRC	Caractère transmis	VRC	LRC	VRC
---------------------------	------------	---------------------------	------------	-------	------------	------------

Exemple: Soit à transmettre le mot HELLO en mode synchrone (parité paire).

	H	E	L	L	O	LRC
Bit7	1	1	1	1	1	1
Bit6	0	0	0	0	0	0
Bit5	0	0	0	0	0	0
Bit4	1	0	1	1	1	0
Bit3	0	1	1	1	1	0
Bit2	0	0	0	0	1	1
Bit1	0	1	0	0	1	0
VRC	0	1	1	1	1	0

La suite à transmettre est : 10010000**1**0001011100110011001100110011111**10000100**

5.2.2 La détection d'erreurs par CRC (Cyclic Redundancy Check)

CRC ou **vérification par redondance cyclique** permet de détecter les erreurs avec une très grande précision dans des messages de toute longueur. Pour ce faire il utilise un polynôme commun entre *émetteur /récepteur* appelé **polynôme générateur**.

La forme de base utilisée est la forme polynomiale mais afin de faciliter les calculs on peut passer à une forme binaire.

Informations de base :

- **G(x)** : polynôme générateur de degré r . Exemple : $G(x) = x^2 + 1 \rightarrow G = 101$
- **M(x)** : message à transmettre
- **M'(x)** : message réellement transmis (après application du CRC)

Méthode appliquée à l'émission:

Multiplication

$x^r * M(x) \rightarrow$ Ajout de r zéros à la fin de **M**

Calcul du reste

$R(x) = \text{Reste } (x^r * M(x) / G(x)) \rightarrow$ Division modulo 2
- **R** sur r bits

Soustraction

$M'(x) = x^r * M(x) - R(x) \rightarrow$ Ajout des r bits de **R** à la fin de **M**
pour avoir **M'**

Méthode appliquée à la réception**Division****M' (x) / G(x) -> M' / G (Division module 2)****Si reste = 0 Alors**

Transmission sans erreur

Sinon

Erreur de transmission

Fin si**Remarque**

La division modulo 2 est basée sur la soustraction modulo 2.

Le principe de la soustraction modulo 2 est le suivant:

$$\begin{array}{r} 0011 \\ 0101 \\ \hline 0110 \end{array}$$
Exemple 1

Soit à transmettre la suite $F = 101100111010001$, la méthode utilisée est le CRC avec le polynôme générateur $G(x) = x^6 + x^4 + x + 1$.

Quelle est la suite réellement transmise?

Solution: (application de la méthode à l'émission) $F = 101100111010001 \rightarrow$ information initiale $G(x) = x^6 + x^4 + x + 1 \rightarrow G = 1010011$ Multiplication: 101100111010001000000 Division : pour avoir le reste R (sur $r=6$ bits)

$$\begin{array}{r}
 101100111010001000000 \\
 \underline{1010011} \\
 0001010110 \\
 \underline{1010011} \\
 00001011000 \\
 \underline{1010011} \\
 0001011100 \\
 \underline{1010011} \\
 0001111000 \\
 \underline{1010011} \\
 01010110 \\
 \underline{1010011} \\
 0000101 \rightarrow R
 \end{array}
 \quad
 \begin{array}{l}
 1010011 \\
 \hline
 \end{array}$$

La suite réellement transmise est: $F' = 101100111010001000101$

Exemple 2

On suppose la réception de la suite binaire suivante: 1011001110010100 et que la méthode utilisée est CRC avec le même polynôme générateur précédant. Est-ce que la transmission de la suite est faite sans erreurs?

Solution: (Application de la méthode lors de la réception)

$F' = 1011001110010100 \rightarrow$ information Reçue

$G(x) = x^6 + x^4 + x + 1 \rightarrow G = 1010011$

Division :

1011001110010100	1010011
<u>1010011</u>	
0001010110	
<u>1010011</u>	
00001010101	
<u>1010011</u>	
000011000	

Reste (F'/G) $\neq 0$ alors Erreur de transmission

Remarques

- En cas de transmission sans erreurs l'information initiale est obtenue au niveau du récepteur en enlevant les r bits situés à droite de la suite reçue.
- Les bits ajoutés associés à R sont appelés bits de redondance et R représente une information redondante.

Les polynômes générateurs les plus utilisés sont :

- CRC – 12 : $x^{12} + x^{11} + x^3 + x^2 + 1$
- CRC – 16 : $x^{16} + x^{15} + x^2 + 1$
- CRC – CCITT : $x^{16} + x^{12} + x^5 + 1$

5.2.3 Codes auto-correcteurs : Le code de Hamming

Distance de Hamming : La distance de Hamming entre deux séquences binaires de même taille est égale au nombre de bits de même rang qui les différencient.

Exemple : $d(1100110, 1010110) = 2$

- Soit un code composé de N mots valides.
- La distance de Hamming de ce code est définie comme la distance minimale qui sépare deux mots valides du code.
- Exemple : le code : $C = [000000, 001110, 010101, 011011, 100011, 101101]$ a une distance de Hamming = 3
- Un code avec une distance d détecte $d-1$ erreurs et corrige k erreurs où $d=2K+1$

Structure d'un mode de code de Hamming

- les **m** bits du message à transmettre et les **n** bits de contrôle de parité.
 - longueur totale : $2^n - 1$
 - longueur du messages : $m = (2^n - 1) - n$
- on parle de code $x - y$ où $x = n + m$ et $y = m$.

Exemple

- un mot de code 7-4 a un coefficient d'efficacité de $4/7 = 57\%$,
- un mot de code 15-11 a un coefficient d'efficacité de $11/15 = 73\%$,
- un mot de code 31-26 a un coefficient d'efficacité de $26/31 = 83\%$,
- Les bits de contrôle de parité C_i sont en position 2^i pour $i=0,1,2,\dots$ (**puissance de 2**)
- Les bits du message D_j occupe le reste du message.

D3	D2	D1	C2	D0	C1	C0
7	6	5	4	3	2	1

Retrouver l'erreur dans un mot de Hamming

- Si les bits de contrôle de réception $C'_2 C'_1 C'_0$ **de somme de 0** (parité paire); **pas d'erreurs** sinon la valeur des bits de contrôle indique la position de l'erreur entre 1 et 7

- Si C'_0 vaut 1, les valeurs possibles de $C'_2 C'_1 C'_0$ sont 001, 011, 101, 111, c'est-à-dire 1, 3, 5, 7.
- Si C'_1 vaut 1, les valeurs possibles de $C'_2 C'_1 C'_0$ sont 010, 011, 110, 111, c'est-à-dire 2, 3, 6, 7.
- Si C'_2 vaut 1, les valeurs possibles de $C'_2 C'_1 C'_0$ sont 100, 101, 110, 111, c'est-à-dire 4, 5, 6, 7.

→ **Il s'agit des positions possibles pour une erreur**

Émission pour un contrôle de parité paire

C_0 est calculé par rapport aux bits d'indice 7, 5, 3 et sa valeur 1.

C_1 est calculé par rapport aux bits d'indice 7, 6, 3 et sa valeur 2.

C_2 est calculé par rapport aux bits d'indice 7, 6, 5 et sa valeur 4.

On souhaite envoyer le message 1010, compléter le mot de Hamming correspondant

1	0	1	—	0	—	—
7	6	5	4	3	2	1

- C_2 vaut 0 pour pouvoir rendre pair $1 + 0 + 1$ (les bits d'indices 7, 6, 5)

1	0	1	0	0	—	—
7	6	5	4	3	2	1

- C1 vaut 1 pour pouvoir rendre pair $1 + 0 + 0$ (les bits d'indices 7, 6, 3)

1	0	1	0	0	1	—
7	6	5	4	3	2	1

- C0 vaut 0 pour pouvoir rendre pair $1 + 1 + 0$ (les bits d'indice 7, 5, 3)

1	0	1	0	0	1	0
7	6	5	4	3	2	1

5.2.4 Les mécanismes de correction par retransmission

Afin de contrôler les erreurs et d'assurer une transmission fiable, plusieurs techniques peuvent être utilisées, comme nous l'avons vu jusqu'à présent :

- ✓ Les méthodes de correction : rarement utilisées comme Hamming
- ✓ Méthodes de détection : Largement utilisées comme les méthodes VRC, LRC, CRC. Il faut noter Mais elles sont complétées par des méthodes appelées de **retransmission**.

Dans le reste de ce paragraphe, on va détailler ces méthodes de retransmission.

1. Les méthodes de retransmission automatique (ARQ : Automatic Repeat ReQuest)

Il existe deux grandes classes de méthodes ARQ :

- Envoyer et attendre : Send & Wait ARQ (ou bien Stop & wait).
- Continuous ARQ.

a. Send & Wait ARQ: Il s'agit d'envoyer une trame à la fois et d'attendre son accusé de réception. Il est soit positif (Ack) s'il n'y a pas d'erreur, soit négatif (Nack) dans le cas contraire (figure 5.1). **Ack:** accusé de bonne réception **Nack:** accusé de mauvaise réception

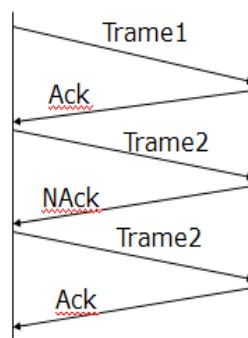


Figure 5.1 Send & Wait

b. Continuous ARQ: Consiste à la transmission de plusieurs trames avant d'attendre leurs acquittements. Deux méthodes sont disponibles:

- **Systématique:** se base sur la retransmission de toutes les trames à partir de la dernière erronée.
- **Sélective:** consiste à la retransmission de la trame erronée seulement.

b.1 Méthode du rejet Systématique (Go Back N)

- Transmission de N trames avant d'attendre leurs acquittements.
- A la réception d'un NACK ou à l'expiration du time-out d'une trame, la transmission est reprise depuis la trame en question afin de garder le séquençement des trames.

Inconvénient : élimination des trames bien reçues hors séquençement.

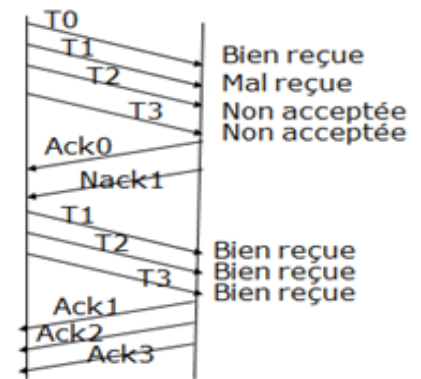


Figure 5.2 Rejet systématique

Remarque: Une amélioration du principe précédent consiste à utiliser la notion d'**acquiescement groupé** (HDLC par exemple).

b.2 Méthode du rejet Sélectif (Selective reject)

- Seules les trames erronées ou perdues sont retransmises individuellement.
- **Contrainte :** Mémorisation de Toutes les trames reçues hors Séquençement et ré-ordonnancement après la Réception des trames Retransmises.
- **Solution:** Nécessité d'avoir des mémoires tampon (buffers).

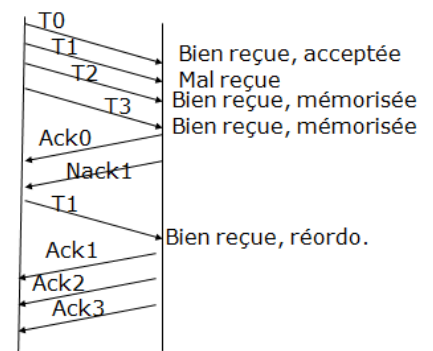


Figure 5.3 Rejet Sélectif

5.3 Le protocole de liaison de données HDLC (HDLC: High Data Level Control)

HDLC est un protocole de haut niveau qui est destiné à la gestion des liaisons de données. Il apporte une amélioration aux protocoles basés sur la transmission synchrone, qui consistent à envoyer un message et à attendre un accusé de réception, et ce en procédant à une retransmission par anticipation. Il utilise 3 types de trames :

- Les trames d'information (I)
- Les trames de supervision (S)
- Les trames non numérotées (U)

- **Les trames d'information :** S'écrivent de la façon suivante: $I N(S), N(R), P/F$ Avec

- N(S) : Numéro de la trame
- N(R) : Numéro de la trame attendue
- P : Commande F: Réponse

Exemple: I_{4,2,P}

- **Les trames de supervision** : S'écrivent de la façon suivante:

$S_{N(R), P/F}$

Il existe quatre types de trame S:

- RR : Received & Ready
- RNR : Received & Not Ready
- REJ : Reject (systématique)
- SREJ: Selective reject (sélective)

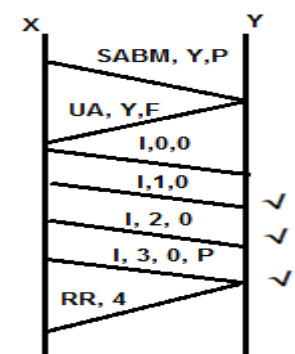
- **Les trames non numérotées UA**

- SABM : Etablissement de la connexion
- SABME : Etablissement de la connexion
- DISC : Libération de la connexion
- UA : Confirmation de la connexion
- FRMR : Récupération des erreurs
- DM : Indication de connexion libérée

Exemple1

Résumé du scénario:

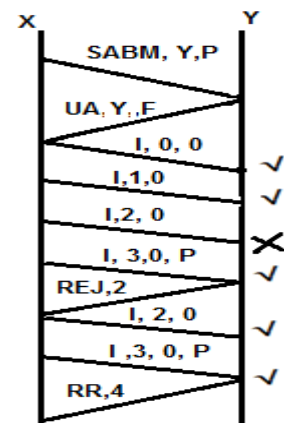
- Demande de connexion par X et acceptation de Y
- X envoie 4 trames
- Transmission sans erreurs et Y accuse la bonne réception.



Exemple 2

Résumé du scénario:

- Demande de connexion par X et acceptation de Y
- X envoie 4 trames
- La 3^e Trame (numéro 2) est erronée et Y la rejette (rejet systématique)
- X retransmis à partir de la trame erronée
- Retransmission sans erreurs et Y accuse la bonne réception



5.4 Conclusion

Dans ce chapitre, nous avons mis en évidence la couche physique en décortiquant son mode de communication et ses caractéristiques. Nous avons également analysé les différentes techniques de détection/correction d'erreurs utilisées dans cette couche.

Le prochain chapitre sera dédié à la présentation de la pile de protocoles TCP/IP; ses différents protocoles, composants, fonctionnalités et caractéristiques.

Chapitre 6

L'architecture TCP/IP

6.1 Introduction

Le modèle **TCP/IP** (TCP: Transmission Control Protocol, IP: Internet Protocol) a été créé dans les années 1970 par le Département de la Défense Américain (DOD) afin de permettre l'utilisation de différents protocoles de communication. Il est progressivement devenu le modèle de référence. Il est né d'une implémentation à la base du réseau ARPANet, la normalisation est survenue plus tard pour devenir avec le temps le cœur du réseau Internet. TCP/IP est donc un modèle mis au point pour s'adapter aux réseaux hétérogène et permettre l'interconnexion des réseaux, indépendamment de leurs technologies et de leurs positions. Il désigne communément une architecture réseau qui consiste en deux protocoles étroitement liés : un protocole de transport, TCP qu'on utilise "par-dessus" un protocole réseau, IP ; le protocole d'Internet.

Ce chapitre portera principalement sur la couche réseau et la version 4 de son principal protocole IP afin d'expliquer les processus fondamentaux comme l'adressage et le routage de données de cette couche. En outre, une analyse de la couche transport et ses principaux protocoles, ainsi que la couche application sera également fournie.

6.2 Le modèle TCP/IP

Le modèle TCP/IP est en fait une architecture de réseau à quatre couches (voir la figure 6.1), dans laquelle les protocoles TCP et IP tiennent une place prépondérante, car ils sont la mise en œuvre la plus courante.

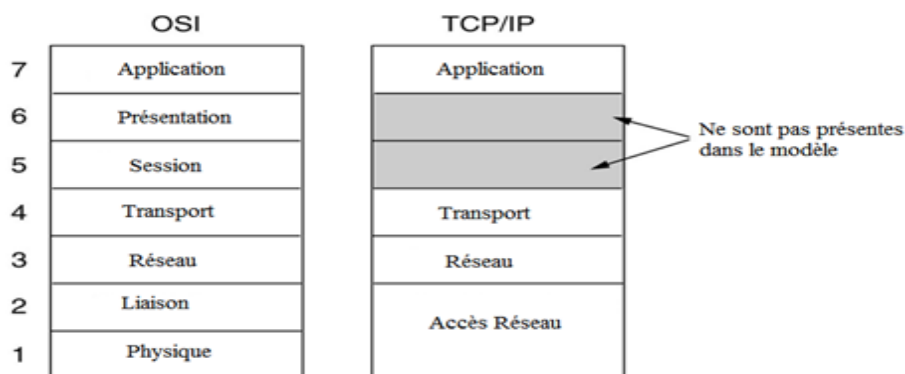


Figure 6.1 La pile protocolaire TCP/IP

▪ Rôle et fonctionnalité de chaque couche de la pile protocolaire TC/IP

Le modèle TCP/IP a repris l'approche modulaire du modèle OSI mais n'a conservé que quatre couches, dont les détails sont donnés ci-dessous. Dans la figure 6.2, les protocoles les plus importants régis par chaque couche sont illustrés.

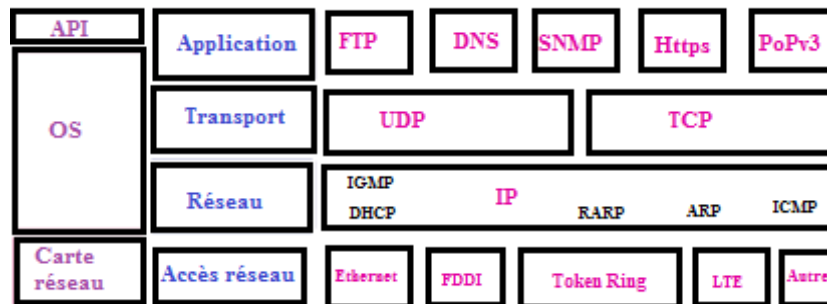


Figure 6.2 Les protocoles TCP/IP

a. La couche Physique / Accès réseau

- Cette couche représente l'interface avec le matériel réseau réel en offrant une connexion palpable au support physique de transmission.
- L'implémentation de cette couche ne spécifié aucun protocole ou technologie, et donc peut utiliser presque toute interface réseau disponible, ce qui illustre sa flexibilité.
- Elle peut fournir une transmission fiable ou non.
- Permet d'assurer la transmission des bits via un canal de transmission.
- Sélectionner le mode de transmission adéquat: unidirectionnel ou bidirectionnel

b. La couche réseau

- Même rôle que la couche Réseau du modèle OSI
- Assure l'adressage et le routage des paquets via le protocole IP (répondre à la question comment router les paquets)
 - Choisir une route pour acheminer les paquets de données de la source vers la destination (les paquets sont acheminés d'une manière indépendante et individuellement, et peuvent ainsi arrivées dans le désordre).
- Assurer l'interconnexion des réseaux hétérogènes distants.

c. La couche Transport

- Même rôle que la couche Transport du modèle OSI
- Assure le transfert des données de bout en bout en les délivrant d'une manière fiable et sans erreur d'une application à son homologue distant.
- L'interface entre la couche application et la couche transport est définie par des numéros de port et des sockets.

- Il existe deux modes de transport de données :
 - Mode connectée: fiable; point à point; dans le même ordre (**TCP**).
 - Sans contrôle d'erreur ni d'ordre (**UDP**).

d. La couche Application

- Cette couche est fournie par le programme qui utilise TCP/IP pour la communication
- Elle fixe les modalités de connexion avec TCP et UDP et les règles de fonctionnement à respecter.
- Elle contient tous les protocoles de haut niveau ; par exemple FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), HTTP (HyperText Transfer Protocol), etc.

6.3 Le Protocole IP

IP (Internet Protocol) est un protocole destiné à acheminer les paquets (de la couche transport) de manière indépendante entre les différentes machines. Il convient à tous les autres protocoles de la famille TCP/IP. Les paquets de données sont acheminés de proche en proche jusqu'au destinataire.

6.3.1 Principe

- IP offre le service attendu de la couche réseau du modèle TCP/IP. D'ailleurs, seuls les protocoles de plus haut niveau sont chargés des informations contenues dans les paquets IP et de leur ordre de réception.
- Il permet de disposer d'un système de transmission de données optimisé. Le terme "**optimisé**" signifie qu'il ne garantit pas la réception des paquets transportés à destination, ni leur arrivée selon leur ordre d'envoi.
- IP offre un fonctionnement **non fiable et sans connexion**
 - **Non fiable** : aucune garantie que les paquets parviendront à leur destination; les paquets peuvent être perdus, retardés, modifiés ou dupliqués à l'insu de la source ou de la destination.
 - **Sans connexion (mode non-connecté)**: Chaque paquet est acheminé indépendamment des autres.
- Deux générations peuvent être distinguées: **IPv4** et **IPv6** (nous étudierons uniquement la version 4 du protocole IP).

6.3.2 Format du datagramme IP

Les messages véhiculés par le protocole IP sont appelés paquets ou datagrammes. Un datagramme IPv4 comprend deux volets : une partie en-tête et une partie données. La somme des deux parties ne peut pas dépasser 64 kilo-octets. En addition, l'en-tête a une valeur fixée de 20 octets.

Ci-dessous, figure un exemple typique de l'en-tête d'un datagramme IP

32 bits			
Version (4 bits)	Longueur de l'en-tête (4 bits)	Type de service (8 bits)	Longueur totale (16 bits)
Identification (16 bits)			Drapeau (3 bits) Décalage fragment (13 bits)
Durée de vie (8 bits)	Protocole (8 bits)		Somme de contrôle en-tête (16 bits)
Adresse IP source (32 bits)			
Adresse IP destination (32 bits)			
Données			

Figure 6.3 L'entête IP

La signification des différents champs :

- **Version** (4 bits) : c'est la version 4 du protocole IP que nous utilisons ici (IPv4), afin de contrôler la conformité du datagramme. Il est codé sur 4 bits.
- **Longueur d'en-tête (IHL : Internet Header Length)** (4 bits) : Il correspond au nombre de mots de 32 bits qui composent l'en-tête (la valeur minimale est de 5). Il est codé sur 4 bits.
- **Type de service** (8 bits) : il précise la méthode de traitement du datagramme.
- **Longueur totale** (16 bits) : il désigne la taille totale du datagramme en octets. La taille de ce champ est de 2 octets, ainsi la taille totale du datagramme ne peut pas dépasser 65536 octets. Associé à la taille de l'en-tête, ce champ permet de déterminer où se trouvent les données.
- **Identification, drapeaux (flags) et déplacement de fragment** : ce sont des champs qui permettent la fragmentation des datagrammes.
- **Durée de vie** appelée aussi **TTL (Time To Live)** (8 bits) : Ce champ représente le nombre maximum de routeurs par qui peuvent être traversés par le datagramme. Ainsi ce champ est décrémenté à chaque traversée d'un routeur, lorsqu'il atteint la valeur de 0, le routeur détruit le datagramme. Cela permet d'éviter la congestion du réseau causée par les datagrammes perdus.
- **Protocole** (8 bits) : ce champ, en notation décimale, permet de savoir de quel protocole est issu le datagramme (ICMP : 1, IGMP : 2, TCP : 6, UDP : 17).
- **Somme de contrôle de l'en-tête, ou header checksum (16 bits)** : Ce champ comporte une valeur codée de 16 bits utilisée pour vérifier l'intégrité de l'en-tête afin de déterminer s'il n'a pas été modifié pendant la transmission.
- **Adresse IP source** (32 bits) : il représente l'adresse IP de la machine émettrice, il permet au destinataire de répondre.
- **Adresse IP destination** (32 bits) : adresse IP du destinataire du message.

6.3.3 La fragmentation des datagrammes IP

Un datagramme a une taille maximale de 65536 octets. Cependant, les réseaux étant dépourvus d'une capacité suffisante pour envoyer des paquets aussi volumineux, cette valeur n'est jamais atteinte. De plus, sur Internet, les réseaux utilisent des technologies différentes et, par conséquent, les limites de la taille maximale d'un paquet varient en fonction du type de réseau.

La taille maximale d'une trame est appelée **MTU (Maximum Transfer Unit)**, qui provoquera sa fragmentation s'il est plus grand que le MTU du réseau.

Exemple de MTU :

Type de réseau	MTU (en octets)
Arpanet	1000
Ethernet	1500
FDDI	4470

La **fragmentation** d'un paquet est effectuée au niveau **des routeurs** à la transition d'un réseau dont le **MTU est grand** vers un réseau dont le **MTU est plus petit**. Si le paquet est trop volumineux pour transiter sur le réseau (voir figure 6.4), le routeur va le fragmenter. En d'autres termes, il va le découper en fragments de tailles inférieures au MTU du réseau.



Figure 6.4 Exemple de MTU

- Les fragments d'un datagramme ont chacun un en-tête.
- L'en-tête est copié à partir du datagramme original.
- Un fragment est traité comme un datagramme IP normal lorsqu'il est transporté vers leur destination.
- Si l'un des fragments est perdu, le datagramme complet est considéré comme perdu et cela implique une retransmission complète du segment TCP d'origine.
- Puisque IP ne fournit pas de mécanismes d'accusé de réception, les fragments restants sont rejetés par l'hôte de destination.
- Les fragments sont envoyés d'une manière indépendante
- Seul le destinataire a la capacité de réassembler les différents fragments.

6.3.4 L'adressage IP

La procédure d'identification des différents composants d'un réseau s'appelle l'adressage. Une **adresse IP** est un numéro servant à identifier **chaque appareil** connecté à l'**Internet**. Il désigne en fait, l'**interface réseau** de tout équipement informatique connecté à un réseau utilisant le **protocole Internet (IP)**. Les principales caractéristiques des adresses IP sont :

- Ces adresses sont des adresses logiques qu'il faut absolument différencier des adresses physiques.
- Elles occupent 32 bits (4 octets).
- Le plus souvent, on les écrit sous la forme de 4 entiers décimaux séparés par un point décimal: **oct1.oct2.oct3.oct4** ; où chacune des quatre valeurs **oct** est un nombre compris entre 0 et 255.

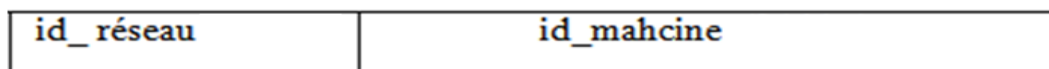
Exemple : Adresse IP: 10000010 00001010 00000111 00000011
 Adresse en décimal: 130.10.7.3.

- Le nombre d'adresses possibles est théoriquement 2^{32} .
- Une machine reliée à plusieurs réseaux (plusieurs interfaces avec des équipements différents) aura donc plusieurs adresses Internet.

a. Format d'une adresse IP

Une adresse IPv4 se décompose en deux parties :

- L'adresse de réseau **id_réseau** (Netid)
- L'adresse de la machine dans le réseau **id_machine** (hostid)

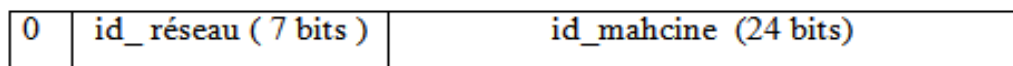


- Les tailles respectives de ces deux parties de l'adresse IP (réseau et machine) dépendent de la classe du réseau

b. Les classes d'adresse IP

L'adresse de réseau pourra avoir une des différentes formes suivantes

1. Classe A



Cette classe est réservée aux très gros réseaux:

- Le premier bit (de poids fort) est à 0.
- Les 7 bits suivants déterminent l'adresse de réseau.
- Les 24 bits restant constituent l'adresse de la machine
- Plus de 16 Millions d'équipements par réseau (possibles).
- Le nombre de tels réseaux est limité au niveau mondial à 128.
- Les adresses IP de classe A sont épuisées.

2. Classe B

10	id_réseau (14 bits)	id_mahcine (16 bits)
----	---------------------	----------------------

La classe B est réservé aux gros réseaux comme les sociétés importantes et les grosses administrations:

- Les deux premiers bits sont respectivement 10.
- Les 14 bits suivants constituent l'adresse de réseau (16384 réseaux).
- 16 bits restants permettent jusqu'à 65536 équipements.
- Toutes Les @ IP de classe B ont déjà été attribuées (classe expirée).

3. Classe C

110	id_réseau (21 bits)	id_mahcine (8 bits)
-----	---------------------	---------------------

La classe C est la classe utilisée par le grand public ; plus précisément les petits réseaux et particuliers :

- Les trois premiers bits sont 110.
- 21 bits indiquent l'adresse de réseau.
- L'adresse machine sur 8 bits (peut comporter 256 équipements).
- Cette classe est presque expirée, et cela explique la transition progressive vers l'IPv6 qui utilise un adressage de 128 bits au lieu de 32 bits pour l'IPv4.

4. Classe D

1110	Adresse multicast
------	-------------------

Elle est réservée à l'adressage du groupe de diffusion : le multicast :

- Chaque groupe a une adresse de groupe sur 28 bits
- Deux types de groupes : *permanents et transitoires*

5. Classe E

1111	Réservée
------	----------

Cette classe est non utilisée et réservée pour les expériences.

Exemple

Soit l'adresse IP : 194.40.20.10

Conversion binaire: 11000010001010000001010000001010

← @ R
← @ M

Classe C

→ C'est une adresse d'une machine de classe C.

c. Les sous réseaux IP (sous adressage IP)

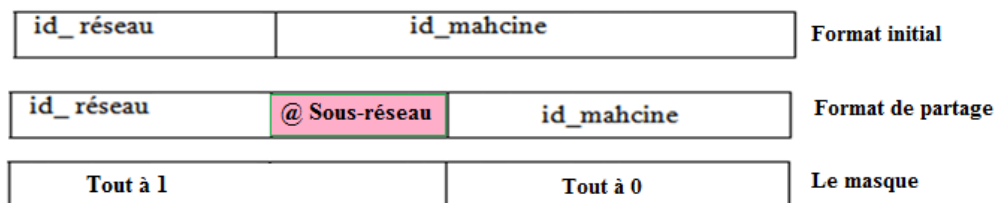
Il est possible de diviser un réseau en plusieurs petites structures appelées sous-réseaux. Ces sous-réseaux ne sont pas visibles en dehors de leur site.

Le concept de division d'un réseau en sous-réseaux repose sur l'utilisation de masques de sous-réseaux (Netmask). Autrement dit, un sous-réseau est une subdivision logique d'un réseau de taille importante définie par un masque.

Le masque

- Un masque est une suite de bits ayant la même longueur qu'une adresse IP.
- Il permet de modifier l'interprétation des adresses logiques localement.
- Cette modification est invisible en dehors du réseau concerné.
- Chaque machine effectuera une opération ET (bit à bit) entre l'adresse IP et le masque.
- Il suffit alors de placer des bits à 1 dans le masque pour conserver le id_réseau et des 0 pour l'id_machine, c.à.d. les bits du masque de sous-réseau sont à :

- "1" : partie de l'adresse réseau et "0" : identificateur de machine.



Exemple 1:

- Le masque de réseau : 11111111 11111111 11111111 00000000

Indique que :

- les *trois premiers octets* identifient le **réseau**
- le *quatrième octet* identifie une **machine** sur ce réseau.

Exemple 2

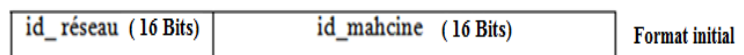
Soit le réseau IP: 130.128.0.0. On veut réaliser un découpage en 30 sous réseaux.

- Donner le masque associé.

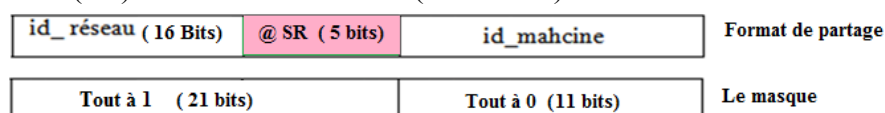
→ Solution

@ binaire du (130.128.0.0)₁₀=(10000010100000000000000000000000)₂

C'est une adresse de la classe B.



30 sous réseaux (SR) → 5 bits nécessaires (30=11110)



D'où le masque: 11111111111111111111000000000000 → En décimal: 255.255.248.0.

d. Les adresses interdites

Il existe des adresses IP interdites que l'on ne peut pas assigner à un équipement :

- **Les adresses réseaux** : une adresse réseau sert à référencer le réseau lui-même dont l'identificateur de machine **id_machine égale à zéro '0'**.
- **Les adresses de diffusion (broadcast)** : identifient toutes les machines du réseau, et ce sont les adresses dont tous les bits de la partie **id_machine sont à 1**.
- **L'adresse de boucle locale (loopback) 127.0.0.1** associé au nom **localhost**.
- **L'adresse 0.0.0.0** signifie une adresse de lien local. Elle est utilisée par des différents services (DHCP, tables de routage, ...) comme adresses de configuration automatique par défaut des interfaces d'hôtes.

e. Affectation des adresses IP

On distingue deux modalités pour attribuer une adresse IP à un équipement.

- **De manière statique** : l'adresse est fixe et configurée le plus souvent manuellement puis stockée dans la configuration du système d'exploitation.
- **De manière dynamique** : l'adresse est automatiquement transmise et assignée grâce au protocole DHCP (Dynamic Host Configuration Protocol).

6.3.5 Le Routage

Le routage est la fonction qui permet en utilisant un protocole spécifique et un système d'adressage approprié de véhiculer les données vers le destinataire lorsque celui-ci n'est pas sur le même réseau physique que l'émetteur (voir figure 6.5). Au fait, le routage IP est effectué de proche en proche car IP ne connaît pas la route complète entre l'émetteur et le destinataire (excepté si les deux machines sont sur le même réseau). La seule information fournie par le routage est l'adresse IP du routeur de saut suivant vers lequel le datagramme doit être envoyé.

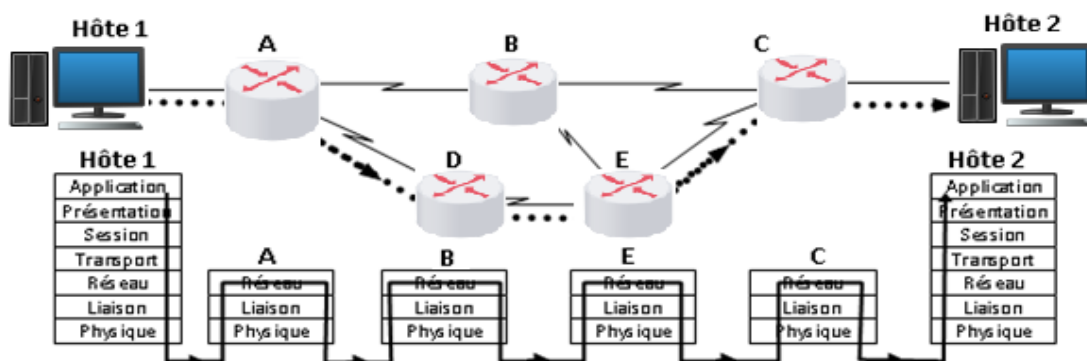


Figure 6.5 Exemple de routage

a. Table de routage

- Dans une table de routage figurent :
 - L'adresse de la destination à atteindre (adresse de la station, adresse du réseau)
 - L'adresse du prochain saut (next hop) de l'équipement suivant à rejoindre.
 - Une route par défaut (toujours fournie).
- Le routage est principalement réalisé par **deux types d'équipements** réseaux :
 - **Les stations** ne possédant qu'une seule interface réseaux.
 - **Les routeurs** qui détiennent plusieurs interfaces réseaux afin de gérer la connexion entre ces réseaux.

Les **Tables de routage** ont généralement les champs suivants.

@ Réseau	Interface	Prochain Saut	Métrique
----------	-----------	---------------	----------

- **Le champ @ Réseau (Network)**: indique l'adresse de la destination
- **Le champ interface**: IP consulte la table de routage pour savoir sur quelle interface envoyer le paquet. Pour effectuer cette consultation il extrait le numéro de réseau de l'adresse destination
- **Le champ prochain saut (Next saut)**: Le routage IP est effectué sur le base de saut à saut (hop to hop routing). Le message est transmis de routeur en routeur par sauts successifs, jusqu'au destinataire.
- **Le champ Métrique (Métic)**: elle désigne le coût relatif de l'utilisation de l'itinéraire pour atteindre la destination. Une métrique standard est le tronçon (ou saut), c'est-à-dire le nombre de routeurs à traverser avant d'atteindre la destination.

Exemple

La figure 6.6 ci-dessous illustre une table de routage d'un routeur

Destination	Routeur de prochain pas	Interface
136.1.0.0	Connecté directement	Port 1 (136.1.0.254)
138.9.0.0	Connecté directement	Port 2 (138.9.0.254)
137.5.0.0	136.1.2.5	Port 1
135.12.0.0	136.1.2.3	Port 1
140.33.0.0	138.9.1.2	Port 2
0.0.0.0	136.1.2.254	Port 1

Figure 6.6 La table de routage d'un routeur

b. L'établissement des tables de routage

Deux stratégies de routage sont utilisées:

- **Statiques:** la mise à jour des tables de routage est établie par les administrateurs des différents équipements de l'Internet (Stations, passerelles...);
- **Dynamiques:** la mise à jour est faite automatiquement en fonction de mesures de trafic; Les différents équipements peuvent s'échanger des informations de routage.

Il est recommandé d'utiliser un routage statique pour les stations et un routage dynamique (protocoles: **RIP**, **OSPF**) pour les routeurs. Il va de soi qu'un équipement a besoin d'une stratégie de routage s'il a deux adresses IP au moins.

6.4 Le Protocole TCP

Pour pallier les problèmes suscités par le manque de fiabilité du protocole IP, un protocole fiable, appelé TCP, a été défini au niveau de la couche Transport.

6.4.1 Principe

TCP est équivalent à la couche transport classe 4 de l'ISO. C'est un **protocole à remise garantie, orienté connexion, qui permet un acheminement sans erreurs des messages** avec retransmission en cas de perte, et élimination des données dupliquées

1. La transmission

- *Orienté connexion*
- *Transferts tamponnés*
- *Connexions bidirectionnelles simultanées*

2. La fiabilité

- *Utilisation des acquittements plus temporisateurs*
- *Mécanisme de fenêtre*

Le protocole TCP permet de :

- Remettre en ordre les paquets reçus,
- Vérifier le flot de données afin d'éviter une saturation du réseau,
- Formater les données en segments de longueur variable afin de les remettre au **protocole IP**
- TCP permet l'initialisation et la fin d'une communication.
- TCP effectue le multiplexage/démultiplexage : faire transiter sur une même ligne des données provenant de différentes applications

- Ces opérations sont réalisées grâce aux **ports (ou sockets)** qui est un numéro associé à un type d'application et combiné à une adresse IP, pour déterminer de façon unique une application qui tourne sur une machine donnée.

6.4.2. Le format d'un segment TCP

Un segment TCP est constitué comme illustré sur la figure 6.7 .

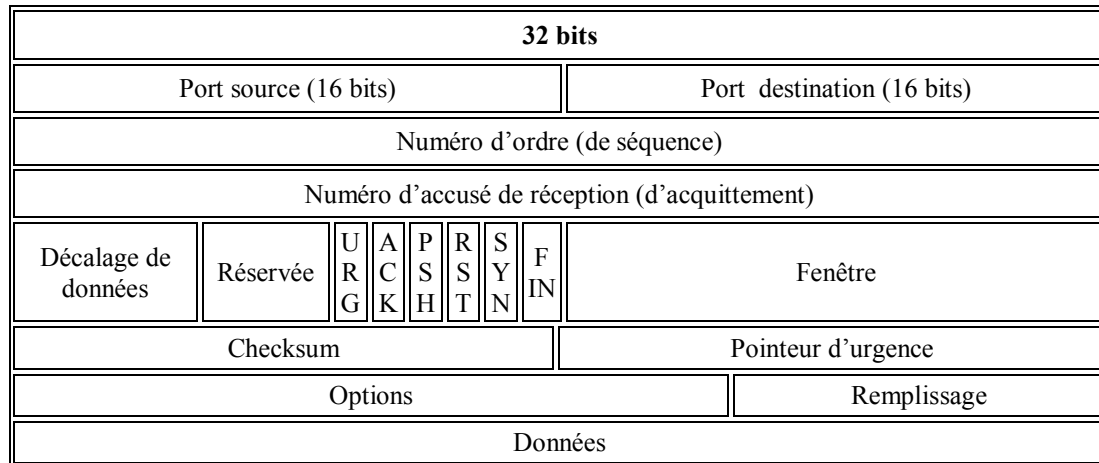


Figure 6.7 L'entête TCP

Signification des différents champs :

- **Port Source** (16 bits): Port relatif à l'application en cours sur la machine source
- **Port Destination** (16 bits): Port relatif à l'application en cours sur la machine de destination
- **Numéro d'ordre** (32 bits): Lorsque le drapeau SYN est à 0, le numéro d'ordre est celui du premier mot du segment en cours. Lorsque SYN est à 1, le numéro d'ordre est égal au numéro d'ordre initial utilisé pour synchroniser les numéros de séquence (ISN)
- **Numéro d'accusé de réception** (32 bits): Le numéro d'accusé de réception également appelé numéro d'acquittement correspond au numéro (d'ordre) du prochain segment attendu, et non le numéro du dernier segment reçu.
- **Décalage des données** (4 bits): il permet de repérer le début des données dans le paquet. Le décalage est ici essentiel car le champ d'options est de taille variable
- **Réservé** (6 bits): Champ inutilisé actuellement mais prévu pour l'avenir
- **Drapeaux (flags)** (6x1 bit): Les drapeaux représentent des informations supplémentaires :
 - **URG**: si ce drapeau est à 1 le paquet doit être traité de façon urgente.
 - **ACK**: si ce drapeau est à 1 le paquet est un accusé de réception.
 - **PSH** (PUSH): si ce drapeau est à 1, le paquet fonctionne suivant la méthode PUSH.
 - **RST**: si ce drapeau est à 1, la connexion est réinitialisée.
 - **SYN**: Le Flag TCP SYN indique une demande d'établissement de connexion.
 - **FIN**: si ce drapeau est à 1 la connexion s'interrompt.

- **Fenêtre** (16 bits): Champ permettant de connaître le nombre d'octets que le récepteur souhaite recevoir sans accusé de réception
- **Somme de contrôle** (Checksum ou CRC): La somme de contrôle est réalisée en faisant la somme des champs de données de l'en-tête, afin de pouvoir vérifier l'intégrité de l'en-tête
- **Pointeur d'urgence** (16 bits): Indique le numéro d'ordre à partir duquel l'information devient urgente
- **Options** (Taille variable): Des options diverses
- **Remplissage**: On remplit l'espace restant après les options avec des zéros pour avoir une longueur multiple de 32 bits

6.4.3 Fiabilité des transferts

Le protocole TCP permet d'assurer le transfert des données de façon fiable, bien qu'il utilise le protocole IP, qui n'intègre aucun contrôle de livraison de datagramme. Il garantit l'arrivée des messages, c'est-à-dire qu'en cas de perte, les deux extrémités sont prévenues. En d'autres termes, le protocole TCP possède **un système d'accusé de réception** permettant à l'émetteur et au destinataire de s'assurer de la bonne réception mutuelle des données.

- Ce concept repose sur les techniques d'acquittement de message: lorsqu'une source S émet un message M_i vers une destination D, S attend un acquittement A_i de D avant d'émettre le message suivant M_{i+1} .
- Si l'acquittement A_i ne parvient pas à S, S considère au bout d'un certain temps (time-out) que le message est perdu et réémet M_i .
- Un numéro de séquence est attribué à chaque octet transmis et requiert un acquittement positif (ACK).
- Lors de la réception, les numéros de séquence servent à ordonner les segments et à éliminer les doublons.

Résumé de principe de fonctionnement

- Lors de l'émission d'un segment, un **numéro d'ordre** (appelé aussi *numéro de séquence*) est associé.
- A la réception d'un segment de donnée, la machine réceptrice va retourner un segment de donnée dont le drapeau ACK est à 1 (afin de signaler qu'il s'agit d'un accusé de réception), accompagné d'un numéro d'accusé de réception égal au numéro d'ordre précédent.
- De plus, grâce à **une minuterie** déclenchée dès réception d'un segment au niveau de la machine émettrice, le segment est réexpédié dès que le temps imparti est écoulé, car dans ce cas la machine émettrice considère que le segment est perdu.

- Toutefois, si le segment n'est pas perdu et qu'il arrive tout de même à destination, la machine réceptrice saura grâce au numéro d'ordre qu'il s'agit d'un doublon et ne conservera que le dernier segment arrivé à destination.

6.5 Le Protocole UDP

Le protocole UDP ne constitue qu'une simple interface au-dessus de la couche réseau (IP). Ainsi l'émission des messages se fait sans garantie de bon acheminement. C'est donc un protocole **non fiable** et sans **contrôle de séquençement** ni celui **de flux**. Le protocole UDP est utilisé:

- Quand il est nécessaire soit de transmettre des données très rapidement (et/où la perte d'une partie de ces données n'a pas grande importance), soit de transmettre des petites quantités de données (la voix sur IP).
- Pour la diffusion comme les applications à modèle 'Questions-Réponses'
- Pour vérifier l'intégrité des données avec un total de control. Comme il est orienté sans connexion. Cela évitera l'ouverture et la fermeture des connexions.
- Le protocole UDP est plus rapide, plus simple et plus efficace que TCP mais il est moins robuste.
- IL est conçu pour les applications qui n'ont pas à assembler des séquences de segments. Donc pas de segmentation ni d'assemblage.

6.5.1 Format de l'en-tête UDP

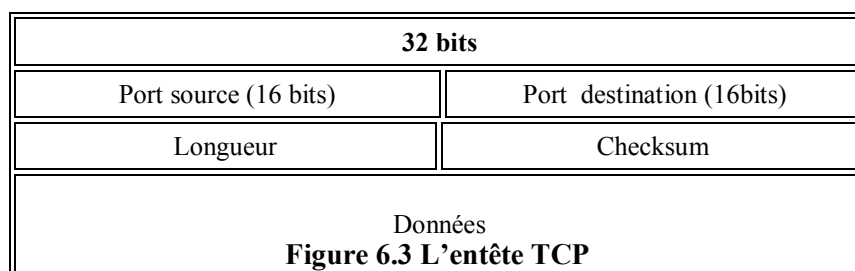


Figure 6.8 L'entête UDP

- **Port source** : ce champ est codé sur 16 bits et correspond au port relatif à l'application en cours sur la machine source.
- **Port destination** : codé sur 16 bits et il correspond au port relatif à l'application en cours sur la machine de destination.
- **Longueur** : le champ *longueur* est codé sur 16 bits et il représente la taille de l'entête et des données. Son unité est l'octet et sa valeur maximale est 64 Koctets.
- **Checksum** : codé sur 16 bits et représente la validité du paquet UDP.

6.6 Les protocoles de la couche Application

Avant de détailler le plus important protocole au sein de la couche application en l'occurrence le protocole DNS, ci-dessous une liste de d'autres protocoles régis par cette couche.

- **HTTP** (HyperText Transport Protocol): Transport des fichiers hypertexts (pages Web)
- **FTP** (File Transfer Protocol): Transfert de fichiers
- **Telnet** : Système de terminal virtuel, permet d'accès distant aux applications
- **SMTP** (Simple Mail Transfert Protocol): offre une service de courrier électronique
- **ICMP** (Internet Control and error Message Protocol)
- **PPP** (Point to Point Protocol)
- **POP3** (Post Office Protocol version 3): récupération du courrier à distance
- **SLIP** (Serial Line Interface Protocol): protocole d'encapsulation des paquets
- **DNS** (Domaine Name System): Service traduisant un nom de domaine en adresses IP

6.6.1 Le système de nom de domaine DNS

DNS permet aux ordinateur qui se connectent sur Internet via un Modem, de leur attribuer des un nommage hiérarchique (valable pour la connexion uniquement) :

- Pour une connexion temporelle le DNS donne une @ temporelle.
- Pour une connexion permanente le DNS donne une @ IP.
- Et d'une façon générale le DNS permet le passage d'une @ IP à une @ de nommage et vis versa.

Le **Nom de domaine** se compose de plusieurs parties séparées par un point (suite de labels séparés par un point). Il se lit de droite à gauche, le champ le plus à droite indique le nom de la **zone**, puis nous avons le **nom de domaine** et enfin le nom de la **machine**.

- ✓ Le nom de zone peut être soit le nom du pays de rattachement (en deux lettres) soit le nom d'une catégorie d'utilisateurs (en trois lettres) souvent localisée aux Etats-Unis.

- ✓ Les noms de zones en trois lettres correspondent à :

com entités commerciales

edu institutions éducatives (Universités);

gov agences gouvernementales (exemple la NASA) (uniquement USA)

mil entités militaires (uniquement USA)

net entités qui gèrent l'Internet

org organisations bénévoles

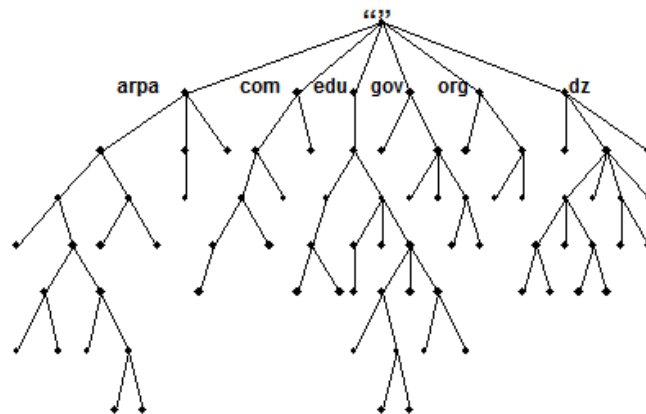
int organisations internationales

Le rôle principal du système DNS consiste d'identifier une machine par un nom représentatif et unique. En outre, assurer les correspondances : Nom machine \rightarrow @ IP machine

@IP machine \rightarrow Nom machine

Organisation de l'espace de nom du DNS

Comme le DNS est un système hiérarchique (Arborescence), en général il commence par un nœud racine noté « . ». Chaque nœud est responsable de ses données



6.8 Conclusion

Dans ce chapitre, il a été question de présenter en détail l'architecture TCP/IP. Nous avons présenté les protocoles TP, TCP, UDP en détaillant leurs caractéristiques et principales fonctionnalités. Nous avons aussi, décrit le système de nomination hiérarchique de nom de domaines DNS.

Bibliographie

- [1] Danièle Dromard, Fetah Ouzzani, Dominique Seret, Kim-Loan Thai, **Réseaux informatiques : cours et exercices**. Eyrolles, 1994.
- [2] Nicolas Turin, **L'univers des réseaux Ethernet: Concepts, produits, mise en pratique**, Masson, 1995.
- [3] Guy Pujolle, **Initiation aux réseaux: Cours et exercices**, Eyrolles. 2000.
- [4] Mike Busby, **Introduction à TCP/IP**, Osman Eyrolles Multimedia, 2000.
- [5] Adolfo Rodriguez, John Gattrell, John Karas, Roland Peschke , **IBM (ibm.com/redbooks), TCP/IP Tutorial and Technical Overview**, Seventh Edition , August 2001.
- [6] Deon Reynders, Edwin Wright, **Practical TCP/IP and Ethernet Networking**, An imprint of Elsevier,2003.
- [7] A. Tanenbaum, **Réseaux**, Pearson Education France, 2003
- [8] Djillali Seba, **SISCO Interconnexion Des Réseaux à L'aide Routeurs Et Commutateurs**, ENI, 2003.
- [9] Charles M. Kozierok, **The TCP/IP Guide**, Version 3.0, 2005.
- [10] Diane Barrett, Todd king, **Computer Networking Illuminated**, Jones And Bartlett Publishers, 2005.
- [11] Danièle Dromard, Dominique Seret, **Architecture des réseaux, Synthèse de cours & exercices Corrigés**, 2009.
- [12] Jean Luc Montagnier, **Réseaux d'entreprise Par La Pratique**, Eyrolles, 2011
- [13] Petit. Bertrand. **Architecture des réseaux: Cours et exercices corrigés**. Ellipses, 2013
- [14] Guy Pujolle, **Les Réseaux**, Eyrolles, 2014.
- [15] José Dordoigne, **Réseaux informatiques, notions fondamentales: Protocoles, Architectures, Réseaux sans fil, Virtualisation, Sécurité, IP**, Volume 6, ENI, 2015

Annexe

Exercices

- **Séries de TD 2017- 2021**
- **Sujets d'examen et interrogation**

Série TD1

Exercice 1

Q1. Compléter les deux paragraphes 1. et 2. par les mots indiqués sur la liste suivante :

Télécommunication, communication, reliées, l'échange, d'ordinateurs - informatique -de communication - d'équipements – logiciels – numérique

1. Un réseau informatique est une collection d'objet de et d'informations. Ces entités sont et connectées entre elles par l'intermédiaire des lignes physiques appelées lignes dequi assure le transport et des données informatiques.

2.Un réseau est un ensembleinformatiques (Matériels et) reliées entre eux par des moyens

Q2. De quoi est composé un réseau ?

Q3. Qu'apportent les réseaux ?

Exercice 2

Q1. Quel est le type de réseau le plus adapté pour connecter deux sites localisés un à Tlemcen et l'autre à Jijel ?

Q2. Quelle est la différence entre la topologie physique et la topologie logique ?.

Q3. Enumérez les principales différences entre les topologies: bus, anneau et étoile.

Q4. C'est quoi la commutation ? Énumérez ses différents types tout expliquant le principe de chaque mode.

Exercice 3

1. Citer quelques types d'informations transmises par les réseaux informatiques.

2. Quels sont les principaux agents physiques employés pour la transmission de l'information ?

3. Quel est le *quantum* d'information ?

- Quels sont ses multiples, et quelle quantité cela représente-t-il ?



Série TD2

Exercice 1

- Décrire la situation du réseau avant la normalisation
- Quelle est l'importance de normalisation ?
- Que signifie une couche, l'entité et le service dans le modèle OSI.

Exercice 2

Q1. A quelle couche du modèle OSI les paquets sont-ils encapsulés en trames?

☐ Liaison de données ☐ Réseau ☐ Transport ☐ Session

Q2. Comment appelle-t-on un ensemble de règles qui détermine le format et la transmission des données?

- ☐ Norme ☐ Modèle ☐ Représentation ☐ Protocole

Q3. Quelle couche du modèle OSI assure la connectivité et la sélection du chemin entre deux systèmes d'extrémité où se produit le routage?

- ☐ Couche physique ☐ Couche liaison de données
☐ Couche réseau ☐ Couche de transport

Q4. Comment s'appelle l'information de contrôle placée avant les données au moment de leur encapsulation pour transmission dans le réseau?

- ☐ Trame ☐ En-tête ☐ Capsule ☐ Information de routage

Q5. Le modèle à 7 couches de l'OSI est utile parce que cela :

- ☐ Réduit la complexité
☐ Permet un développement modulaire
☐ Permet l'interopérabilité
☐ Toutes les réponses précédentes
☐ Aucune des réponses précédentes

Q6. Définissez les deux modèles: Client/Serveur et P2P, tout en détaillant les caractéristiques de chaque type.

Exercice 3

Un message de 30 octets est transmis de la couche application d'un système A vers la couche application d'un système B. Chaque couche de la hiérarchie ISO/OSI ajoute 5 octets d'information de contrôle. Quelle est la taille du message reçu par la couche 7 du système B?

Exercice 4

Supposons qu'un paquet ait une longueur de 128 octets et que, sur ces 128 octets, 40 soient dévolus à la supervision (contrôle de la communication et contrôle d'erreur). Si l'on encapsule ce paquet dans un autre paquet ayant également 40 octets de supervision, calculer le pourcentage de données de supervision qui sont transportées dans le flot ? Qu'est-ce que vous déduisez ?



Série de TD N°3

Exercice 1

Q1. Donner l'équipement qui peut être le meilleur à utiliser dans chaque cas :

- Relier deux segments de câbles sur un même réseau et permet de s'affranchir des limitations de distances imposées par les normes.
- Utilisé dans la couche physique et peut mixer différents media (paire torsadée, fibre optique,...)
- Utilisé dans la couche transport et supérieure (4 et sup.). Permet d'inter-fonctionner des systèmes d'information hétérogènes.

Exercice 2

Q1. Quelle est la topologie utilisée dans les cas suivants :

- ✓ Internet,
- ✓ Ethernet avec utilisation de hub,
- ✓ Ethernet avec utilisation de Switch,
- ✓ Token Ring

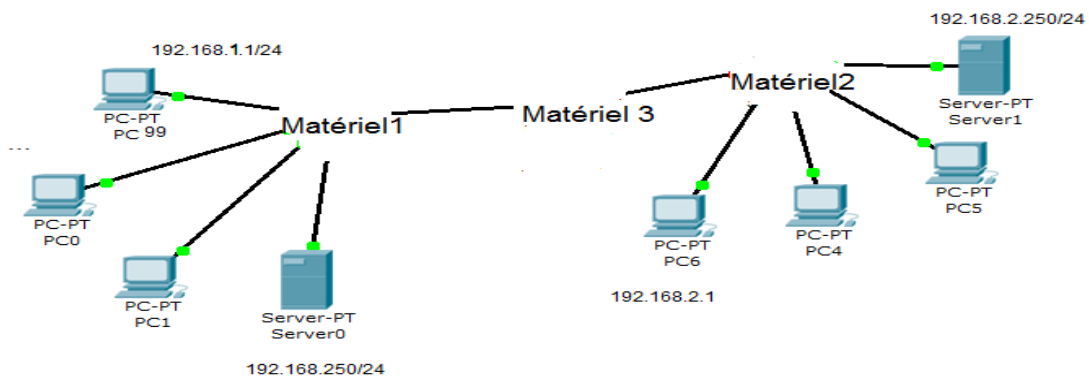
Exercice 3

Soit le schéma du réseau figurant ci-après :

Q1. En justifiant brièvement votre choix, proposer les équipements matériels d'interconnexion réseau nécessaires (matériel_1, matériel_2 et matériel_3).

Q2. Proposer un adressage IP possible pour le matériel_3.

Q3. Expliquez à quoi sert une passerelle.



Exercice 4

Supposons que dans chaque établissement scolaire, les équipements de la salle informatique sont mis en réseau.

Q1. Quel type de réseau s'agit-il dans chaque salle?

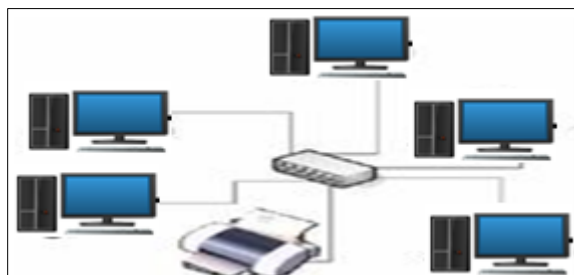
Q2. Peut-on lier les réseaux des salles informatiques aux établissements d'une ville ? Si oui comment appelle-t-on ce réseau ?

Q3. Peut-on faire la même chose au niveau de tout le pays ? Si oui comment appelle-t-on ce réseau ?

Q4. Quels moyens peut-on utiliser comme supports de transmission dans les deux derniers cas?

Exercice 5

La salle d'informatique de la figure ci-contre est équipée d'un réseau comportant 5 ordinateurs et une imprimante partagée.



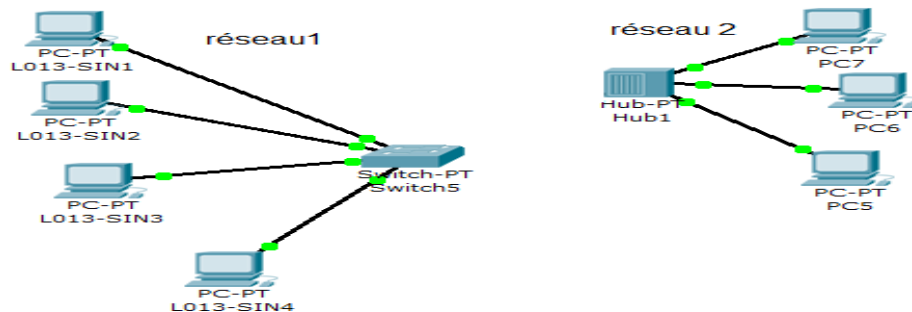
- 1) Il s'agit de quel type de réseau? Quelle est sa topologie?
- 2) Quels sont les équipements matériels utilisés dans ce réseau ?
- 3) Quel est le type de câble utilisé ?
- 4) Est-ce que l'utilisateur de poste1 peut utiliser l'imprimante ? Justifier.

Exercice 6

Soit les deux réseaux suivants :

Q1. On prend en considération le protocole ICMP. Si l'ordinateur L013-SIN1 envoie un PDU vers l'ordinateur L013-SIN2, quelles sont les différentes étapes de cette communication ?

Q2. Même question pour le réseau 2 entre PC7 et PC6.



- Si on veut relier les deux réseaux, que doit-on faire ?



Série de TD N°4

Exercice 1

Q1. On envoie la suite de bits : 01001110.

Quels sont les signaux correspondants en NRZ, Biphasé Manchester , Biphasé différentiel, RZ, Bipolaire ?

Q2. La même question pour la suite de bits: 01001100011.

Exercice 2

Q1. On divise le polynôme $x^7 + x^5 + 1$ par le polynôme générateur $x^3 + 1$. Quel est le reste obtenu ?

Q2. Un code utilise le polynôme générateur $x^2 + x + 1$. Quel est l'encodage du message 11011 ?

Exercice 3

Q1. Quel est le débit binaire proposé par un modem qui utilise une rapidité de modulation de 9600 bauds et une modulation de 4 phases ($V=4$)?

Exercice 4

Q1. Combien de temps cela prendra-t-il pour transmettre **X Koctets** sur un lien de **Y Mbps**? Donnez votre réponse sous le format d'un ratio de X sur Y.

Q2. Quel est le temps de transmission de 1Kb sur un réseau dont le débit est : 10 Mb/s, 100 Mb/s ou 1Gb/s ?

Q3. Quel est le délai de retour d'un message de Q Kbits envoyé sur un anneau comprenant N stations? Chaque station introduit un délai de traversée de t seconds. Les stations sont reliées, deux à deux, par un câble de L mètres. La vitesse de propagation de signaux est V km/s. Le débit du réseau est de d Mb/s.

Exercice 5

On considère un réseau dont le débit est de 10 Mbits/s. Les messages envoyés sur ce réseau ont une taille maximale de 1000 bits dont un champ de contrôle de 16 bits.

Q1. Quel est le nombre de messages nécessaires pour envoyer un fichier F de 4 Mbits d'une station à une autre ?

On considère l'hypothèse où une station ne peut pas envoyer un nouveau message qu'après avoir reçu un acquittement de la bonne réception du message précédemment envoyé.
L'acquittement prend la forme d'un message de 16 bits. Un temporisateur est armé à une durée T après l'envoi de chaque message. Si le temps T expire avant la réception d'un acquittement la station émettrice renvoi le même message. La distance qui sépare les deux stations les plus éloignés sur ce réseau est de 1 Km. La vitesse de propagation de signaux est $V=200000\text{Km/S}$.

Q2. Quelle est la durée minimum de T ?

Q3. En ignorant le temps de propagation, quelle est la durée totale de l'envoi du fichier F ?

Q4. Quelle est l'efficacité du réseau dans ces conditions ?

Exercice 6

On veut transmettre un message entre deux machines (A et B) reliées par un commutateur, d'où le débit de transmission sur la première ligne est 100. 000 bit/s et sur le deuxième est 10 000 bit/s.

Q1. Dessiner un schéma pour relier ces machines en exploitant l'énoncé.

Q2. Calculer le temps de transmission d'un message de taille 40000 octets dans le cas de commutation de paquets de taille 2000 bits.



Série de TD N°5

Exercice 1

Q1. C'est quoi une adresse MAC? C'est quoi une adresse IP?. Quelle est la différence entre les deux adresses

Q2. Indiquez la classe et le type des adresses suivantes:

- 194.199.90.1
- 114.0.2.1
- 10.2.3.4
- 192.168.196.246
- 224.10.20.2
- 194.199.90.255
- 127.0.0.1

Exercice 2

Q1. On travaille maintenant en notation CIDR. Indiquez quels sont les postes situés sur les mêmes réseaux :

192.168.196.10/24, 192.168.197.10/24, 192.168.196.246/24, 172.16.0.2/16,
172.16.10.3/16, 192.168.10.12/25, 192.168.10.50/25, 192.168.10.100/25,

Q2. Donner la topologie du réseau à partir de la table de routage suivante.

Réseau	Masque	Moyen de l'atteindre
192.168.2.0	255.255.255.0	eth0
100.0.0.0	255.0.0.0	eth1
101.0.0.0	255.0.0.0	eth2
192.168.1.0	255.255.255.0	100.0.0.1
192.168.3.0	255.255.255.0	101.0.0.2

Exercice 3

Q1. Une station appartenant à un réseau local possède l'adresse 192.38.241.26.

- 1) Quelle est la classe d'adresse de ce réseau local ?
- 2) Quel est le nombre maximal de stations dans ce réseau ?

Q2. Une machine faisant partie d'un réseau local qui possède la configuration suivante:

– Adresse IP : 192.168.54.53

– Masque : 255.255.255.240

1. Combien ce réseau peut-il posséder de sous-réseaux avec ce masque de sous-réseau?
2. Combien de machines par sous-réseau ?
3. Quel est l'adresse de sous-réseau ?
4. Quel est le numéro de la machine dans ce sous-réseau ?

Exercice 4

Supposons que deux hôtes A et B soient placés en réseau et sont séparés par 03 lignes de transmission et de 02 commutateurs C1 et C2 comme le montre le schéma ci-dessous.



Q1.
En

supposant que les 3 lignes de transmission proposent un débit de 10 000 bits/s chacune et de que le temps de commutation (temps passé par un message ou un paquet sur un commutateur avant retransmission) est de 100 ms sur chaque commutateur, calculer le temps total d'envoi d'un message de 20 000 bits de A à B, dans le cas de la commutation par message et de dans le cas de la commutation par paquets de 1000 bits.

On néglige le temps de propagation du signal: un bit émis est supposé immédiatement reçu.

Interrogation

Exercice 1

Q1. Choisissez la (les) bonne(s) réponse(s).

1. *Quel est l'ordre exact des couches du modèle OSI.*

- a) Application, présentation, session, transport, réseau, liaison de données, physique.
- b) Application, transport, réseau, accès réseau.
- c) Physique, liaison de données, réseau, transport, session, présentation, application.
- d) Application, session, présentation, réseau, liaison de données, physique.

2. *Qu'est-ce qu'un réseau local?*

- a) Un réseau qui relie des postes de travail, des terminaux et d'autres unités dans un endroit géographiquement limité.
- b) Un réseau qui relie des postes de travail, des terminaux et d'autres unités dans une grande région métropolitaine.
- c) Un réseau qui dessert des utilisateurs dans une vaste région géographique et qui utilise souvent des unités de transmission fournies par un transporteur.
- d) Un réseau qui couvre une région plus grande qu'un réseau métropolitain.

3- *Une trame est un(e)*

- a) PDU de couche 2.
- b) PDU de couche 3.
- c) Paquet encapsulé.
- d) a et c.

4. A quelle couche OSI correspond le protocole IP

- a) La couche 2.
- b) La couche 3.
- c) La couche 4 .
- d) a et b.

Q2. Pourquoi les réseaux WAN ont-ils pour la plupart une topologie en anneau ou maillée ?.

Q3. A quelle couche du modèle OSI travaille

- a) un hub, un switch Ethernet et un routeur ?

Q4. Expliquez pourquoi on doit utiliser un modem lors d'une transmission à longue distance.

Exercice 2

Q1. Dans un réseau local dont le débit binaire est de 5 Mbit/s, les signaux se propagent à la vitesse de 250m/μs. Un bit transmis est équivalent à quelle longueur de câble? Ceci a-t-il une influence sur le choix de la longueur des messages ?

Q2. Quelle est la valeur du rapport signal sur bruit nécessaire pour transmettre le débit de 100 Mbit/s sur une ligne offrant une bande passante de 20 MHz ?

Exercice 3

Q1. Illustrez dans des figures les codages NRZ, Biphase Manchester , Bi-phase différentiel, RZ, Bipolaire des séries binaires suivantes:

- a) 01001011000101
- b) 10110100111010



Examen 1

Questions de cours

Q1. Choisissez la (les) bonne(s) réponse(s).

1. Les fonctions que chaque couche du modèle OSI peut traiter:
 - a) Le niveau physique réceptionne un flux de bits et le formate en trame pour remise à la couche liaison de données.
 - b) Le chemin à travers le réseau est déterminé par la couche transport.
 - c) La synchronisation des échanges de données est gérée par la couche application.
2. Pour connecter deux ordinateurs, on a besoin :
 - a). d'un câble RJ45 direct
 - b). d'un câble Rj45 croisé
 - c). un câble série
 - d). un câble console
3. Quelle sera le mot encodé avec un polynôme générateur $G(x) = x^2 + x + 1$ et l'information 11011 ?
 - a) 11011111
 - b) 11011101
 - c) 11011110
 - d) 11011011
4. Pour la classe C, le nombre maximum de machines par réseau est :
 - a). 253
 - b). 255
 - c). 254
 - d). 256

5. On distingue trois grands types d'adresses IPv4 :

- a) Les adresses Unicast.
- b) Les adresses Broadcast.
- c) Les adresses Anycast.
- d) Les adresses Multicast.

6. Le terme *socket*

- a) Précise l'identité physique de l'ordinateur dans le réseau.
- b) Un numéro associé à un type d'application.
- c) Désigne un canal de communication par lequel un processus peut envoyer ou recevoir des données.
- d) Désigne l'identification de diffusion du sous réseau.

Q2. Quelles sont les différences principales entre un réseau de transmission de circuit et un réseau de transmission à commutation par paquets ?

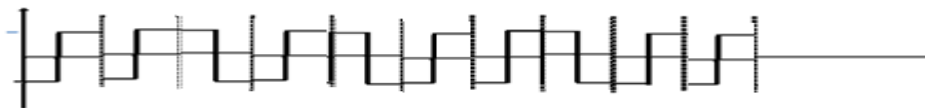
Q3. Supposons qu'un ensemble de machines sont connectées à un réseau local Ethernet. Si ces machines ne communiquent que l'une avec l'autre, est-il sensé d'utiliser IP dans ces dernières?

Ces machines devraient-elles exécuter TCP directement sur Ethernet? Dans ce cas, comment l'adressage est-il géré?.

Exercice 1

Q1. Pourquoi la plupart des protocoles fiables utilisent-ils un code détecteur avec une stratégie de retransmission plutôt qu'un code correcteur ?

Q2. La figure suivante illustre le signal qui représente l'information transmise de la machine A vers B en utilisant le codage Manchester.



- Donner la suite binaire représentée par le signal.

Q3. La machine B récupère l'information envoyée par la machine A . Elle calcule le CRC associé à cette information et elle trouve la valeur X^3+X^2+X .

- 1. Expliquer brièvement le principe du CRC .
- 2. Sachant qu'on utilise le polynôme générateur X^4+X+1 . Est-ce que l'information reçue est correcte ou non ? justifier votre réponse.
- 3. Dans le cas où l'information est mal reçue, que doit faire la machine B ?

Exercice 2

Q1. Qu'est-ce que la transmission en bande de base ?

Q2. On utilise dans la transmission de trames d'un émetteur A vers un récepteur B un protocole défini de la manière suivante.

- a) L'émetteur envoie successivement trois trames puis attend leur acquittement de la part de B.
- b) Quand cet acquittement arrive, l'émetteur envoie les trois trames suivantes et attend un nouvel acquittement.
- c) Les trames sont composées de 1024 bits dont 80 bits de service
- d) Les acquittements sont composés de 64 bits
- e) Le débit de la voie est de 2 Mbits/s et la vitesse de propagation des ondes électromagnétiques est de 3.10^8 m/s sur la voie de 10 km reliant A et B.

- 1. Quelle est la durée nécessaire à l'expédition confirmée d'une trame ?
- 2. Quel est le taux d'occupation de la voie ?
- 3. Un message de 1 Mo est envoyé de A vers B par utilisation du protocole précédent. Quelle est la durée totale de la transmission de ce message ?

Exercice 3

Q1. Expliquez la différence entre le contrôle de flux et le contrôle de congestion.

Q2. Un datagramme IP peut être segmenté en plusieurs fragments.

- De quelles informations dispose-t-on pour savoir qu'un datagramme contient un fragment ?
- Comment reconstitue-t-on un datagramme à l'arrivée ?
- Une passerelle peut-elle confondre deux fragments qui ont les mêmes éléments suivants: source, destination et numéro de fragment ?

Q3. L'Architect réseau demande votre aide pour l'attribution des adresses IP. Les adresses IP doivent être attribuées à deux salles ou chacune d'elles comporte 6 machines. Sachant que l'Architect dispose de l'adresse réseau suivante: 192.168.2.0/2, aider le pour créer ses sous réseaux.

1. Quelle est la classe du 192.168.2.0/28 ? Combien d'adresses IP valides comporte ce réseau ?

Justifier votre réponse.

2. Donnez pour chaque sous réseaux :

- l'adresse sous réseaux,
- le masque sous réseaux,
- les plages d'adresses IP valides,
- l'adresse de broadcast.

- Supposons que la machine 192.168.2.9/28 souhaite envoyer un message à l'hôte 192.168.2.13/28.

Quel est le nombre minimum de routeurs que les paquets doivent traverser? Comment cela est déterminé?



Examen 2

Questions de cours

Q1. Choisissez la (les) bonne(s) réponse(s).

1. Si la zone couverte par un LAN est supérieur à 200 mètres, on doit utiliser :

- Une autre carte réseau
- Un pont
- Un répéteur
- Un autre serveur.

2. Quelle est la signification particulière des adresses suivantes?

- | | |
|--------------|---------------------|
| a.) 0.0.0.0 | 3.) 255.255.255.255 |
| b.) 0.0.0.18 | 4.) 161.115.255.255 |

3. L'adresse IP 127.0.0.1 est une adresse:

- | | | |
|--------------|------------|--------------------------|
| a). Réservee | b). Privée | c). Adresse de diffusion |
|--------------|------------|--------------------------|

4. Lesquels des éléments suivants sont garantis sous IP?:

- Les paquets arriveront dans le même ordre que leur envoi.
- IP utilise l'adresse IP stockée dans chaque datagramme pour acheminer le paquet.
- Les paquets IP contiendront les adresses IP source et de destination.
- IP utilise le numéro de port stocké dans chaque datagramme pour acheminer le paquet.
- Les paquets ont une longueur fixe.
- Une fois la connexion établie, les paquets empruntent tous le même itinéraire.

5. Complétez les phrases suivantes

La fragmentation d'..... se fait au niveau des....., lors de la transition d'un réseau dont le MTU est important à un réseau dont le MTU est plus.....

Si le datagramme est trop grand pour passer sur le réseau, le routeur va le fragmenter et le en fragments de tailles inférieures au MTU du réseau.

Les mots proposés : un message, une trame, switches, routeurs, répéteurs, faible, un datagramme, grand, découper, données, réassembler, tailler, passerelles, MTU.

Exercice 1

Q1. On utilise le polynôme générateur $x^4 + x^2 + x$.

1. Si on reçoit les deux messages suivants : 1111000101010, 11000101010110, sont-ils corrects ?

2. Si on souhaite envoyer le mot 11000101. Calculer le code CRC ajouté ?

Quel mot obtiendra-t-on alors ?

Q2. Calculer LRC/VRC associé à la transmission du message « HELLO » sachant que les codes ASCII des caractères HELLO sont : H → 0001001, E → 1010001, L → 0011001, O → 1111001

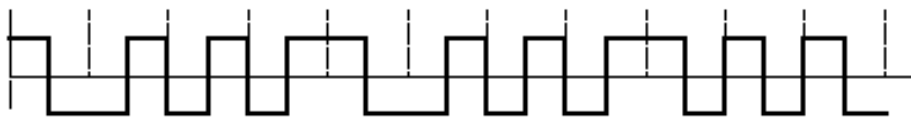
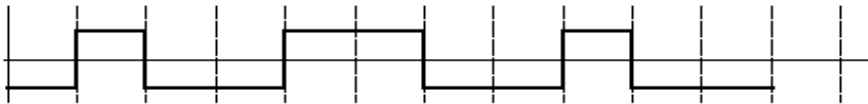
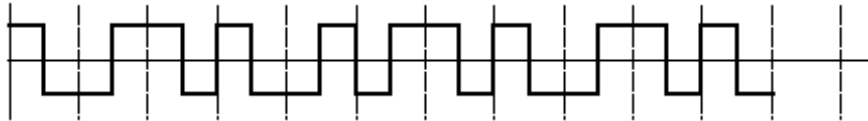
Exercice 2

Q1. Qu'est-ce que la transmission en bande de base ?

Q2. Expliquez pourquoi on doit utiliser un modem lors d'une transmission à longue distance.

Q3. Soit l'information binaire 0100110100 transmise de la machine A vers B en utilisant différents types de codages.

- Donner pour chaque figure le type de codage utilisé.



Exercice 3

Q1. Quelle est l'utilité d'une adresse IP par rapport à une adresse physique?

Q2. Pour définir 26 sous-réseaux si on dispose de l'adresse IP 150.35.0.0

a) Quel sera le masque de sous-réseau à utiliser.

Q3. Comparez entre un protocole orienté connexion et un protocole non orienté connexion . Quel type de protocole est IP, TCP et UDP?

Protocole orienté connexion	Protocole non orienté connexion

Q4. Une entreprise veut se raccorder à Internet. Pour cela, elle demande une adresse réseau de classe B afin de contrôler ses 2 853 machines installées en Algérie.

1. Une adresse réseau de classe B sera-t-elle suffisante ?

2. L'organisme chargé de l'affectation des adresses réseau lui alloue plusieurs adresses de classe C consécutives au lieu d'une adresse de classe B .

- Combien d'adresses de classe C faut-il allouer à cette société pour qu'elle puisse gérer tous ses terminaux installés ?

3. Finalement, la société a pu obtenir une adresse réseau de classe B. L'administrateur du réseau choisit de découper le réseau pour refléter la structure de l'entreprise, c'est-à-dire qu'il crée autant de sous-réseaux que la société compte de services différents. L'administrateur a donc prévu 12 sous-réseaux, numérotés de 1 à 12.

- Proposez le masque de sous-réseau utilisé dans l'un des services de la société.

- Combien reste-t-il de bits pour identifier les machines de chaque service ?

- Combien de machines peut-on identifier dans chaque service ?

Q5. L'adresse réseau de la société est : 139.47.0.0.

- Indiquez l'adresse réseau du sous-réseau 9.

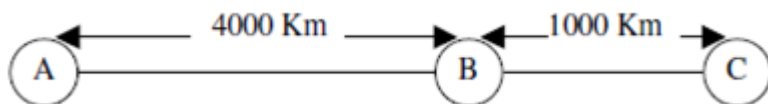
- Dans le sous-réseau choisi, donnez l'adresse IP complète de la machine ayant comme identifiant de machine 7.48.

- Donnez les adresses réseau et les adresses de diffusion du sous-réseau 12.

Exercice 4

On considère trois noeuds A, B, et C reliés comme indiqué par la figure ci-dessous.

Des trames générées par A sont envoyées vers C à travers B.



- Déterminer la débit de transmission minimal requis entre B et C afin que les tampons mémoire au niveau de B ne soient pas débordés, en se basant sur les hypothèses suivantes:

- Le débit entre A et B est de 100 Kbps,
- Le délai de propagation est de 5ms/Km pour les deux lignes,
- Les lignes sont full duplex entre les trois noeuds,
- Toutes les trames de données ont une taille de 1000 bits; les ACKs ont une taille négligeable,
- Entre A et B un protocole de contrôle de flux basé sur une fenêtre coulissante est utilisé avec une fenêtre = 3,
- Entre B et C le protocole utilisé est le stop-and-wait.
- Il n'y a pas d'erreurs de transmission.