Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Mohamed Khider - Biskra
Faculté des Sciences Exactes et des Sciences de la Nature et de la Vie
Département d'informatique

$2^{ème} année LMD$

Cours de Réseaux de Communication

Dr. Abdelhamid DJEFFAL
Site web : www.abdelhamid-djeffal.net

Année Universitaire 2019/2020

Plan du cours

1 Introduction aux réseaux informatiques

1.1 Définition d'un réseau informatique

1.2 Types de réseaux

1.3 Modes de communication

1.4 Fonctionnement des communications

1.5 Différentes techniques de commutation

1.6 Modèle OSI

1.6.1 Communication par couches

1.6.2 Encapsulation

1.7 Modèle TCP/IP

2 Couche physique

2.1 Modes de transmission

2.1.1 Transmission en parallèle

2.1.2 Transmission en série

2.1.3 Transmission en simplexe

2.1.4 Transmission en half duplex

2.1.5 Transmission en full duplex

2.2 Signal transmis

2.2.1 Signal analogique

2.2.2 Signal numérique

2.3 Caractéristiques d'une ligne de communication

2.3.1 La bande passante

2.3.2 Rapidité de modulation

2.3.3 Taux d'erreur

2.3.4 Débit binaire

2.3.5 Délai de propagation T_p

2.4 Supports de transmission
2.4.1 Supports à guide physique
2.4.2 Supports sans guide physique
2.5 Codage de l'information
2.5.1 Transmission numérique (en bande de base)
2.5.2 Modulation (large bande)
2.6 Multiplexage
2.6.1 Multiplexage temporel TDMA (Time Division Multiplexing Access)
2.6.2 Multiplexage fréquentiel FDM (Frequency Division Multiplexing)
2.6.3 Multiplexage statistique ATDM (Asyncronous Time Division Multiplexing)
2.7 Exercices

3 Couche Liaison de données
3.1 Délimitation de trames
3.1.1 Comptage des caractères
3.1.2 Utilisation des fanions
3.2 Détection et Correction d'erreurs
3.2.1 Définitions générales
3.2.2 Duplication de données
3.2.3 Code de contrôle de parité
3.2.4 Code de Hamming
3.2.5 Codes polynomiaux
3.2.6 Codes auto-correcteurs
3.3 Contrôle de flux
3.3.1 Envoyer et attendre (Sent and Wait)
3.3.2 Fenêtre d'anticipation
3.4 Procédures de gestion des données
3.4.1 Procédure BSC
3.4.2 Procédure HDLC
3.5 Protocole PPP
3.6 Exercices

4 Réseaux locaux
4.1 Standardisation

4.2 Topologies des réseaux locaux
4.2.1 Topologies physiques
4.2.2 Topologie Logique
4.3 Constituants d'un réseau local
4.4 Sous couche MAC
4.4.1 Adressage
4.4.2 Techniques d'accès au support
4.4.3 CSMA/CD
4.4.4 Token Ring
4.5 Sous couche LLC
4.6 Interconnexion des LANs
4.7 Réseaux locaux virtuels (VLAN)
4.8 Réseaux locaux sans fil WLAN
4.8.1 Architecture des WLANs
4.8.2 Technique d'accès
4.9 Exercices

5 Réseaux grande distance

5.1 Définition
5.2 Organisation physique
5.3 Connexion
5.3.1 Les opérateurs
5.3.2 Les lignes spécialisées (ou louées)
5.3.3 Les lignes multiplexées
5.4 Commutation
5.4.1 Réseaux de commutation
5.4.2 Techniques de commutation
5.5 Exercices

6 Couche Réseaux

6.1 Adressage et nommage
6.1.1 Adressage
6.1.2 Nommage
6.2 Routage
6.2.1 Principe

6.2.2 Routage statique
6.2.3 Routage dynamique
6.3 Protocole IP
6.3.1 Structure d'un paquet IP
6.3.2 RIP
6.3.3 ARP
6.3.4 RARP
6.3.5 ICMP
6.3.6 IGMP
6.4 Exercices

7 Couche Transport

7.1 Segmentation des messages
7.2 Séquencement des messages
7.3 Multiplexage et démultiplexage
7.4 Protection contre les erreurs
7.5 Protocoles de transport
7.5.1 TCP
7.5.2 UDP
7.6 Les sockets
7.6.1 Définition d'une socket
7.6.2 Utilisation des sockets

8 Solutions des exercices

8.1 Couche physique
8.2 Couche Liaison de données
8.3 Réseaux locaux
8.4 Réseaux grande distance
8.5 Couche Réseaux

9 Sujets d'examens

Références

Chapitre 1

Introduction aux réseaux informatiques

Les réseaux informatiques de nos jours sont devenus indispensables dans, pratiquement, dans tous les domaines de la vie : banques, assurance, sécurité, internet, santé, administration, transport, ...

Les besoins de communication de données informatiques entre systèmes plus ou moins éloignés sont multiples : transmission de messages (messagerie), partage de ressources (imprimante, disque dur, internet), transfert de fichiers (FTP), consultation de bases de données, gestion de transactions, télécopie ...

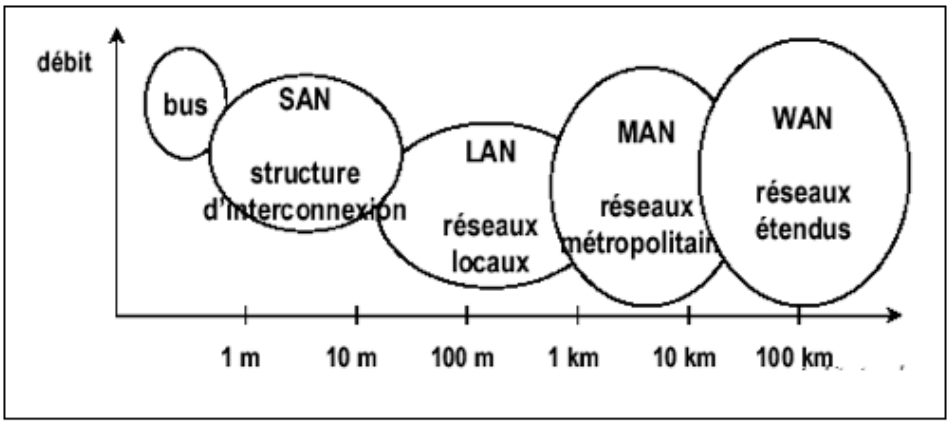
1.1 Définition d'un réseau informatique

C'est un ensemble d'ordinateurs et de périphériques autonomes connectés entre eux et qui sont situés dans un certain domaine géographique.

1.2 Types de réseaux

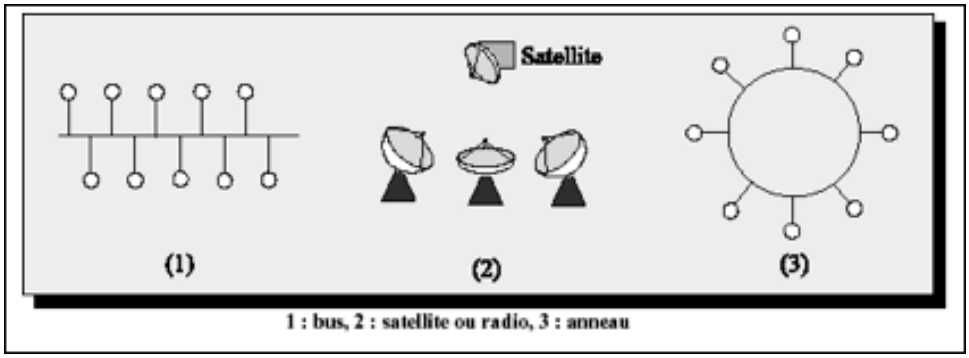
- Bus : Communication entres composants < 1m
- Architectures parallèles (réseaux d'interconnexions) >10m
- Réseaux locaux (LAN) : correspondent par leur taille à des réseaux intra - entreprises. La distance de câblage est de quelques centaines de mètres
- Réseaux métropolitain (MAN) : Correspondent à une interconnexion de quelques bâtiments se trouvant dans une ville (Campus).
- Réseaux étendus (WAN) destinés à transporter des données à l'échelle d'un pays.

Ces réseaux peuvent être terrestres (Utilisation d'infra - structure au niveau : câble, fibre, ...) ou satellite (Mise en place d'engins spatiaux pour retransmettre les signaux vers la terre).

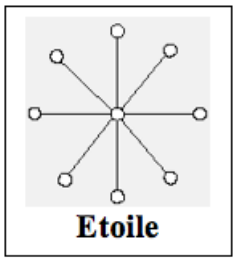


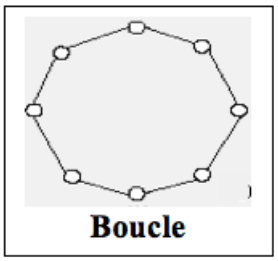
1.3 Modes de communication

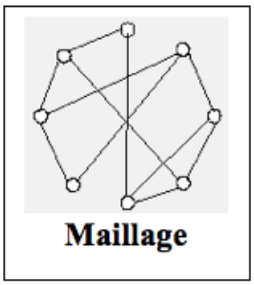
– Mode diffusion : Un émetteur ⇒ Plusieurs récepteurs



– Mode point à point : Un émetteur ⇒ Un récepteur







1.4 Fonctionnement des communications

Quelque soit l'architecture, on a deux modes de communications :

- **Avec connexion** (permanente) ⇒ demande de connexion
  1. Emetteur demande,
  2. Si récepteur refuse ⇒ pas de communication.
  3. Sinon circuit virtuel,
  4. Transfert de données,
  5. Libération de la connexion
  6. Lourde si peu d'informations (gaspillage du réseau)
  7. Difficulté des communications multiples.
- **Sans connexion** (Sans demande de connexion)
  1. Sans vérification que le récepteur est actif : boites aux lettres.
  2. Les organes du réseau gèrent les communications.
  3. Utilisations des buffers si le récepteur n'est pas actif

1.5 Différentes techniques de commutation

Le réseau doit permettre l'échange de messages entre les abonnés quel que soit leur localisation.

Définition : La commutation rassemble toutes les techniques qui réalise la mise en relation de 2 abonnés quelconques.

Il existe 4 techniques de commutation :

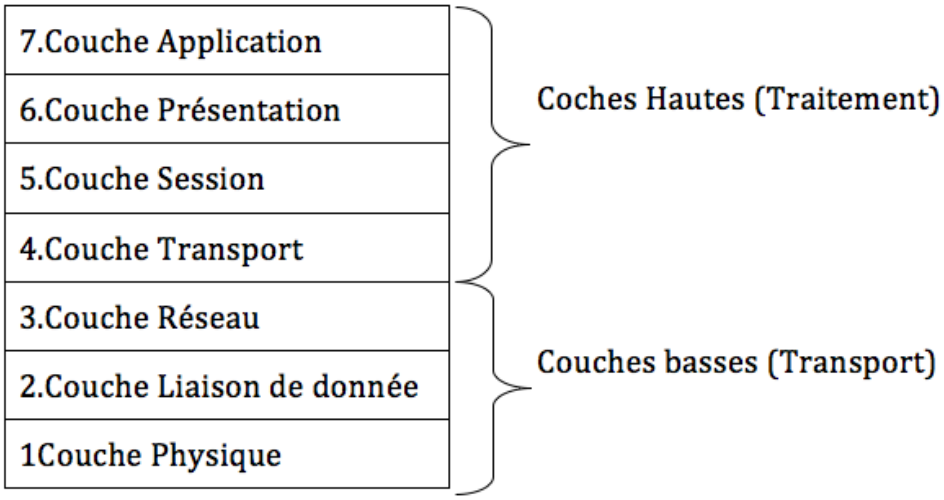
- **Commutation de circuits** (ex : le téléphone) : Un chemin physique est établi à l'initialisation de la communication entre l'émetteur et le récepteur et reste le même pendant toute la durée de la communication. Si les deux correspondants n'ont pas de données à transmettre pendant un certain temps, la liaison restera inutilisée.
- **Commutation de messages :** Un message est un ensemble d'information logique formant un tout (fichier, mail) qui est envoyé de l'émetteur vers le récepteur en transitant nœud à nœud à travers le réseau. On a un chemin logique par message envoyé. Le message ne peut être envoyé au nœud suivant tant qu'il n'est pas reçu complètement et sans erreur par le nœud actuel.
- **Commutation de paquets :** optimisation de la commutation de message qui consiste à découper les messages en plusieurs paquets pouvant être acheminés plus vite et indépendamment les uns des autres. Cette technique nécessite la mise en place de la numérotation des paquets.

– **Commutation de cellule :** commutation de paquets particulière. Tous les paquets ont une longueur fixe (1 paquet = 1 cellule de 53 octets dans ATM). Un chemin est déterminé pour la transmission des cellules. Commutation de cellule = superposition de 2 types de commutation : commutation de circuit et commutation de paquets.

1.6 Modèle OSI

A la fin des années 70 on a connu le développement de plusieurs solution réseaux indépendantes (SNA d'IBM, DECNET de DEG, DSA de Bull...) et on avait besoin d'une norme internationale pour inter communiquer.

L'ISO (International Standard Organisation) a pris en charge l'établissement de l'OSI (Open system interconnections : norme d'interconnexion des systèmes ouverts), cette norme se présente sous la formes de sept couches :



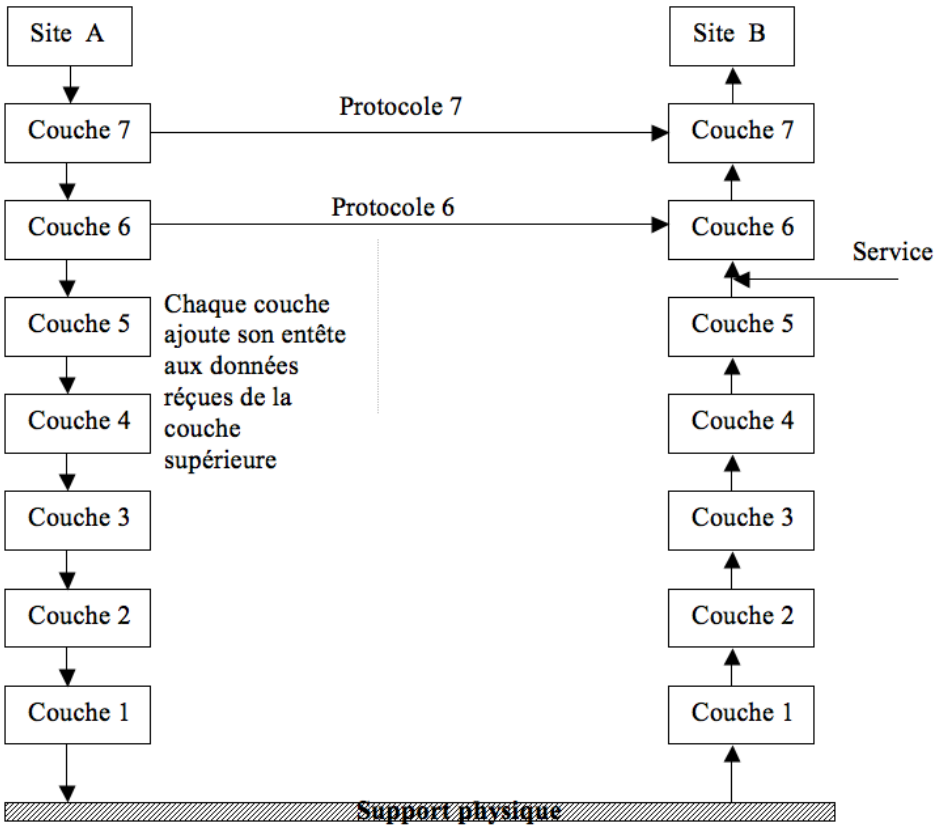
1. **Couche physique :** Etudie les signaux porteurs des informations (modulation, puissance, portée) ainsi que les supports de transmission (câbles, fibres optiques,...).
2. **Couche liaison de donnée :** Responsable de l'établissement, le maintient et la libération des connexions entre les éléments du réseau. Elle est responsable aussi de la détection et la correction des erreurs.
3. **Couche réseau :** Responsable de l'adressage des machines, et le routage des données dans le réseau.
4. Couche transport : Assure un transfert transparent de données entre les utilisateurs, en leur rendant invisible la façon dont les ressources de communications sont mises en œuvre.

5. **Couche session :** Assure l'optimisation et le réglage de quelques problèmes non dus au réseau tel que la reprise de transfert d'un fichier long après une erreur d'accès au disque.
6. **Couche présentation :** Assure des fonctions tel que la compression des données, la représentation des données (Exemple : poids fort à gauche ou à droite).
7. **Couche application :** Permet d'offrir aux logiciels les mêmes principes et standards d'accès aux réseaux (Notion de fichier virtuel).

1.6.1 Communication par couches

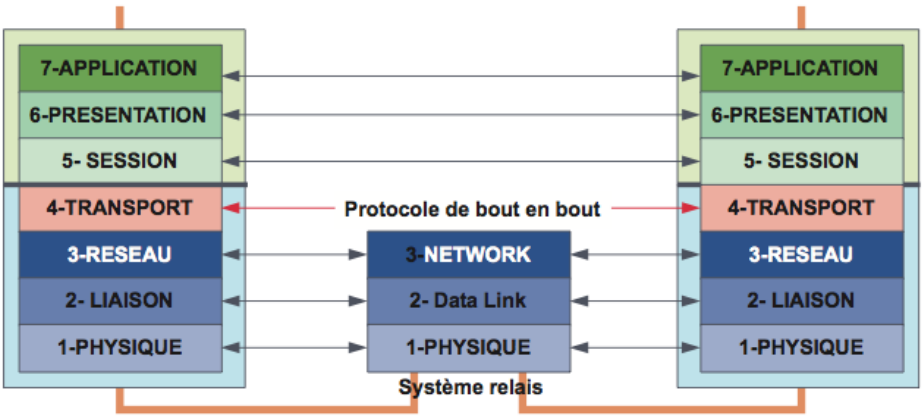
On appelle **protocole**, un dialogue connu par les deux parties, entre deux couches de même niveau. Une couche de niveau (n) ne sera capable de dialoguer qu'avec une autre couche de même niveau qu'elle.

On appelle **service** l'ensemble des fonctions que doit absolument remplir une couche, fournissant l'interface pour transmettre des données de la couche (n) à la couche (n+1).



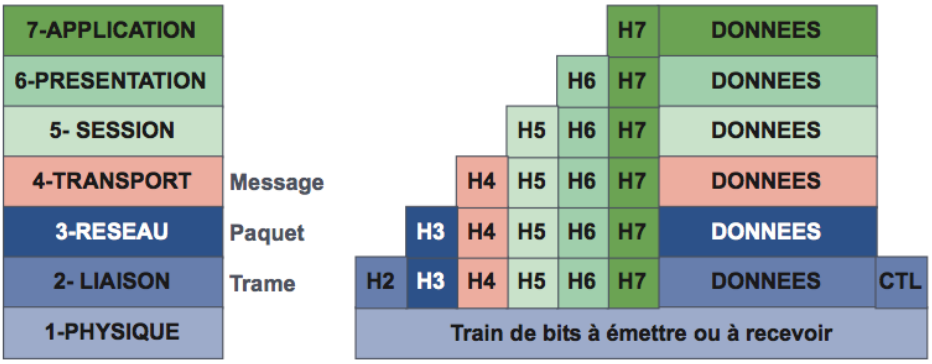
Pour réaliser une communication à travers un ou plusieurs systèmes intermédiaires (relais) il faut :

1. relier les systèmes par un lien physique (couche PHYSIQUE) ;
2. contrôler qu'une liaison peut être correctement établie sur ce lien (couche LIAISON) ;
3. s'assurer qu'à travers le relais (réseau) les données sont correctement acheminées et délivrées au bon destinataire (couche RÉSEAU) ;
4. contrôler, avant de délivrer les données à l'application que le transport s'est réalisé correctement de bout en bout (couche TRANSPORT) ;
5. organiser le dialogue entre toutes les applications, en gérant des sessions d'échange (couche SESSION) ;
6. traduire les données selon une syntaxe de présentation aux applications pour que celles-ci soient compréhensibles par les deux entités d'application (couche PRÉSENTATION) ;
7. fournir à l'application utilisateur tous les mécanismes nécessaires à masquer à celle-ci les contraintes de transmission (couche APPLICATION).



1.6.2 Encapsulation

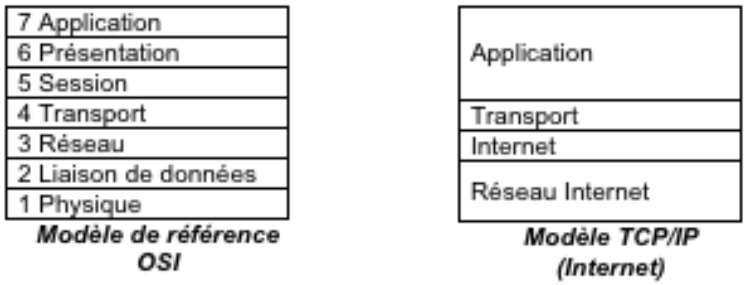
Lorsqu'une application envoie des données à travers le modèle OSI, les données traversent de haut en bas chaque couche jusqu'à aboutir au support physique où elles sont alors émises sous forme de suite de bits. Chaque couche ajoute aux données reçues de la couche supérieure des informations appelées "Entête" avant de les transférer à la couche inférieure. Cette entête permet à cette couche d'accomplir son rôle. A la réception, chaque couche retire l'entête, ajouté par la couche du même niveau, des données avant de les transmettre à la couche supérieure.



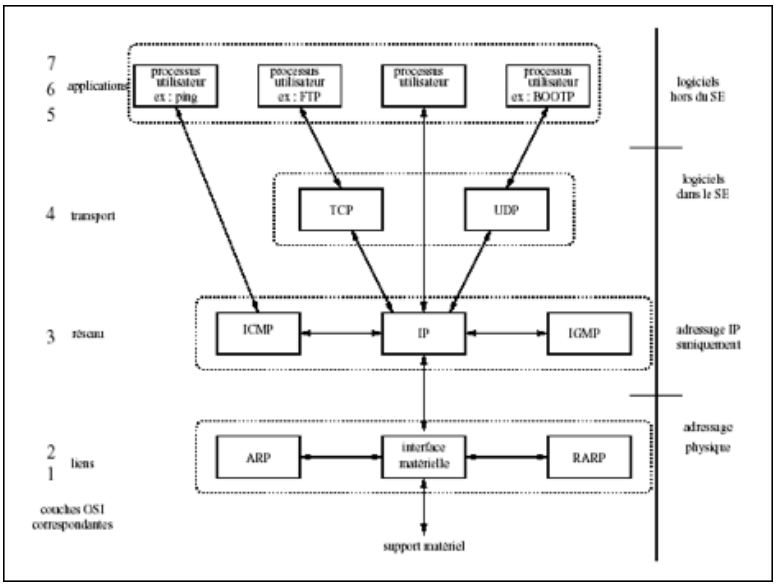
1.7 Modèle TCP/IP

La série des protocoles TCP/IP (Transmission Control Protocol / Internet Protocol) provient du projet DARPA (Defense Advanced Research Project Agency) de l'agence de recherche de projets avancés de la défense des USA vers la fin des années 60. Les protocoles ont évolué dans les années 70 pour passer en 1980 à l'utilisation dans les équipes de recherche et les universités des USA. Le nombre de réseaux utilisant TCP/IP a rapidement augmenté pour former une grande communauté appelée l'Internet. Aujourd'hui, le bureau d'activités inter réseaux ou l'IAB (Internet Activities Board) se charge du développement et de ratification des protocoles TCP/IP.

L'architecture TCP/IP est similaire au modèle OSI en couche, mais ne dispose que de 4 couches dans la plupart des cas.

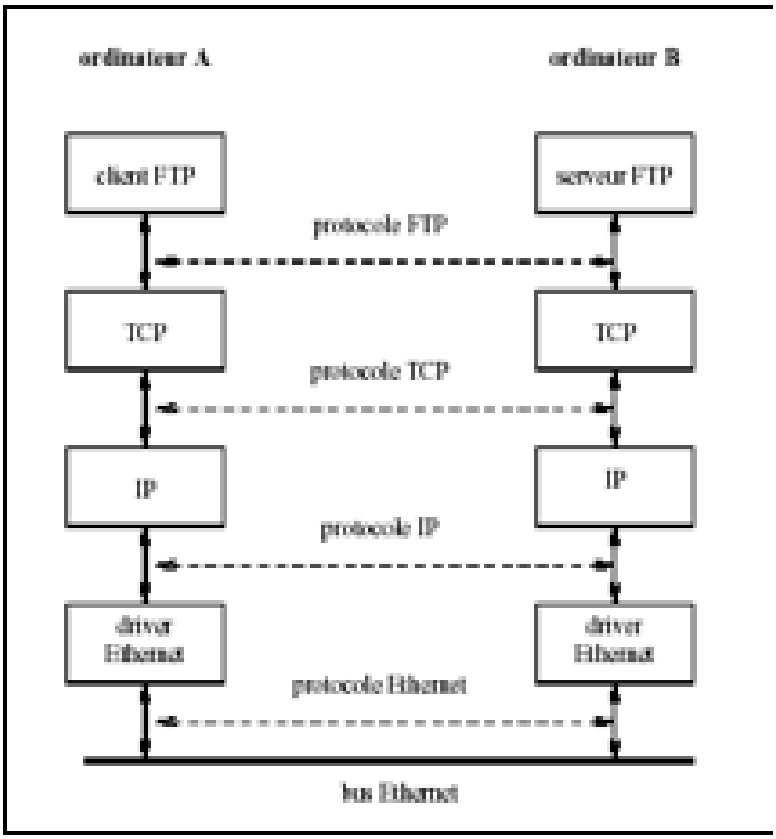


- Couche application : FTP, TELNET, HTTP, SMTP.
- Couche Transport : TCP (fiable), UDP (non fiable)
- Couche Internet : IP, ICMP
- Couche réseau Internet : Interface avec le réseau utilisé : ARP.

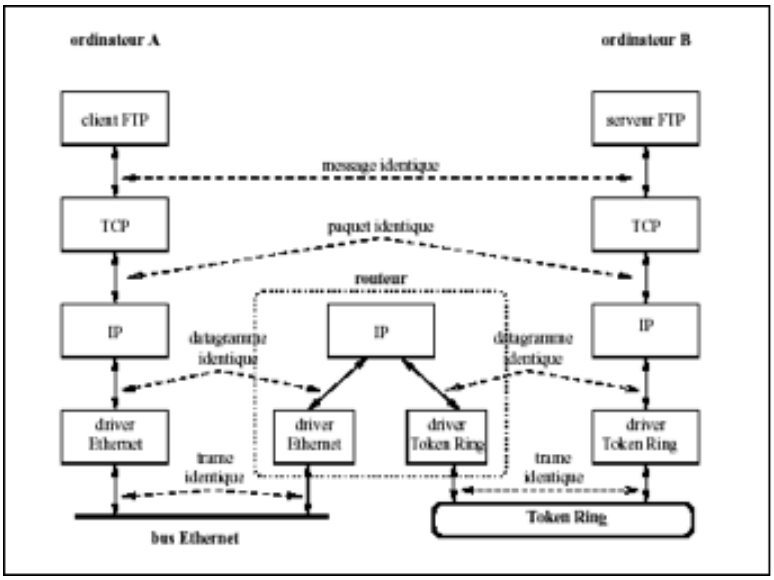


- **La couche de liens** est l'interface avec le réseau et est constituée d'un driver du système d'exploitation et d'une carte d'interface de l'ordinateur avec le réseau (carte réseau, modem,..).
- **La couche réseau** ou couche IP (Internet Protocol) gère la circulation des paquets à travers le réseau en assurant leur routage. Elle comprend aussi les protocoles ICMP (Internet Control Message Protocol) et IGMP (Internet Group Management Protocol)
- **La couche transport** assure tout d'abord une communication de bout en bout en faisant abstraction des machines intermédiaires entre l'émetteur et le destinataire. Elle s'occupe de réguler le flux de données et assure un transport fiable (données transmises sans erreur et reçues dans l'ordre de leur émission) dans le cas de TCP (Transmission Control Protocol) ou non fiable dans le cas de UDP (User Datagram Protocol). Pour UDP, il n'est pas garanti qu'un paquet (appelé dans ce cas datagramme) arrive à bon port, c'est à la couche application de s'en assurer.
- **La couche application** est celle des programmes utilisateurs comme telnet (connexion à un ordinateur distant), FTP (File Transfert Protocol), SMTP (Simple Mail Transfert Protocol), etc...

Cette architecture et ces différents protocoles permettent de faire fonctionner un réseau local, par exemple sur un bus Ethernet reliant un ordinateur client A qui interroge un serveur FTP B :



Mais, ceci permet surtout de constituer un Internet, c'est-à-dire une interconnexion de réseaux éventuellement hétérogènes :

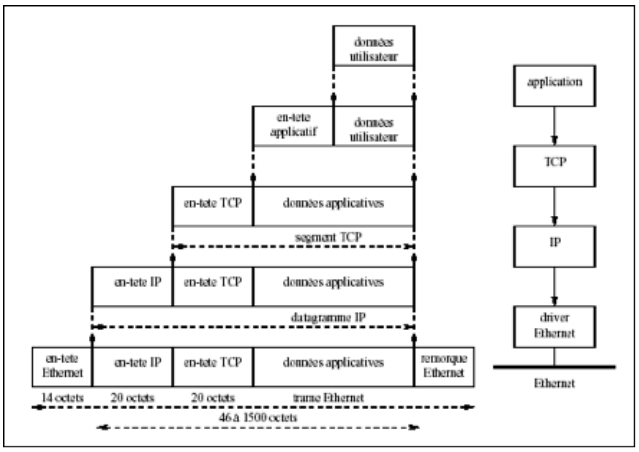


Les ordinateurs A et B sont des systèmes terminaux et le routeur est un système intermédiaire. Comme on peut le voir, la remise du datagramme nécessite l'utilisation de deux trames différentes, l'une du réseau Ethernet entre la machine A et le routeur, l'autre du réseau Token-Ring entre le routeur et la machine B. Par opposition, le principe de

structuration en couches indique que le paquet reçu par la couche transport de la machine B est identique à celui émis par la couche transport de la machine A.

Lorsqu'une application envoie des données à l'aide de TCP/IP les données traversent de haut en bas chaque couche jusqu'à aboutir au support physique où elles sont alors émises sous forme se suite de bits. Chaque couche ajoute aux données reçues de la couche supérieur des informations appelées "Entête" avant de les transférer à la couche inférieure. Cette entête permet à cette couche d'accomplir son rôle.

A la réception, chaque couche retire l'entête des données avant de les transmettre à la couche supérieur



Chapitre 2

Couche physique

Le rôle de la couche physique est de transformer une suite de bits en signaux (et inversement) pour les adapter au canal de communication et les transmettre d'une machine à une autre. Les bits transformés représentent des informations numérisées (codées) tel que le code ASCII pour les textes, avi pour le multimédia, ...etc.

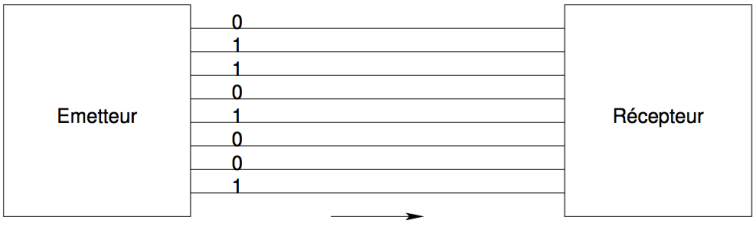
La couche physique détermine la façon selon laquelle les bits sont transportés sur le support physique. Elle permet d'introduire les bits 0 et 1 sur le support sous une forme spécifique, reconnaissable par le récepteur. Plusieurs composants sont utilisés dans cette couche, comme les modems, multiplexeurs, concentrateurs, etc. Ce chapitre étudie les supports de transmission et leurs caractéristiques ainsi que les méthodes utilisées pour transmettre l'information sur ces supports.

2.1 Modes de transmission

Les blocs d'informations transmis sur des fils peuvent l'être en parallèle ou en série.

2.1.1 Transmission en parallèle

Dans la transmission parallèle, les bits d'une même entité (octet, mot, ...) sont envoyés sur des fils distincts pour arriver ensemble à destination. On peut avoir 8, 16, 32 ou 64 fils parallèles.



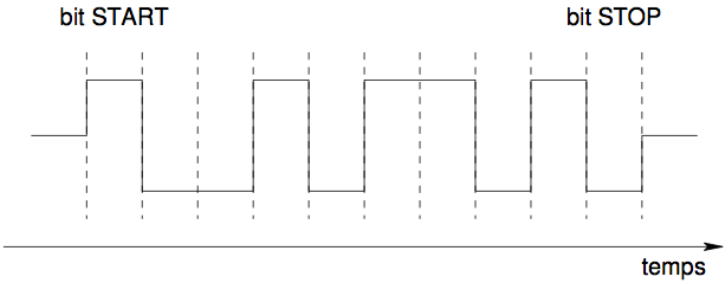
La transmission parallèle pose des problèmes de synchronisation à cause des déphasages possibles entre les différents fils. C'est pour cette raison que ce mode n'est utilisé que sur de très courtes distances tel que le bus d'un ordinateur.

2.1.2 Transmission en série

Dans ce mode de transmission, les bits sont émis les uns après les autres. C'est le mode utilisé dans la réseaux informatiques, il peut être asynchrone ou synchrone.

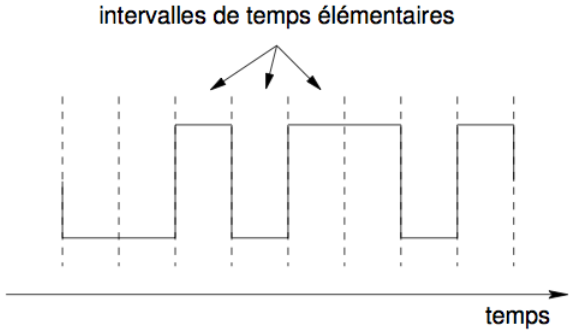
2.1.2.1 Transmission asynchrone

La transmission peut être effectuée n'importe quand, et ne dépend pas d'intervalles de temps précis. Le récepteur commence la réception à l'arrivée d'un bit START et la conclue à l'arrivée d'un bit STOP



2.1.2.2 Transmission synchrone

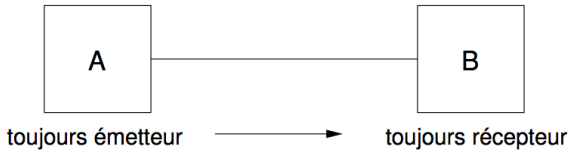
Dans la transmission synchrone, l'émetteur et récepteur sont d'accord sur un intervalle de temps élémentaire constant qui se répète sans cesse. L'émetteur transmet en début d'intervalle pour une durée d'un intervalle par information (ex : 1 bit)



Ce mode est utilisé pour les très hauts débits

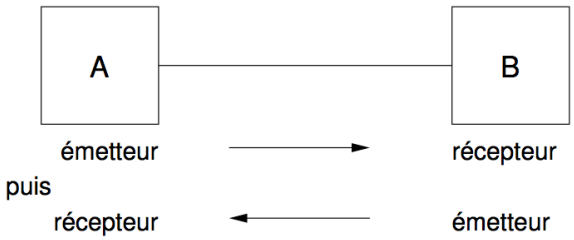
2.1.3 Transmission en simplexe

Dans certains cas d'échange d'information une partie est toujours émettrice et l'autre est toujours réceptrice. Les données circulent toujours dans le même sens. L'exploitation du canal de transmission est appelée dans ce cas en simplexe.



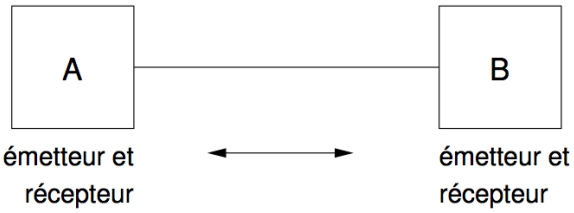
2.1.4 Transmission en half duplex

Dans la transmission en semi-duplex (half-duplex), le canal est exploité à l'alternat pour l'émission : les deux parties émettent tous les deux mais pas en même temps.



2.1.5 Transmission en full duplex

La transmission en full-duplex est bidirectionnelle simultanée. Cela est possible en partageant la bande passante et affecter une partie pour un sens et l'autre pour l'autre sens.



2.2 Signal transmis

Le signal est le véhicule d'information entre deux équipements. Il se propage dans un canal (liaison), matériel ou immatériel sous forme d'onde électromagnétique ou lumineuse. Le signal est une forme ondulatoire résultant de la propagation d'un phénomène vibratoire. Selon la grandeur physique que l'on fait varier, trois types d'ondes sont utilisées :

– ondes électriques (câbles, fils, ...),

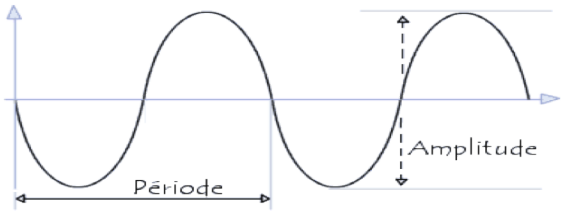
– ondes radio (faisceau hertzien, satellite),

– ondes lumineuses (fibres optiques, infrarouge).

Dans le cas le plus simple une onde est exprimée par une sinusoïde :

$$y(t) = Asin(2\pi ft + \varphi)\,;$$

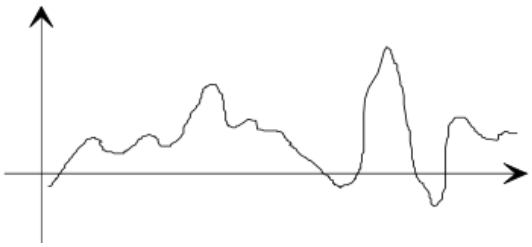
Où A est l'amplitude, f la fréquence et φ la phase.



Les signaux peuvent être de forme analogique ou numérique, les signaux analogiques sont utilisés généralement pour les longues distances, et les signaux numériques pour les courtes distances.

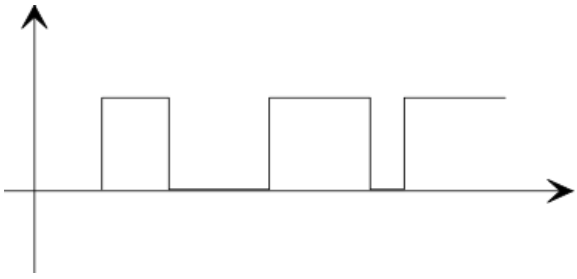
2.2.1 Signal analogique

Un signal analogique est caractérisé par une variation continue, les niveaux de valeurs sont proportionnels aux valeurs de l'information (son, image).



2.2.2 Signal numérique

Le signal numérique est caractérisé par une forme carrée, une variation discontinue et un faible nombre de niveaux de valeurs fixés.



2.3 Caractéristiques d'une ligne de communication

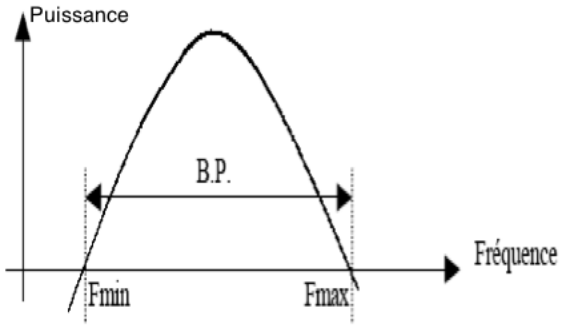
Certaines caractéristiques physiques des supports perturbent la transmission. La connaissance de ces caractéristiques (la bande passante, la sensibilité aux bruits, les limites des débits possibles) est donc nécessaire pour fabriquer de bons signaux, c'est-à-dire les mieux adaptés aux supports utilisés.

2.3.1 La bande passante

La bande passante d'une voie est la plage de fréquence sur laquelle la voie est capable de transmettre des signaux sans que leur affaiblissement soit trop important. Elle est définie par :

$$W = f_{max} - f_{min}$$

Où f_{min} est la fréquence transmise la plus basse et f_{max} la plus haute.



Lorsqu'on parle de la bande passante, on indique une largeur d'intervalle sans préciser les bornes de cet intervalle. Par exemple, la largeur de bande de la ligne téléphonique est 3100Hz.

2.3.2 Rapidité de modulation

La rapidité de modulation R, exprimée en *bauds*, indique le nombre de symboles transmis par unité de temps. Si Δ représente la durée (en secondes) de l'intervalle de temps séparant deux valeurs significatives du signal, alors :

$$R = \frac{1}{\Delta}\ bauds$$

Pour un support de transmission, la rapidité de modulation maximale dépend de sa bande passante (critère de Nyquist). La rapidité de modulation maximale R_{max} est égale au double de la fréquence la plus élevée disponible sur le support :

$$R_{max} = 2F_{max}$$

2.3.3 Taux d'erreur

Il représente la probabilité de perte ou d'altération d'une information (1 bit). On peut la mesurer en calculant pendant un temps significatif le rapport du nombre de bits erronés sur le nombre de bits émis.

2.3.4 Débit binaire

Le débit binaire D est le nombre de bit transmis par unité de temps. Par exemple 512 Kbits/s ou 1 Gigabit/s.

La relation liant la rapidité de modulation au débit binaire est exprimé par la formule :

$$D = R \times log_2(V)$$

Où V désigne la *valence* du signal représentant le nombre des états significatifs que peut prendre le signal.

Une valence de valeur V permet le transports de $P(bits) = log_2(V)$ à chaque baud. Par exemple, pour des modulations simples (des signaux de valence 2) chaque intervalle Δ transporte 1 bit. Les valeurs numériques du débit binaire et de la rapidité de modulation sont alors égales ($R = D$).

Exercice : Si la durée d'un bit est 20ms, quel est le débit binaire ?

2.3.5 Délai de propagation T_p

C'est le temps nécessaire à un signal pour parcourir un support d'un point à un autre. Ce temps dépend de la nature du support, de la distance, de la fréquence du signal,...etc.

2.4 Supports de transmission

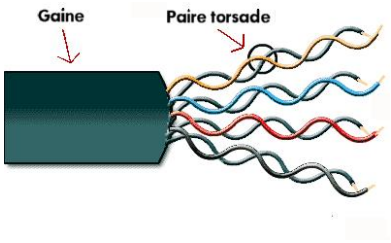
Les supports de transmission sont nombreux et se divisent en deux familles : les supports à guide physique et les supports sans guide physique. Les supports à guide physique, comme les paires torsadées et les câbles coaxiaux, sont les plus anciens, les plus largement utilisés et servent à transmettre des courants électriques. Les supports de verre ou de plastique, comme les fibres optiques, transmettent de la lumière, tandis que les supports sans guide physique des communications sans fil transmettent des ondes électromagnétiques et sont en plein essor.

2.4.1 Supports à guide physique

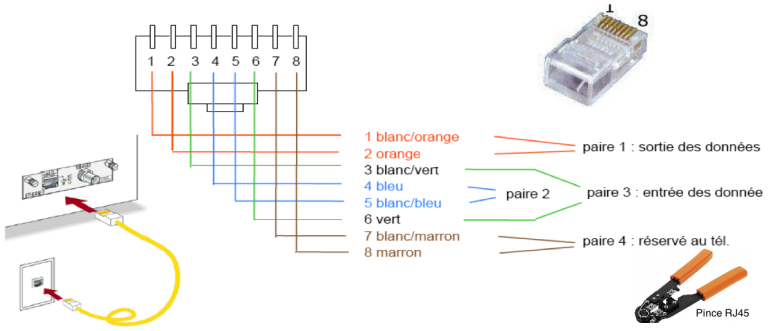
C'est des supports qui utilisent les câbles de différents types pour transmettre l'information.

2.4.1.1 Paires torsadées

La paire torsadée ou enroulée (twisted) est constituée de deux conducteurs identiques torsadés. L'enroulement réduit les conséquences des parasites provenant de l'environnement. L'utilisation la plus courante de la paire torsadée est le raccordement des usagers au central téléphonique (norme RJ11 : Registered Jack). Les réseaux locaux informatiques, où les distances se limitent à quelques kilomètres, utilisent la norme RJ45 utilisant des câbles contenant 4 paires torsadées.



Le raccordement des câbles RJ45 se fait à travers les connecteurs RJ45 permettant de connecter les fils selon le schéma suivant :



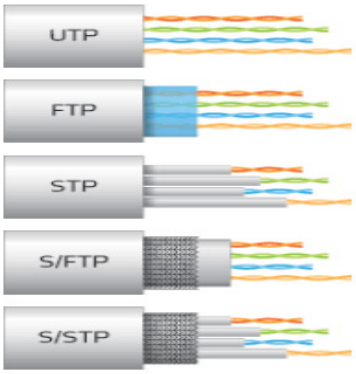
La fabrication manuelle des câbles RJ45 se fait par un pince spéciale appelé "pince RJ45".

Le principal inconvénient des paires torsadées est l'affaiblissement des courants transmis. Elles utilisent souvent, à intervalles réguliers, des éléments appelés répéteurs qui régénèrent les signaux transmis.

Pour les réseaux locaux d'entreprise, la paire torsadée peut suffire. Ses avantages sont nombreux : technique maitrisée, facilité de connexion et d'ajout de nouveaux équipements,

faible coût ainsi qu'elle peut être utilisée en point à point ou en diffusion. Il existe, généralement trois types de câbles :

- UTP (Unshielded Twisted Pairs) : câble à paires torsadées non blindées et non écrantées. Parfois utilisé pour la téléphonie, pas recommandé pour l'informatique.
- FTP (Foiled Twisted Pairs) : paires torsadées entourées dans leur ensemble d'une feuille d'aluminium (écran). C'est le type standard.
- STP (Shielded Twisted Pairs) : paires torsadées entourées chacune par une feuille d'aluminium.
- SFTP (Shielded Foiled Twisted Pairs) et SSTP (Shielded Shielded Twisted Pairs) : câbles FTP ou STP blindés. A utiliser dans les locaux avec fortes perturbations électromagnétiques.

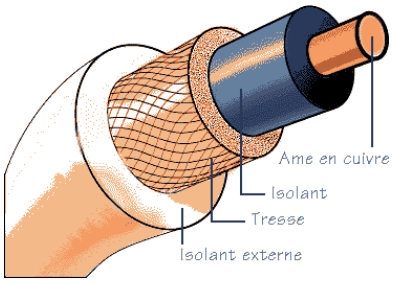


Les câbles à apires torsadées sont normalisés en catégories de Cat1 à Cat7, Les plus utilisées actuellement sont :

- Catégorie 3 : Bande passante 16MHz, utilisée pour la téléphonie.
- Catégorie 5 : Bande passante 100MHz, Débit 100MB/s sur 100m utilisée pour la téléphonie et les réseaux
- Catégorie 6 : Bande passante 250MHz, Débit GB/s sur 100m utilisée pour les réseaux
- Catégorie 6a : Bande passante 500MHz, Débit 10GB/s sur 100m
- Catégorie 7 : Bande passante 600Mhz, Débit 10GB/s

2.4.1.2 Câble coaxial

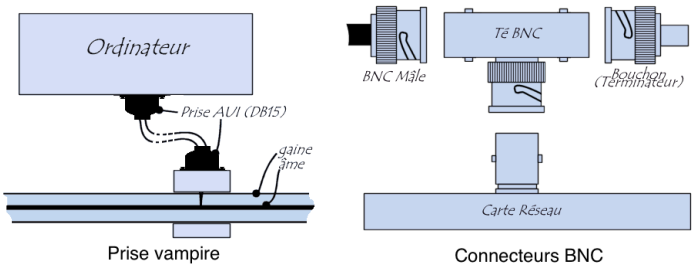
Le câble coaxial est formé de deux conducteurs cylindriques de même axe séparés par un isolant, le tout étant protégé par une gaine plastique.



Il esiste deux types de câble coaxial :

- Le câble 75 Ω, dit "large bande" (broadband) utilisé pour la transmission analogique : c'est le câble de télévision !
- le câble 50 Ω, dit "bande de base" (baseband) généralement utilisé pour transmettre des signaux numériques. Il permet une bande passante de quelques centaines de MHz et des débits allant jusqu'à 2Gbit/s.

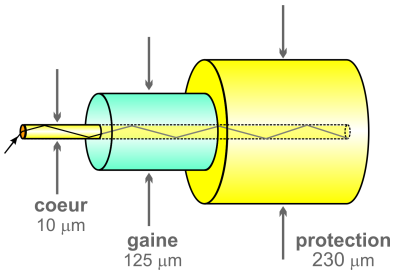
Le câble coaxial est raccordé par des prises vampire pour les gros câbles et les fiches BNC (British Naval Connector) pour les câbles fins.



Le câble coaxial est d'une qualité de transmission et débits meilleures que les paires torsadées et peut être utilisé en point à point ou en diffusion. Cependant, il est un peu plus cher.

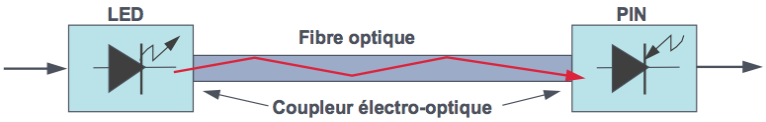
2.4.1.3 Fibre optique

Une fibre optique est constituée d'un fil de verre très fin. Elle comprend un cœur, dans lequel se propage la lumière émise par une diode électroluminescente ou une source laser, et une gaine optique dont l'indice de réfraction garantit que le signal lumineux reste dans la fibre.



Un système de transmission par fibre optique met en œuvre :

- un émetteur de lumière (transmetteur), constitué d'une diode électroluminescente (LED, Light Emitting Diode) ou d'une diode LASER (Light Amplification by Stimulated Emission of Radiation), qui transforme les impulsions électriques en impulsions lumineuses ;
- un récepteur de lumière, constitué d'une photodiode de type PIN (Positive Intrinsic Negative) qui traduit les impulsions lumineuses en signaux électriques ;
- une fibre optique.

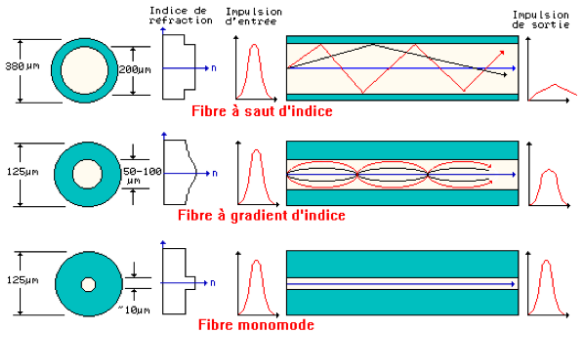


La fibre étant un système de transmission unidirectionnel, une liaison optique nécessite l'utilisation de 2 fibres.

Il existe trois types de fibre optique.

1. Fibre multimode à saut d'indice : le cœur d'indice de réfraction n_1 est entouré d'une gaine d'indice n_2. La variation d'indice entre le cœur et la gaine est brutale (saut d'indice). La propagation s'y fait par réflexion totale à l'interface cœur/gaine. Le diamètre du cœur est important ce qui lui permet d'admettre plusieurs rayons qui se propagent sur des chemins différents ou modes de propagation. La porté des rayons étant de 10 km.
2. Fibre multimode à gradient d'indice : dans ce type, l'indice du cœur décroit de façon continue, depuis le centre du cœur jusqu'à l'interface cœur/gaine suivant une loi parabolique. Tous les rayons sont focalisés au centre de la fibre, ils ont une trajectoire proche de la sinusoïde. La dispersion étant réduite ce qui autorise des portées d'environ 50 km.
3. Fibre monomode : le diamètre du cœur est réduit à 8 μm. Cette réduction, peut être telle que, pour une longueur d'onde donnée, la fibre n'admette plus qu'un seul rayon.

La fibre est alors dite monomode et la distance franchissable est de l'ordre de 100 km.



Le raccordement de la fibre optique utilise des connecteurs de types SC (Subscriber Connector), ST (Straight Tip), FC (Fiber Connector), LC (Lucent Connector).

Malgré que la fibre optique ne permet que les connexion en point à point, ses avantages sont nombreux :

- Débits allant jusqu'à 50 GBit/s (débit théorique 50 TBit/s),
- Transmission simultanée de très nombreux canaux de télévision, de téléphone,...
- Insensible aux parasites électromagnétiques,
- Diamètre extérieure est de l'ordre de 0,1 mm,
- Poids de quelques grammes au kilomètre.
- Difficile à pirater.

2.4.2 Supports sans guide physique

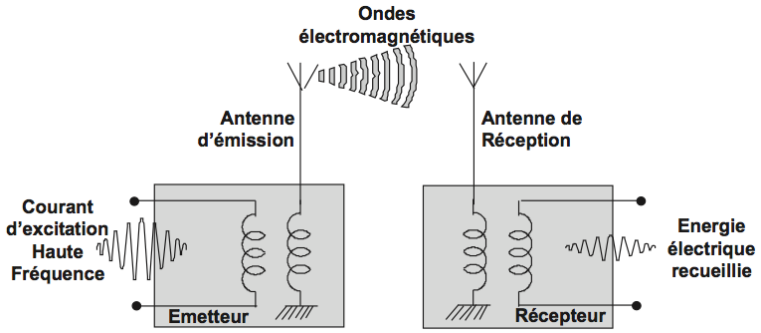
Les supports sans guide physique transmettent des ondes électromagnétiques ou la lumière.

2.4.2.1 Ondes électromagnétiques

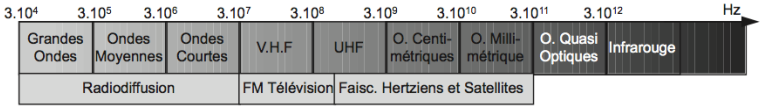
Les ondes électromagnétiques se propagent dans l'atmosphère. L'absence de support matériel apporte une certaine souplesse et convient aux applications comme la téléphonie ou les télécommunications mobiles, sans nécessiter la pose coûteuse de câbles.

Une antenne d'émission rayonne une énergie (onde électromagnétique). Cette énergie

électromagnétique recueillie par un autre conducteur distant ou antenne de réception est transformée en un courant électrique similaire à celui d'excitation de l'antenne d'émission.



Chaque type de liaison ou d'application utilise des bandes de fréquences différentes. L'espace de fréquences utilisables est limité et géré par des organismes nationaux et internationaux. La figure suivante décrit l'utilisation des différents plages de fréquences.



Les hautes fréquences (faisceaux hertziens) sont utilisées pour franchir de grandes distances tandis que les basses (ondes radioélectriques) pour atteindre des récepteurs géographiquement dispersés.

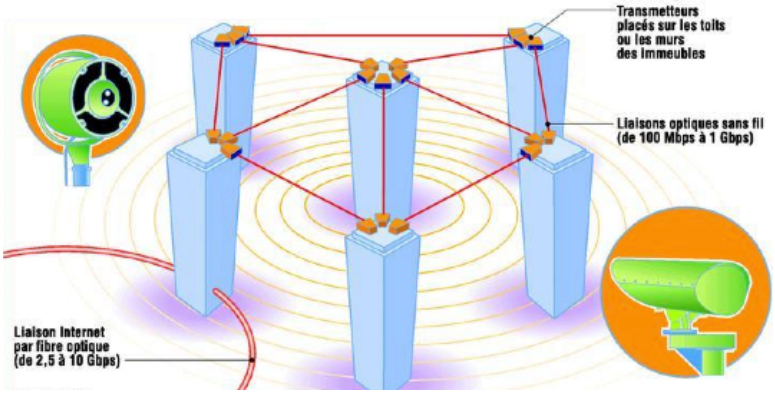
2.4.2.1.1 Faisceaux hertziens Les faisceaux hertziens reposent sur l'utilisation de fréquences très élevées (de 2 GHz à 15 GHz et jusqu'à 40 GHz) et de faisceaux directifs produits par des antennes directionnelles qui émettent dans une direction donnée. La propagation des ondes est limitée à l'horizon optique ; la transmission se fait entre des stations placées en hauteur, par exemple sur une tour ou au sommet d'une colline, pour éviter les obstacles dus aux constructions environnantes. Les faisceaux hertziens s'utilisent pour la transmission par satellite, pour celle des chaînes de télévision ou pour constituer des artères de transmission longue distance dans les réseaux téléphoniques.

2.4.2.1.2 Ondes radioélectriques Les ondes radioélectriques correspondent à des fréquences comprises entre 10 kHz et 2 GHz. Un émetteur diffuse ces ondes captées par des récepteurs dispersés géographiquement. Contrairement aux faisceaux hertziens, il n'est pas nécessaire d'avoir une visibilité directe entre émetteur et récepteur, car celui-ci utilise l'ensemble des ondes réfléchies et diffractées. En revanche, la qualité de la transmission est

moindre car les interférences sont nombreuses et la puissance d'émission beaucoup plus faible.

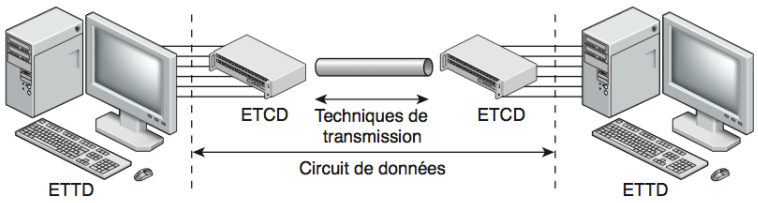
2.4.2.2 Ondes lumineuses

Les liaisons infrarouges et lasers constituent un cas particulier des liaisons hertziennes. Elles sont généralement utilisées, pour interconnecter deux réseaux privés, sur de courtes distances, de l'ordre de quelques centaines de mètres. Elle utilisent des technologies comparables à celles des fibres optiques, mais au lieu d'emprunter un canal en verre, les données prennent la voie des airs à un très hauts débits pouvant dépasse 1 GBit/s. Le signal est numérisé et transmis par un rayon infrarouge ou Laser dans une ligne de visée précise. Le plus souvent, ces liaisons s'effectuent entre des transmetteurs installés au sommets d'immeubles et communiquant en point à point par le biais de faisceaux.



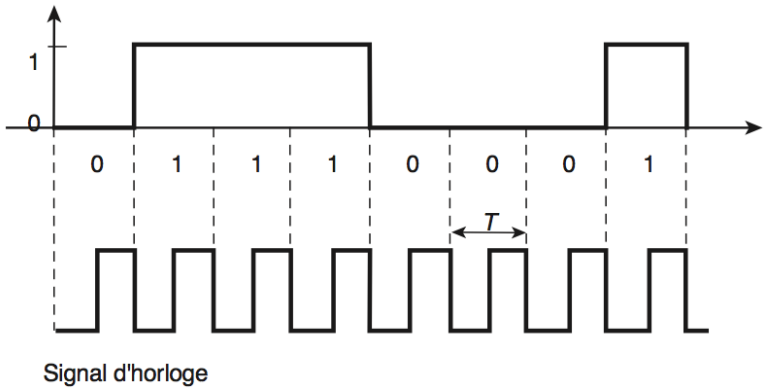
2.5 Codage de l'information

Pour transmettre les données, un équipement spécifique est placé à chaque extrémiste du support : soit un modem (modulateur-démodulateur), soit un codec (codeur-décodeur). Cet équipement assure la fabrication des signaux en émission et leur récupération en réception. Pour émettre les données, le modem reçoit la suite de données binaires à transmettre et fournit un signal dont les caractéristiques sont adaptées au support de transmission. Inversement, en réception, le modem extrait la suite des données binaires du signal reçu. Le support de transmission est ainsi transparent à l'utilisateur. Le support de transmission et les deux modems placés à chacune de ses extrémités constituent un ensemble appelé circuit de données.



L'ISO et l'ITU (Union International des Télécommunications) ont attribué des appellations génériques normalisées aux différents éléments de ce système. Ainsi, le modem et le codec s'appellent des ETCD (équipement de terminaison du circuit de données) et l'ordinateur s'appelle ETTD (équipement terminal de traitement des données).

L'ETTD émetteur fournit à l'ETCD, régulièrement dans le temps, les données à transmettre. L'ETCD les émet sous forme d'un signal à deux valeurs (correspondant à 0 et 1), appelé message de données synchrone.



Les intervalles de temps alloués à chaque symbole sont égaux et coïncident avec les périodes successives d'une base de temps (ou horloge) indispensable à l'interprétation du message de données.

Si la distance entre les deux ETCDs le permet, le signal numérique est transmis directement, la transmission est appelée dans ce cas *bande de base* c'est-à-dire dans la même bande du signal original. Dans le cas contraire, le signal est modulé et la transmission est appelée en *large bande* ou en *bande transposée*.

2.5.1 Transmission numérique (en bande de base)

Lorsque la longueur de la liaison ne dépasse pas quelques centaines de mètres, les informations peuvent être transmises sur le support de liaison sans transformation du signal numérique en signal analogique.

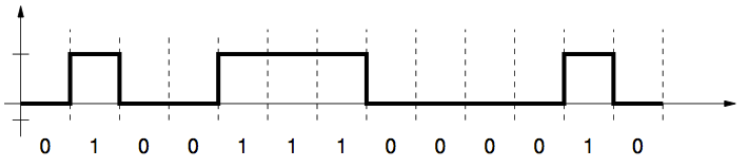
La transmission en bande de base rencontrée principalement dans les réseaux locaux

permet d'obtenir des circuits de données à grand débit et faible portée (débits supérieurs à 1 Mbit/s pour des distances inférieures à 1 Km) en utilisant directement des supports physiques de types métallique (paires torsadées ou câble coaxiaux) ou optique avec éventuellement l'adjonction de répéteurs disposés sur des intervalles allant de 500 mètres à quelques kilomètres.

La transmission de longues suites de 0 ou de 1 (silences) peut rendre difficile la la récupération de l'horloge causer, par conséquent, la perte de la synchronisation entre l'émetteur et le récepteur. Plusieurs types de codage sont utilisés pour introduire des changements d'état fréquents sur le signal pour éviter les silences.

2.5.1.1 Codage unipolaire

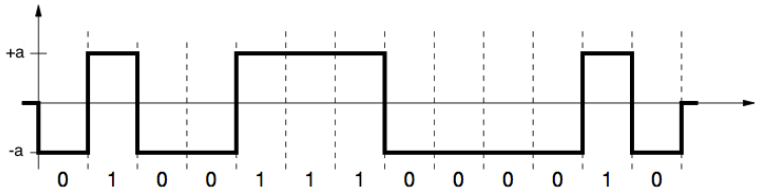
Le signal est transmis sans le moindre changement.



Le problème de ce codage est qu'il ne permet pas de distinguer le cas de 0 du cas d'absence d'information.

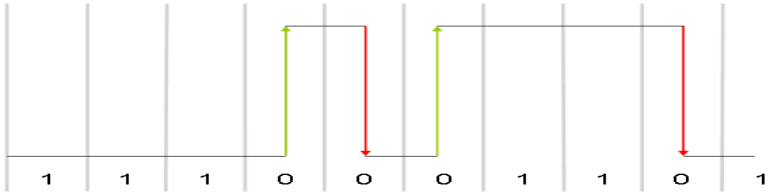
2.5.1.2 Codage NRZ

Pour éviter la valeur nulle, le codage NRZ(No return to zero) utilise une valeur $+a$ du signal pour représenter un 1 et $-a$ pour un 0.



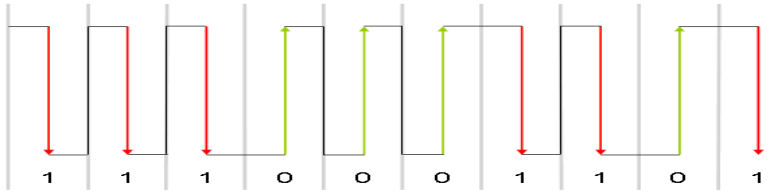
2.5.1.3 Codage NRZI

Le code NRZI (No Return to Zero Inverted) présente les mêmes caractéristiques mais pour éviter les successions de 0, le signal reste dans le même état pour coder un 1 et change d'état pour coder un 0.



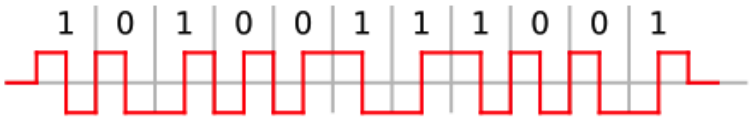
2.5.1.4 Code biphase ou code Manchester

Une opération XOR (OU exclusif) est réalisée entre l'horloge et les données, d'où une transition systématique au milieu de chaque bit du signal binaire.



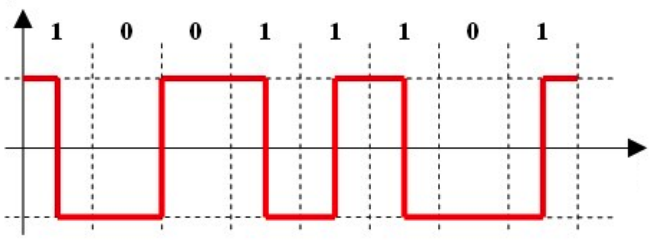
2.5.1.5 Code Manchester différentiel

Une transition systématique est réalisée au milieu de chaque bit. Pas de transition pour coder un bit à 1, une transition pour coder un bit à 0



2.5.1.6 Code Miller

Une transition au milieu du bit pour un 1, pas de transition en milieu de bit pour un 0. Une transition à la fin du bit pour un 0 si le bit suivant est aussi un 0.



2.5.2 Modulation (large bande)

Les techniques en bande de base ne sont pas fiables dès que la distance dépasse quelques centaines de mètres. Pour avoir un signal que l'on puisse récupérer correctement, il faut lui

donner une forme spéciale (sinusoïdale) en le modulant. La transmission par modulation consiste à envoyer une onde sinusoïdale appelée porteuse. Le fait de n'avoir plus de fronts montants ni descendants protège beaucoup mieux le signal des dégradations occasionnées par la distance parcourue par le signal dans le câble puisque le signal est continu et non plus discret. Les opérations de modulation en émission et de démodulation en réception sont réalisées par l'ETCD couramment appelé modem (modulateur-démodulateur).

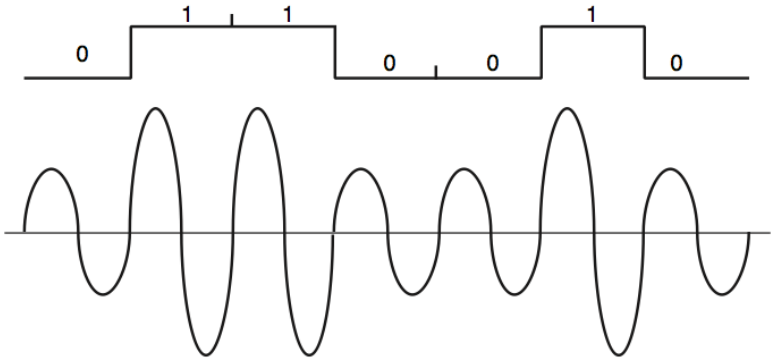
En fonction de la donnée à transmettre, le modem modifie l'un des paramètres de la porteuse (fréquence, phase ou amplitude). On distingue les trois grandes catégories de modulation suivantes :

- modulation d'amplitude, ou ASK (Amplitude-Shift Keying) ;
- modulation de phase, ou PSK (Phase-Shift Keying) ;
- modulation de fréquence, ou FSK (Frequency Shift Keying).

On utilise, souvent, des modulations combinées des trois types précédents.

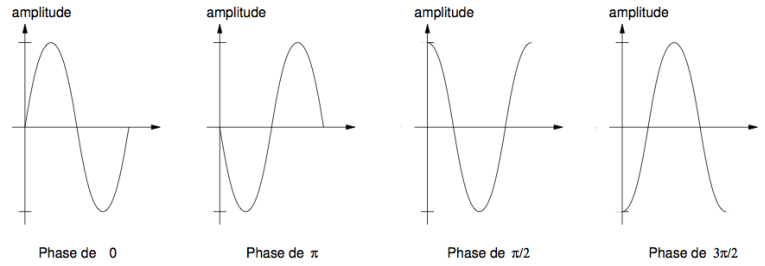
2.5.2.1 ASK (Amplitude-Shift Keying)

Dans la modulation d'amplitude, la distinction entre le 0 et le 1 est obtenue par une différence d'amplitude du signal.

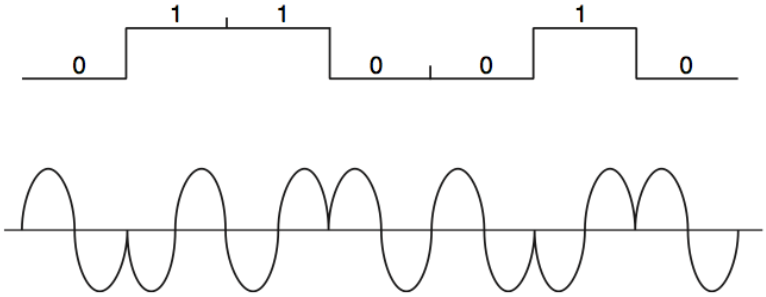


2.5.2.2 PSK (Phase-Shift Keying)

Pour la modulation de phase, la distinction entre 0 et 1 est effectuée par un signal qui commence à des emplacements différents de la sinusoïde, appelés phases.

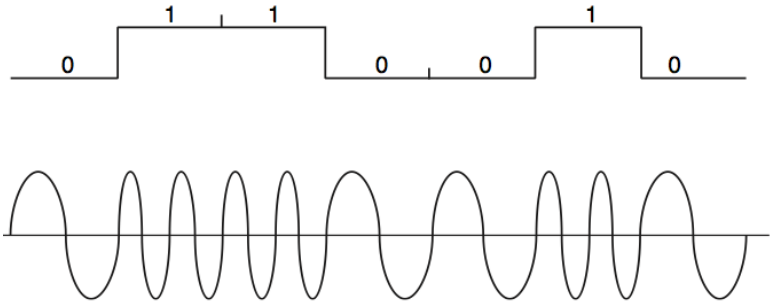


A la figure suivante, les valeurs 0 et 1 sont représentées par des phases respectives de 0 et de π.



2.5.2.3 FSK (Frequency Shift Keying)

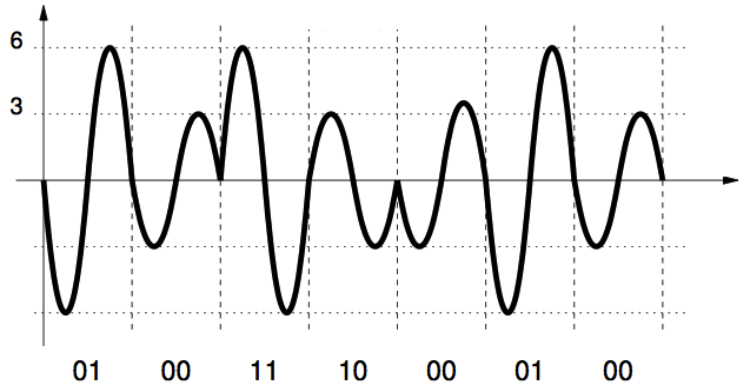
En modulation de fréquence, l'émetteur a la possibilité de modifier la fréquence d'envoi des signaux suivant que l'élément binaire à émettre est 0 ou 1.



2.5.2.4 Modulation de phase et d'amplitude (PSK + AM)

Pour obtenir des vitesses de transmission encore plus élevées dans une modulation de type PSK, il est nécessaire de multiplier le nombre d'états de phase (couramment 4, 8, 16 états ou plus). En combinant une modulation de phase à une modulation d'amplitude, on obtient une meilleure répartition des points sur le diagramme spatial et donc une meilleure immunité au bruit. Par exemple, dans la figure suivante, on combine 2 phases et 2 amplitudes :

– 00 : phase de π et amplitude de 3
– 01 : phase de π et amplitude de 6
– 10 : phase de 0 et amplitude de 3
– 11 : phase de 0 et amplitude de 6



2.5.2.5 Transmission ADSL

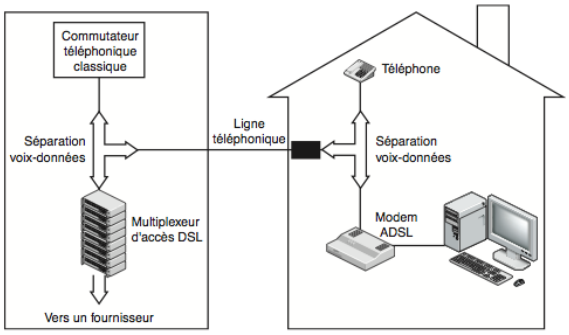
La capacité des lignes téléphoniques en paires torsadées est limitée d'une part par la bande passante, et d'autre part, par le rapport signal/bruit. Toutefois, sur des distances limitées à quelques kilomètres, en améliorant le rapport signal/bruit, il est possible de dépasser les débits de quelques dizaines de kbit/s obtenus avec les modulations précédentes.

La technique utilisée dans l'Asymetric Digital Subscriber Line, permet d'atteindre des débits de plusieurs Mbit/s sur des distances inférieures à 5 km. Cette solution est mise en œuvre pour permettre, entre autres, aux abonnés du réseaux téléphonique commuté RTC (fixe) d'accéder à Internet à des débits élevés. Elle permet de plus, d'assurer une communication téléphonique simultanément aux transferts de données.

Compte tenu des objectifs, les débits dans le sens abonné vers réseau (flux montant ou upstream) sont moins élevés que dans le sens réseau vers abonné (flux descendant ou downstream).

Les valeurs typiques de débit sont de 640 kbit/s et 2 Mbit/s respectivement pour les flux montant et descendant, ce qui correspond à des requêtes sur des serveurs ou des bases de données. Pour obtenir de tels débits, la bande des fréquences utilisées sur les paires téléphoniques va de 0 Hz à 1,1 MHz (pour des lignes supportant de telles fréquences sur des distances courtes). La bande de 0 Hz à 4 kHz est réservée aux communications de type voix analogique. La bande de 64 kHz à 1,1 MHz est utilisée pour la transmission des données en deux bandes distinctes, une pour chaque flux.

Le raccordement, au niveau du réseau et de l'abonné, se fait selon le schéma suivant :



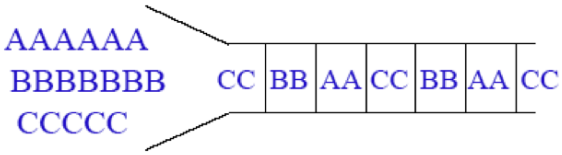
2.6 Multiplexage

Le multiplexage consiste à faire transiter sur une seule et même ligne de liaison, dite voie haute vitesse, des communications appartenant à plusieurs paires d'équipements émetteurs et récepteurs. Chaque émetteur (récepteur) est raccordé à un multiplexeur (démultiplexeur) par une liaison dite voie basse vitesse.

Plusieurs techniques sont possibles :

2.6.1 Multiplexage temporel TDMA (Time Division Multiplexing Access)

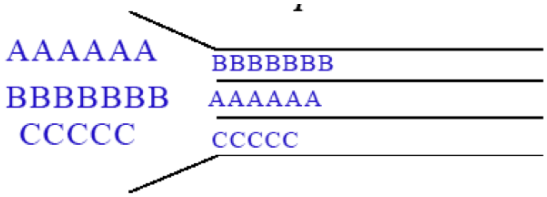
Il partage dans le temps l'utilisation de la voie haute vitesse en l'attribuant successivement aux différentes voies basse vitesse même si celles-ci n'ont rien à émettre. Suivant les techniques chaque intervalle de temps attribué à une voie lui permettra de transmettre 1 ou plusieurs bits.



2.6.2 Multiplexage fréquentiel FDM (Frequency Division Multiplexing)

Il consiste à affecter à chaque voie basse vitesse une bande passante particulière sur la voie haute vitesse en s'assurant qu'aucune bande passante de voie basse vitesse ne se chevauche. Le multiplexeur prend chaque signal de voie basse vitesse et le remet sur la voie haute vitesse dans la plage de fréquences prévues. Ainsi, plusieurs transmissions peuvent être faites simultanément, chacune sur une bande de fréquences particulières, et à l'arrivée

le démultiplexeur est capable de discriminer chaque signal de la voie haute vitesse pour l'aiguiller sur la bonne voie basse vitesse.



2.6.3 Multiplexage statistique ATDM (Asyncronous Time Division Multiplexing)

Il améliore le multiplexage temporel en n'attribuant la voie haute vitesse qu'aux voies basse vitesse qui ont effectivement quelque chose à transmettre. En ne transmettant pas les silences des voies basses, cette technique implantée dans des concentrateurs améliore grandement le débit global des transmissions mais elle fait appel à des protocoles de plus haut niveau et est basée sur des moyennes statistiques des débits de chaque ligne basse vitesse.

2.7 Exercices

Exercice 1 On désire transférer un fichier texte de 320 KOctets d'un ordinateur vers un autre. Chaque caractère du fichier est codé sur 08 bits. La transmission est asynchrone avec un bit Start, un bit Stop et un bit de contrôle sur une ligne d'un débit 9600bits/sec.

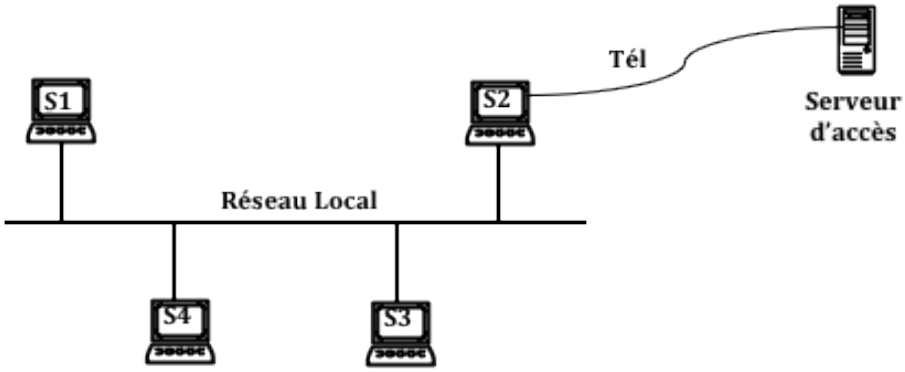
1. Calculer les durées T_1 et T_2 de transfert de ce fichier tel que :
   - durée T_1 : sans tenir compte des bits Start, Stop et de contrôle.
   - durée T_2 : en tenant compte des bits Start, Stop et de Contrôle.
   - Calculer puis Commenter le Rapport R= $\frac{T_2-T_1}{T_2}$
2. Sachant que dans le cas précédent la valence du signal utilisée était de 2. Calculer le délai T3 de transfert total si on passe à une valence du signal égale à 16.

Exercice 2 Une connexion numérique en full-duplex est établie entre 02 points A et B de la terre via un satellite géostationnaire situé à 36000 km de chacun des deux points. Un signal est émis depuis A à raison de 64 Kbits/sec et ou la vitesse de propagation dans l'air est égale à 300000 km/sec. Une fois le début du signal reçu, B retourne un acquittement (réponse).

1. Calculer le temps T1 que mettra le premier bit pour arriver à B.

2. Combien de bits pourront être émis par A avant que ce dernier ne sache que B a bien reçu les premières informations.
3. Sachant que la station A désire envoyer vers B une chaîne d'informations de taille égale à 96Kbits. Calculer le temps T2 total de transfert de cette chaîne.

Exercice 3 Soit le réseau suivant :



Les stations S_1, S_2, S_3, S_4 sont reliées par un réseau local en bus offrant un débit de 10 Mbits/s. La station S2 est reliée à un serveur d'accès internet par une liaison téléphonique dont la bande de fréquence est de [300-3400 Hz].

1. Calculer la capacité de transmission de la liaison téléphonique.
2. Sachant que le débit de la ligne est de 62 Kbits/s :
   - Calculer la valence du signal,
   - Calculer le rapport signal/bruit permettant le bon fonctionnement de la ligne, donner sa valeur en décibels.
3. La station S_1 veut envoyer la suite binaire [1 1 0 0 0 0 0 1 0 1] à la station S_2. Donner la forme du signal émis en utilisant le codage Manchester et Miller.
4. La station S_1 veut envoyer la suite binaire [0 1 0 1 1 0 1 1 0 0] à la station S_2. Donner la forme du signal émis en utilisant le codage Manchester différentiel et Bipolaire.
5. Sachant que le codage du signal sur la ligne téléphonique utilise une modulation à deux phases (0 et 180°) et deux amplitudes (V et 2V) :
   - Donner la valence du signal
   - Donner la forme du signal utilisé pour émettre la série de bits précédente de la station S2 au serveur d'accès Internet.
6. Sachant que le codage du signal sur la ligne téléphonique utilise une modulation à quatre phases (0, 90, 180 et 270°) et deux amplitudes (V et 2V) :

- Donner la valence du signal
- Dessiner un diagramme (cercle des phases et amplitudes) représentant les signaux utilisés et leurs codes correspondant.
- Donner la forme du signal utilisé pour émettre la série de bits [001110111000101011101] de la station S_2 au serveur d'accès Internet.

7. Calculer de débit moyen de transmission entre la station S_1 et le serveur Internet.

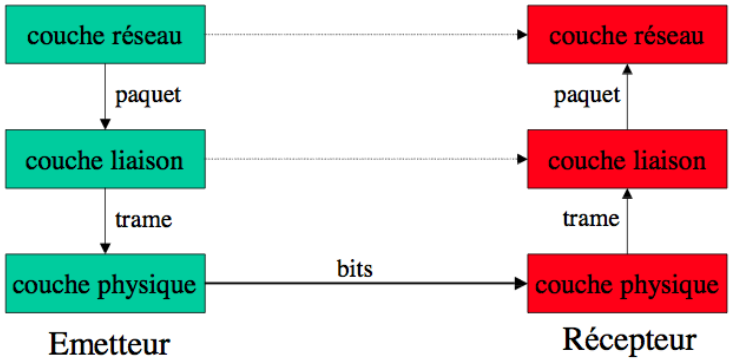
Exercice 4 Quatre terminaux asynchrones sont connectés à un multiplexeur statistique temporel (MPX dynamique) intégrant une mémoire tampon et ayant une vitesse de transmission de 19200 bits/sec. Sachant que le débit d'un des terminaux est de 9600 bits/sec et les autres de 4800 bits/sec chacun, on vous demande de calculer le débit effectif De à la sortie du multiplexeur et la durée d'une trame T_s en étudiant les différent cas possible ou :

1. 02 terminaux sont seulement connectés en même temps.
2. Seulement 03 terminaux sont connectés en même temps.
3. Les 04 terminaux sont connectés en même temps.

Chapitre 3

Couche Liaison de données

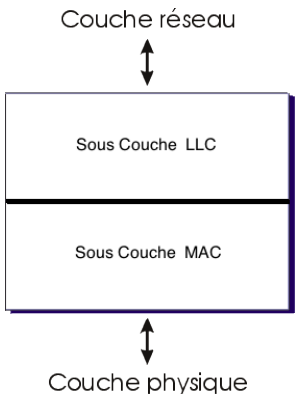
La couche physique permet de transmettre un flot de bits entre deux systèmes distants. La couche liaison (couche n° 2) doit s'assurer de la corrections des bits transmis et les rassembler en paquets pour les passer à la couche Réseaux. La couche liaison récupère des paquets de données de la couche réseau, les enveloppe en des trames qui les envoie une à une à la couche physique.



Pour rendre la transmission fiable, la couche liaison doit assurer :

- La délimitation des blocs de données échangées ;
- Le contrôle de l'intégrité des données reçues ;
- L'organisation et le contrôle de l'échange.
- Le contrôle d'accès à un canal partagé

En fait, la couche liaison se compose de deux sous-couches : LLC (Logical Link Control) et MAC (Media Access Control). La sous-couche LLC Assure les trois premières fonctions tandis que la sous-couche MAC assure la dernière.



3.1 Délimitation de trames

A l'instar des transmissions asynchrones où les bits de start et de stop encadrent les bits d'information, en transmission synchrone une information spéciale permet de repérer le début et la fin des données transmises. Il existe deux méthodes :

3.1.1 Comptage des caractères

On utilise un champ dans l'entête de la trame pour indiquer le nombre de caractères de la trame.

06	'S'	'U'	'P'	'E'	'R'	03	'L'	'E'	06	'C'	'O'	'U'	'R'	'S'

Un problème sérieux peut se poser avec cette méthode si la valeur du champ ajouté est modifiée au cours de la transmission. Généralement, cette méthode est rarement utilisée seule.

3.1.2 Utilisation des fanions

La trame est délimité par une séquence particulière de bits appelée **fanion** ou flag.

Pour garantir le bon fonctionnement de cette méthode, des bits de transparence sont nécessaires pour qu'une séquence binaire dans la trame ne corresponde accidentellement au fanion. Par exemple, si le fanion est l'octet 01111110, un bit de transparence "0" est inséré après toute séquence de cinq 1 successifs dans la trame.

Exemple :

Données :

01011001111110

Trame :

01111110 010110011111010 **01111110**

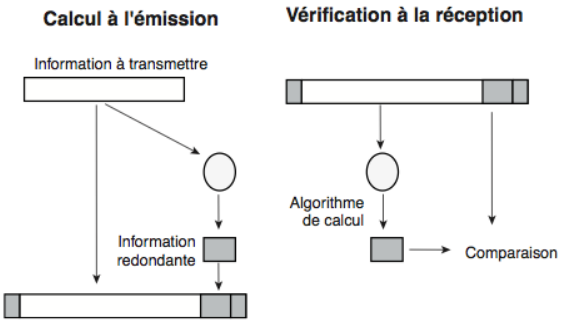
Cette technique est utilisée également en considérant des caractères de délimitation et des caractères de transparence.

L'avantages des fanions est qu'ils permettent de trouver toujours la synchronisation et d'envoyer des trames de tailles quelconques.

3.2 Détection et Correction d'erreurs

D'une manière générale on doit, lors d'une transmission de données, s'assurer que les données reçues n'ont pas été altérées durant la transmission. Plusieurs facteurs peuvent modifier le contenu des données tel que les interférences causées par des rayonnements électromagnétiques ou la distorsion des câbles de transmissions.

Les méthodes de protection exploitent la redondance de données en ajoutant des bits de contrôle aux bits de données. Les bits de contrôle sont calculés, au niveau de l'émetteur, par un algorithme spécifié dans le protocole à partir du bloc de données. À la réception, on exécute le même algorithme pour vérifier si la redondance est cohérente. Si c'est le cas, on considère qu'il n'y a pas d'erreur de transmission et l'information reçue est traitée ; sinon, on est certain que l'information est invalide.



3.2.1 Définitions générales

Un code $C(k, n)$ transforme (code) tout bloc initial de k bits d'information en un bloc codé de n bits. Le code ajoute une redondance puisque $n \geq k$.

$$
\begin{array}{ll}
 & 1\,0\,0\,0\,1\,0\,0\,1 \\
\oplus & 1\,0\,1\,1\,0\,0\,0\,1 \\
\hline
= & 0\,0\,1\,1\,1\,0\,0\,0 \quad \text{Dist(x,y)} = 3
\end{array}
$$

3.2.1.1 Code Systématique

Un code est dit systématique si les k premiers bits du bloc codé sont égaux aux bits du bloc initial. Alors les r $(r = n - k)$ derniers bits forment un champ de contrôle d'erreur.

3.2.1.2 Rendement d'un code

Le rendement R d'un code $C(k, n)$ est donné par le rapport entre le nombre de bits du bloc initial et le nombre de bits du bloc codé : $R = \frac{k}{n}$

3.2.1.3 Mot de code

On appelle mot du code, la suite de n bits obtenue après un codage $C(k, n)$. Le nombre n de bits qui composent un mot du code est appelé la longueur du code. La dimension k étant la longueur initiale des mots.

3.2.1.4 Poids de Hamming

Le poids de Hamming d'un mot est le nombre de bits à 1 qu'il contient. Par exemple le poids de Hamming de la séquence 01110110 est 5.

3.2.1.5 Distance de Hamming d'un code

La distance de Hamming entre deux mots de même longueur est définie par le nombre de positions binaires qui diffèrent entre ces deux mots. On l'obtient par le poids de Hamming de la somme binaire des 2 mots.

La distance de Hamming d'un code est la distance minimum entre tous les mots du code. Soit C un code ;

$$Dist(C) = min\{Dist(x, y) \;\; / \;\; x \in C \wedge y \in C\}$$

3.2.1.6 Capacité d'un code

La capacité de détection (de correction) d'un code est définie par les configurations erronées qu'il est capable de détecter (corriger).

Une erreur simple (resp. double, ou d'ordre p) affecte une seule (resp. 2, ou p) position(s) binaire(s) d'un mot.

Pour qu'un code ait une capacité de détection (resp. correction) des erreurs d'ordre e, il faut que sa distance de Hamming soit supérieure ou égale à $(1 + e)$ (resp. $(1 + 2e)$).

Exemple : Si la distance de Hammind d'un code est égale à 3, sa capacité de détection est de 2, et sa capacité de correction est 1.

Plusieurs méthodes de protection contre les erreurs peuvent être utilisées :

3.2.2 Duplication de données

Un exemple des bits de contrôle est la duplication des bits transmis (détection par répétition). Le message code est un double exemplaire du message initial, le récepteur sait qu'il y a eu erreur si les exemplaires ne sont pas identiques, il demande alors la retransmission du message. Si la même erreur se passe sur les deux exemplaires, l'erreur ne sera pas détectée.

Si on envoie le message en trois exemplaires, le récepteur pourra même corriger l'erreur en prenant les valeurs des deux copies identiques sans demander la retransmission de l'émetteur.

3.2.3 Code de contrôle de parité

C'est un code dans lequel un bit (le bit de parité) est ajouté au mot initial pour assurer la parité. Son rendement est faible lorsque k est petit.

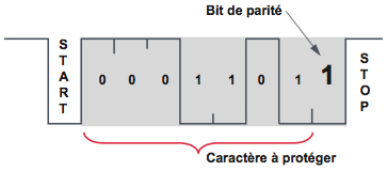
Exemple : Transmission de caractères utilisant un code de représentation (le code ASCII sur 7 bits).

Lettre	Code ASCII	Mot codé (parité paire)	Mode codé (parité impaire)
E	1010001	10100011	10100010
V	0110101	01101010	01101011
A	1000001	10000010	10000011

Ce code est capable de détecter toutes les erreurs en nombre impair mais il ne détecte pas les erreurs en nombre pair. Il permet de détecter une erreur de parité, mais ne permet pas de la localiser.

3.2.3.1 Parité verticale

À chaque caractère on rajoute un bit (bit de redondance verticale ou bit de parité, VRC :Vertical Redondancy Check)



3.2.3.2 Parité longitudinale

A chaque bloc de caractère, on ajoute un champ de contrôle supplémentaire (LRC : Longitudinal Redondancy Check)

Caractère à transmettre	bit de parité	Caractère à transmettre	bit de parité	...	Caractère LRC	bit de parité

La parité longitudinale était initialement utilisée pour les bandes magnétiques pour compléter la détection des erreurs de parité verticale.

3.2.3.3 Parité longitudinale et verticale

Le bloc de données est disposé sous une forme matricielle ($k = a \bullet b$). On applique la parité sur chaque ligne et chaque colonne. On obtient une matrice $(a+1, b+1)$. Un caractère le LRC est ajouté au bloc transmis. Chaque bit du caractère LRC correspond à la parité des bits de chaque caractère de même rang : le premier bit du LRC est la parité de tous les 1^{er} bits de chaque caractère, le second de tous les 2^e bits... Le caractère ainsi constitué est ajouté au message. Le LRC est lui-même protégé par un bit de parité (VRC).

	H	E	L	L	O	*LRC* →
bit 0	0	1	0	0	1	0
bit 1	0	0	0	0	1	1
bit 2	0	1	1	1	1	0
bit 3	1	0	1	1	1	0
bit 4	0	0	0	0	0	0
bit 5	0	0	0	0	0	0
bit 6	1	1	1	1	1	1
VRC ↓	0	1	1	1	1	0

1001000	0	1000101	1	1001100	1	1001100	1	1001111	1	1000010	0
H		E		L		L		O		LRC	

3.2.4 Code de Hamming

Le code de Hamming permet de détecter et de corriger une erreur survenue dans un bloc transmis. Aux d bits de données, on ajoute c bits de contrôle de parité. On a donc $d+c=n$ bits. Puisque les c bits de contrôle doivent indiquer les $n+1$ possibilités d'erreurs (dont l'absence d'erreur, ce qui explique le $+1$), il faut que $2^c \geq n+1$. Les 2^c possibilités de codage sur les c bits servent à coder la position de l'erreur. Dès que cette position est calculée, on peut corriger le bit en erreur.

On numérote les bits de chaque mot de code de droite à gauche à partir de 1, les bits de contrôle sont placés aux positions représentant des puissances de 2 (1,2,4,8,...) et les bits de données sont intercalés.

Exemple :

					1	0	0	1	0	0	0
							+	c_3	c_2	c_1	c_0
=	1	0	0	c_3	1	0	0	c_2	0	c_1	c_0
	11	10	9	8	7	6	5	4	3	2	1

La liste des bits de parité contrôlant un bit donné est fourni par les positions à 1 dans sa représentation binaire. Par exemple :

- le bit numéro $11 = (1011)_2$ est contrôlé par les bits c_3, c_1 et c_0
- le bit numéro $7 = (0111)_2$ est contrôlé par les bits c_2, c_1 et c_0
- le bit numéro $4 = (0100)_2$ est contrôlé par le bits c_2
- ...

Ainsi, la liste des bits contrôlée par chaque bit de parité est :

- c_0 : {1,3,5,7,9,11}
- c_1 : {2,3,6,7,10,11}
- c_2 : {4,5,6,7}
- c_3 : {8,9,10,11}

Dans l'exemple précédent et pour une parité paire, les c_i peuvent être calculé comme suit :

- $c_0 = 0(0+0+0+1+0+1)$
- $c_1 = 0(0+0+0+1+0+1)$
- $c_2 = 1(1+0+0+1)$
- $c_3 = 1(1+0+0+1)$

Et le mot de code envoyé sera donc : 10011001000

À la réception, un mot binaire est construit de longueur c qui peut être déduite à partir de la longueur du mot de code reçu (pour coder 11 position on a besoin de 4 bits). Chaque bit est égal à 1 si le contrôle de parité est OK et 0 sinon. Si le mot est égal à 0, on conclut qu'il n'y a pas eu d'erreur, sinon la valeur du mot représente le numéro du bit erroné.

Par exemple si on reçoit 10011001000, on calcule les c_i :

- $c_0 = 0 + 0 + 0 + 1 + 0 + 1 = 0$
- $c_1 = 0 + 0 + 0 + 1 + 0 + 1 = 0$
- $c_2 = 1 + 0 + 0 + 1 = 0$
- $c_3 = 1 + 0 + 0 + 1 = 0$

On conclut donc que le mot reçu est correct.

Si par contre on reçoit 1$\underline{1}$011001000 on trouve :

- $c_0 = 0 + 0 + 0 + 1 + 0 + 1 = 0$
- $c_1 = 0 + 0 + 0 + 1 + 1 + 1 = 1$
- $c_2 = 1 + 0 + 0 + 1 = 0$
- $c_3 = 1 + 0 + 1 + 1 = 1$

Le mot de contrôle est donc $(1010)_2 = (10)_{10}$, on conclut que le bit numéro 10 est erroné.

Exercice : Le codage de Hamming est utilisé . Un récepteur reçoit : 1110101. Que peut-on en conclure ?

Calcul simplifié du code de Hamming

Coder 10101011001 avec une parité paire : $d = 11$, donc $k = 4$. Le message à transmettre contient donc $n = 15$ bits et est égal :

1	0	1	0	1	0	1	?	1	0	0	?	1	?	?
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Dans le message à transmettre, on a des bits à 1 dans les positions suivantes : 15, 13, 11, 9, 7, 3. On transforme ces positions en leur valeur binaire et on les additionne modulo 2 : On met 1 lorsque l'on a un nombre impair de 1 et 0 pour un nombre pair de 1.

15	=	1	1	1	1
13	=	1	1	0	1
11	=	1	0	1	1
9	=	1	0	0	1
7		0	1	1	1
3	=	0	0	1	1
c_i		0	1	0	0

Le message codé est donc 101010101001100.

Le même procédé peut être fait à la réception pour vérifier le mot reçu.

3.2.5 Codes polynomiaux

La méthode des codes polynômiaux (ou le CRC : Cyclic Redondant Coding) est la méthode la plus utilisée pour détecter des erreurs groupées. Avant la transmission, on ajoute des bits de contrôle. Si des erreurs sont détectées à la réception, il faut retransmettre le message.

Dans ce code, une information de n bits est considérée comme la liste des coefficients binaires d'un polynôme de n termes, donc de degré $n-1$.

Exemple :

- $1101 \rightarrow x^3 + x^2 + 1$
- $110001 \rightarrow x^5 + x^4 + 1$
- $11001011 \rightarrow x^7 + x^6 + x^3 + x + 1$

Pour calculer les bits de contrôle, on effectue un certain nombre d'opérations avec ces polynômes à coefficients binaires. Toutes ces opérations sont effectuées modulo 2. C'est ainsi que, dans les additions et dans les soustractions, on ne tient pas compte de la retenue : Toute addition et toute soustraction sont donc identiques à une opération XOR. Par exemple :

	1	0	0	1	1	0	1	1
+	1	1	0	0	1	0	1	0
=	0	1	0	1	0	0	0	1

	1	1	1	1	0	0	0	0
-	1	0	1	0	0	1	1	0
=	0	1	0	1	0	1	1	0

La source et la destination choisissent un même polynôme $G(x)$ dit générateur car il est utilisé pour générer les bits de contrôle (Checksum).

L'algorithme pour calculer le message à envoyer est le suivant. Soit $M(x)$ le polynôme correspondant au message original, et soit r le degré du polynôme générateur $G(x)$ choisi :

- Multiplier $M(x)$ par x^r, ce qui revient à ajouter r zéros à la fin du message original
- Effectuer la division suivante modulo 2 :

$$\frac{M(x)x^r}{G(x)} = Q(x) + R(x)$$

- Le quotient $Q(x)$ est ignoré. Le reste $R(x)$ (Checksum) contient r bits (degré du reste $r-1$). On effectue alors la soustraction modulo 2 :

$$M(x).x^r - R(x) = T(x)$$

Le polynôme $T(x)$ est le polynôme cyclique : c'est le message prêt à être envoyé. Le polynôme cyclique est un multiple du polynôme générateur $T(x) = Q(x).G(x)$

A la réception, on effectue la division suivante :

$$\frac{T(x)}{G(x)}$$

- Si le reste $= 0$, il n'y a pas d'erreur
- Si le reste $\neq 0$, il y a erreur, donc on doit retransmettre

En choisissant judicieusement $G(x)$, on peut détecter toute erreur sur 1 bit, 2 bits consécutifs, une séquence de n bits et au-delà de n bits avec une très grande probabilité.

Exemple

Soit à transmettre le message 1011011 en utilisant le polynôme générateur $G(x) = x^4 + x + 1$. On procède comme suit pour calculer le message à transmettre

1. message original $= 1011011 \Rightarrow M(x) = x^6 + x^4 + x^3 + x^1 + 1$
2. $G(x) = x^4 + x + 1$
3. $M(x).x^4 = x^10 + x^8 + x^7 + x^5 + x^4$
4. Calculer $R(x)$ par division polynomiale

$$
\begin{array}{llllllllll}
x^{10} & + & x^8 & + & x^7 & + & x^5 & + & x^4 & \\
x^{10} & + & x^7 & + & x^6 & & & & & \\
\hline
x^8 & + & x^6 & + & x^5 & + & x^4 & & & \\
x^8 & + & x^5 & + & x^4 & & & & & \\
\hline
x^6 & & & & & & & & & \\
x^6 & + & x^3 & + & x^2 & & & & & \\
\hline
 & & x^3 & + & x^2 & & & & &
\end{array}
\quad
\begin{array}{|llllll}
x^4 & + & x & + & 1 & \\
\hline
x^6 & + & x^4 & + & x^2 &
\end{array}
$$

5. $R(x) = x^3 + x^2 = (1100)_2$
6. Le message à envoyer $T(x) = M(x).x^r - R(x) = x^10 + x^8 + x^7 + x^5 + x^4 - x^3 - x^2 = (10110111100)_2$

À la réception, un calcul semblable s'effectue sur le mot reçu, mais il faut, ici, que le reste soit nul. Dans le cas contraire, c'est qu'une erreur est survenue en cours de route.

Codes polynomiaux utilisés

Les principaux polynômes générateurs (diviseurs) sont :

- LRCC-8 : $x^8 + 1$
- LRCC-16 : $x^{16} + 1$
- CRC 12 : $x^{12} + x^{11} + x^3 + x^2 + x + 1$
- CRC 16 Forward : $x^{16} + x^{15} + x^2 + 1$
- CRC 16 Backward : $x^{16} + x^{14} + x + 1$
- CRC CITT Forward : $x^{16} + x^{12} + x^5 + 1$
- CRC CITT Backward : $x^{16} + x^{11} + x^4 + 1$

3.2.6 Codes auto-correcteurs

Un code de distance de Hamming α peut :

- détecter toute erreur portant sur $\alpha - 1$ bits
- corriger toute erreur portant sur $\frac{\alpha-1}{2}$ bits

Supposons le code suivant :

Mot naturel	Mot de code
00	10011
01	10100
10	01001
11	01110

La distance de Hamming du code est 3, il peut donc détecter des erreurs sur 2 bits et corriger des erreurs sur un bit.

Par exemple, si on veut transmettre 00(10011) et une erreur survient sur un bit, les possibilité sont :00011, 11011, 10111, 10001, 10010.

Supposons recevoir 11011.On Calcule la distance de Hamming avec tous les mots de code :

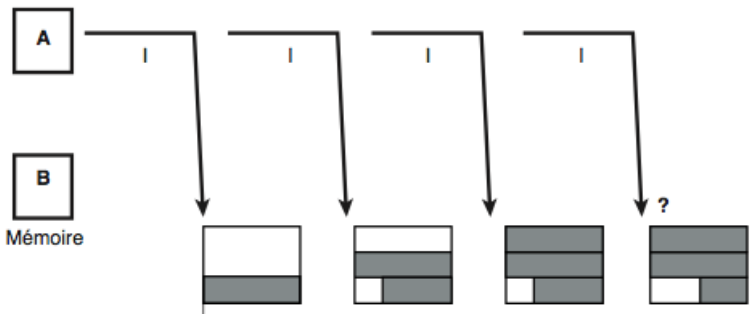
- $D(11011, 10011) = 1$
- $D(11011, 10100) = 4$
- $D(11011, 01001) = 2$
- $D(11011, 01110) = 3$

Le mot correcte est le mot plus proche 10011 c-à-d 00.

Remarquons que si une erreur survient sur 2 bits, le nombre de possibilités augmente et on tombe sur plusieurs mots proches et la décision devient impossible.

3.3 Contrôle de flux

Dans une transmission d'information d'un émetteur A vers un récepteur B, si l'émetteur produit les données à une vitesse nettement supérieure à la vitesse de consommation du récepteur, ce dernier sera engorgé (saturé ou surchargé) et les informations émises seront perdues. Pour résoudre ce problème, on peut penser à doter le récepteur d'une mémoire tampon lui permettant de stoker les messages en attendant leur traitement. On peut constater rapidement que quelque soit la taille de la mémoire utilisée, elle peut être saturée.



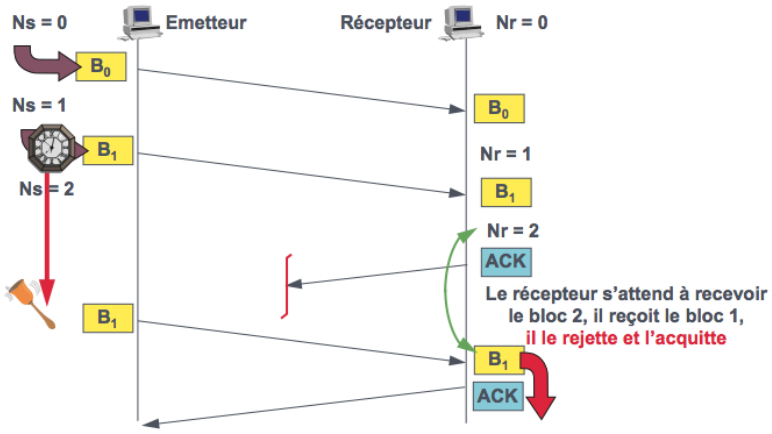
Le contrôle de flux sert à mettre en place un mécanisme de contrôle du rythme d'envoi des informations vers le récepteur. Il peut être réalisé par plusieurs méthodes :

3.3.1 Envoyer et attendre (Sent and Wait)

Après l'envoi d'un bloc d'information, L'émetteur s'arrête dans l'attente d'un accusé de réception. À la réception de l'acquittement, noté ACK pour Acknowledge, l'émetteur envoie le bloc suivant.

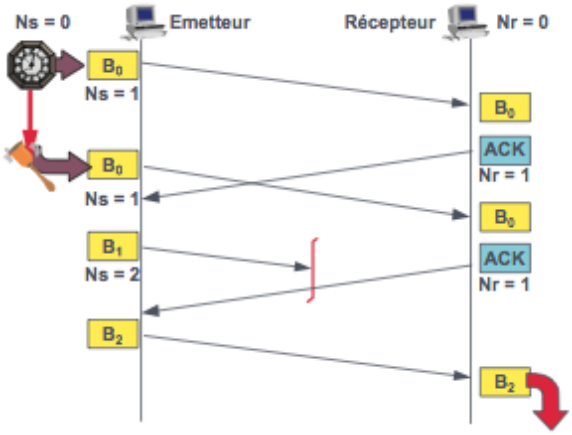
En cas d'erreur de transmission, le bloc reçu est rejeté. Le bloc est dit perdu, il n'est pas acquitté. L'émetteur reste alors en attente. Pour éviter un blocage de la transmission, à l'émission de chaque bloc de données, l'émetteur arme un temporisateur (Timer). À l'échéance du temps imparti (Time Out), si aucun accusé de réception (ACK) n'a été reçu, l'émetteur retransmet le bloc non acquitté.

Une difficulté survient si la perte concerne l'ACK. En effet, bien que les données aient été correctement reçues, l'émetteur les retransmet sur temporisation. Les informations sont ainsi reçues 2 fois. Pour éviter la duplication des données, il est nécessaire d'identifier les blocs. À cet effet, l'émetteur et le récepteur entretiennent des compteurs Ns (Ns, Numéro émis, s pour send) et Nr (Numéro du bloc à recevoir, r pour receive).Les deux compteurs sont initialisés à zéro. Le contenu du compteur Ns est transmis avec le bloc, le récepteur compare ce numéro avec le contenu de son compteur Nr. Si les deux valeurs sont identiques le bloc est réputé valide et accepté. Si les valeurs diffèrent, le bloc reçu n'est pas celui attendu. Il est rejeté et acquitté s'il correspond à un bloc déjà reçu.



Dans les cas où les délais de consommation sont plus importants, les données peuvent ne pas être acquittées à temps. Par exemple, si A transmet un bloc B0 et B se tarde dans son traitement, A va retransmettre B0 avant de recevoir l'acquittement. Si A transmet un

nouveau bloc B1 et se perd, il va considérer l'acquittement du deuxième B0 comme un acquittement de B1.



Pour éviter cette confusion d'interprétation, il est aussi nécessaire de numéroter les ACK.

Le temps d'attente des acquittements rend la méthode send and wait peu efficace. En plus, il est unidirectionnel.

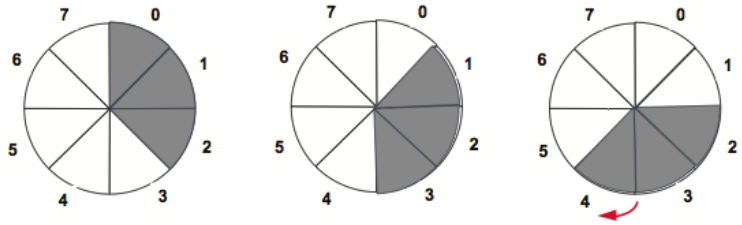
3.3.2 Fenêtre d'anticipation

Pour améliorer le protocole précédent et réduire le temps d'attente des acquittements, on émet plusieurs blocs sans attendre les ACK, ce processus se nomme anticipation. Ainsi, un acquittement n'acquitte plus une seule trame mais un ensemble de trames qui se suivent sans erreur. Le nombre de trames successives qu'on peut émettre sans réception d'acquittement est limité par une valeur notée W, appelée fenêtre (Window). Le principe est d'autoriser l'émetteur à envoyer les trames de numéro de séquence compris entre le numéro r de la prochaine trame attendue (communiqué par le récepteur) et $r + W - 1$:

$$r \leq Ns \leq r + W - 1$$

Remarque : $W = 1$ dans le cas d'une procédure Send-and-Wait.

Pour pouvoir réenvoyer les trames en cas d'erreur, l'émetteur met les blocs non acquittés dans W mémoires tampons. À la réception d'un acquittement d'une trame, l'émetteur libère la mémoire correspondante et envoie une nouvelle trame.



Problème : que se passe-t-il si, de façon temporaire, le récepteur n'est pas prêt à recevoir les W trames d'information de la fenêtre ? L'utilisation d'une fenêtre d'anticipation peut nécessiter la mise en œuvre d'un mécanisme de régulation supplémentaire de type tout-ou-rien. L'idée est d'utiliser une trame de contrôle particulière est utilisée pour indiquer que le récepteur est momentanément dans l'incapacité de continuer à recevoir. L'émetteur recevant cette trame de contrôle cesse immédiatement toute émission (même s'il n'avait pas utilisé toute sa "fenêtre" d'émission). Une autre trame de contrôle est alors nécessaire pour indiquer à l'émetteur que le récepteur est revenu dans un état normal et qu'il est donc prêt à recevoir de nouvelles trames.

3.4 Procédures de gestion des données

Les procédures de gestion de données sont des protocoles de la couche liaison qui mettent en œuvre les techniques précédentes (délimitation des trames, correction des erreurs et contrôle de flux). Elles sont de deux familles :

1. Les procédures orientées caractère : qui fonctionnent généralement à l'alternat (de type send and wait).
2. Les procédures orientées bit : conçues pour les transmissions bidirectionnelles simultanées à hauts débits.

3.4.1 Procédure BSC

BSC (Binary Synchronous Communications) est une procédure orientée bit développé par IBM pour la transmission synchrone des blocs de caractères. Elle permet d'exploiter principalement deux types de liaisons :

1. Les liaisons point à point : où les stations communiquent à l'alternat (half duplex) et en cas de conflits, une station privilégiée dite station primaire prend le contrôle de la station secondaire.

2. Les liaisons multipoints : où la station primaire représente le nœud central par rapport aux stations secondaires.
   - Pour la réception, on utilise le mode *polling* (interrogation). La station primaire invite les stations secondaires à émettre chacune à son tour. La station consultée répond par un message si elle a quelque chose à émettre, sinon elle répond négativement.
   - Pour l'émission, on utilise le mode *adressing* ou *selecting*. La station primaire envoie un message de sélection à la station secondaire pour l'informer qu'elle veut émettre un message ; la station secondaire répond positivement si elle est prête à recevoir, négativement si elle n'est pas prête.

Le codage des messages utilisé par BSC repose essentiellement sur les principaux alphabets internationaux tel que le code ASCII. La procédures réserve des caractères du code (caractères de contrôle) pour la gestion de la liaison de données. Certains caractères ont une fonction universellement reconnue, tel que :

- SYN (SYNchronous idle) : utilisé pour assurer la synchronisation caractère. L'émetteur commence par envoyer une séquence de caractères SYN (séquence préfixe) avant tout message ou séquence de supervision.
- **ENQ** (ENQuiry) : placé dans une séquence de supervision. Il invite une station à émettre ou à recevoir.
- **SOH** (Start Of Heading) : signale un début d'en-tête.
- **STX** (Start of TeXt) : délimite à la fois la fin de l'en-tête (lorsqu'il existe) et le début du texte.
- **ETB** (End of Transmission Block) : peut être employé pour distinguer une fin de bloc de données d'une fin de message.
- **ETX** (End of TeXt) : indique la fin d'un texte et le début des caractères de contrôle servant à la détection des erreurs.
- **ACK** (ACKnowledgement) : figure dans une séquence envoyée par le récepteur pour accuser positivement le message qu'il vient de recevoir.
- **NAK** (Négative AcKnowledgement) : figure dans une séquence envoyée par le récepteur pour refuser le message qu'il vient de recevoir. Ce message doit alors être réémis.
- **DLE** (Data Link Escape) : utilisé lors des transmissions en mode transparent (lorsque toutes les configurations de l'alphabet de transmission, y compris les caractères de procédure, sont susceptibles de se retrouver dans le champ de données). Il

Signale que le caractère suivant doit être interprété comme un caractère de procédure et non comme un caractère de données (STX, ETB, ETX,...). Lorsque le caractère à transférer est lui-même DLE, il faut émettre deux DLE consécutifs (technique dite de doublement du DLE).

– **EOT** (End Of Transmission) : signale la fin d'un transfert de données.

Les formats des messages utilisés par BSC reposent sur la notion de bloc. Un message est un champ de données d'une taille quelconque, susceptible d'être découpé en blocs de taille optimale. La procédure BSC permet la transmission de nombreux types de messages :

– en-tête seul : SYN, SOH, ...{l'entête}..., ETX, BCC, PAD ;
  - BCC : Block Check Character - PAD (padding) : séquence de remplissage.
– un seul message sans en-tête : SYN, STX,...,ETX, BCC, PAD,
– un seul message avec en-tête : SYN, SOH, ..., STX,...,ETX, BCC, PAD
– plusieurs blocs pour un même message, sans en-tête :
  – SYN, STX,... ,ETB, BCC, PAD pour les premiers blocs,
  – SYN , STX,..., ETX, BCC, PAD pour le dernier bloc du message ;
– plusieurs blocs pour un même message, avec en-tête :
  – SYN, SOH, ..., STX,...,ETB, BCC, PAD pour les premiers blocs,
  – SYN, SOH, ..., STX, ..., ETX, BCC, PAD pour le dernier bloc.

Pour la détection des erreurs, la procédure BSC utilise un CRC 16 avec un polynôme générateur $G(x) = x^{16} + x^{12} + x^5 + 1$

3.4.2 Procédure HDLC

La procédure HDLC (High-level Data Link Control) est une procédure orientée bit, développée par IBM et normalisée par l'UIT en 1976. HDLC est une procédure point à point et multipoints en full duplex, utilisant des trames séparées par des fanions de valeur 01111110 (7E). Trois modes peuvent être exploités par HDLC :

1. le mode de réponse normal (Normal Response Mode ou NRM) : la station secondaire doit attendre un ordre explicite du primaire avant de pouvoir émettre.
2. le mode de réponse asynchrone (Asynchronous Response Mode ou ARM) :la station secondaire a le droit d'émettre des données sans attendre l'invitation du primaire. Ce mode de fonctionnement est également connu sous le nom protocole LAP (Link Access Protocol). Il suppose que les deux stations possèdent à la fois le statut primaire et le statut secondaire.

3. le mode de réponse asynchrone équilibré ou symétrique (Asynchronous Balanced Mode ou ABM) : la liaison est obligatoirement point à point ; comme pour LAP, les deux stations possèdent à la fois le statut primaire et le statut secondaire. Ce mode de fonctionnement est connu aussi sous le nom de protocole LAP-B (Link Access Protocol-Balanced). De nos jours, c'est le seul mode utilisé.

3.4.2.1 Types de trames HDLC

HDLC utilise trois types de trames :

1. les trames diinformation ou trames **I** : assurent le transfert de données ;
2. les trames de supervision ou trames **S** (Supervisor) : assurent la transmission des commandes de supervision (accusé de réception...),
3. les trames non numérotées ou trames **U** (Unnumbered) : supervisent la liaison (connexion, déconnexion).

3.4.2.2 Structure de la trame HDLC

La trame HDLC est organisée comme suit :

8 bits	8 bits	8 bits	n bits	16 bits	8 bits
fanion	adresse	contrôle	information	FCS	fanion

- Fanion (flag) : 01111110
  . délimite les trames : toutes les trames doivent commencer et finir par un fanion.
  . permet la synchronisation des trames : toutes les stations rattachées à la liaison doivent rechercher en permanence cette séquence ;
  . un même fanion peut servir de fanion de fermeture pour une trame et de fanion d'ouverture pour la trame suivante ;
  . mécanisme de transparence au fanion par bits de bourrage : en émission, un 0 est inséré dès que cinq 1 consécutifs apparaissent en dehors des champs F ; ces 0 sont enlevés en réception. Si sept 1 apparaissent n'importe où dans une trame, elle est déclarée en erreur.
- Champ d'adresse : permet d'identifier la trame comme étant une commande ou une réponse. En mode ABM, les valeurs que peut prendre ce champ sont prédéfinies. Quatre valeurs sont suffisantes pour distinguer les commandes et les réponses dans les deux sens de transmission (ex : 11000000, 10000000, 11110000 et 1110000).

– Champ de contrôle : il indique le type de trame avec les paramètres nécessaires.
– FCS (Frame Check Sequence) : calculé sur les champs d'adresse, de commande et d'information, à partir du code polynômial V.41 ($x^{16} + x^{12} + x^5 + 1$).

3.4.2.3 Champ de contrôle et formats de trame

Il existe trois formats de trame qui correspondent à des codages différents du champ de contrôle :

	1	2	3	4	5	6	7	8
Information	0	Ns			P/F	Nr		
Supervision	1	0	S	S	P/F	Nr		
Non numérotée	1	1	M	M	P/F	M	M	M

– Ns : numéro de séquence de la trame émise,
– Nr : numéro de la prochaine trame attendue (acquittement dans les données),
– P/F (Poll/Final) : Ce bit est positionné à 1 par le primaire lorsque celui-ci sollicite une réponse immédiate du secondaire.

La signification des trames de type S dépend des deux bits SS selon le tableau suivant :

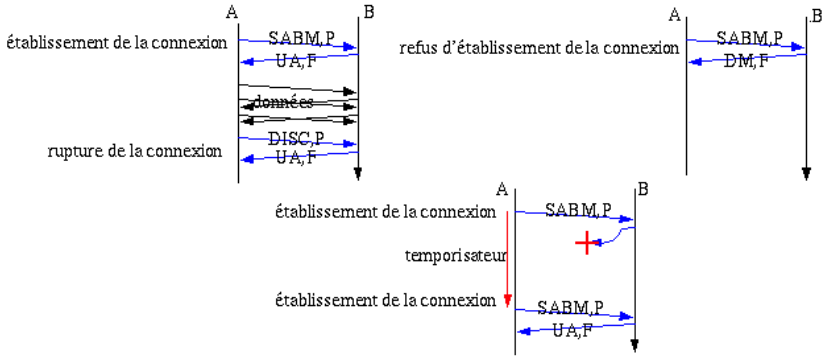
S	S	Commande	Signification
0	0	RR (Receiver Ready)	La station est prête à recevoir la trame numéro Nr et accuse positivement la réception des trames jusqu'à (Nr - 1)
0	1	RNR (Receiver not Ready)	La station n'est pas prête à recevoir des trames mais et accuse positivement la réception des trames jusqu'à (Nr - 1)
1	0	REJ (Reject)	La station rejette les trames à partir du numéro Nr. L'émetteur est obligé de retransmettre (P/F = 1)
1	11	SREJ (Reject)	= REJ mais uniquement pour la trame numéro Nr.

La signification des trames de type U dépend des deux bits M selon le tableau suivant :

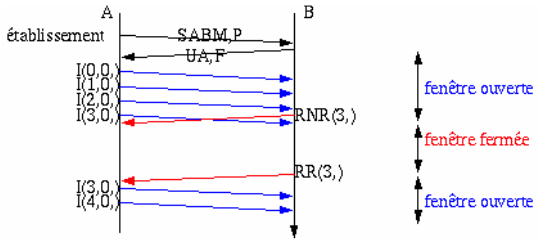
Trame	Commande	Signification
11111100	SABM	Set ABM demande l'établissement en mode ABM
11110000	DM	Disconnect Mode indique que la station se trouve en mode déconnecté
11001010	DISC	Disconnect libère la liaison
11000110	UA	Unnumbered Acknowledge indique la réception et l'acceptation d'une commande non numérotée

3.4.2.4 Exemples des échange

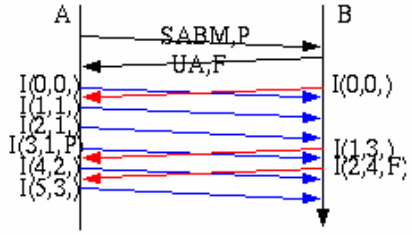
La figure suivante illustre des exemples des échanges entre deux stations utilisant la procédure HDLC pour établir la connexion.



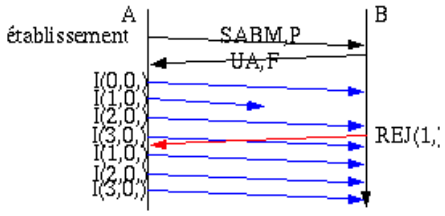
L'exemple suivant, illustre un cas d'échange unidirectionnel.



L'exemple suivant, illustre un cas d'échange bidirectionnel.



L'exemple suivant, illustre un cas d'échange unidirectionnel avec perte de trames.



3.5 Protocole PPP

Le protocole PPP est le protocole de liaison point à point utilisé dans Internet. Il utilise les lignes téléphoniques de l'abonné pour accéder au réseau (la liaison concerne typiquement un ordinateur personnel et le fournisseur d'accès à Internet). Il s'agit d'une version très simplifiée d'HDLC qui ne comprend ni contrôle de flux, ni mécanisme de reprise sur erreurs. La structure d'une trame PPP est donnée dans la figure suivante.

Flag	Address	Control	Data PPP	Flag

Les 8 bits du champ Address sont à 1 (la liaison étant point à point, une seule valeur d'adresse suffit). Le champ Control a la même signification que dans HDLC. Le champ Data PPP commence par deux octets (le champ protocole), qui identifient le protocole de niveau supérieur auquel est destinée la trame ; il se termine par un champ FCS dont le mode de calcul est identique à celui d'une trame HDLC. La seule trame transportant des données sur une liaison fiable est une trame U de type UI (Unnumbered Information). Cette trame contient un champ d'informations mais n'est pas numérotée (car il n'y a pas de contrôle de flux). L'absence de mécanisme de reprise sur erreur ne signifie pas que le circuit est fiable : le champ FCS sert à valider les trames reçues.

PPP comprend trois composants principaux :

- Une méthode pour encapsuler les datagrammes de plusieurs protocoles.
- Un protocole de contrôle du lien "Link Control Protocol" (LCP) destiné à établir, configurer, et tester la liaison de données.
- Une famille de protocoles de contrôle de réseau "Network Control Protocols" (NCPs) pour l'établissement et la configuration de plusieurs protocoles de la couche réseau.

Deux variantes très connues du protocole PPP :

- **PPPoA** (en anglais point-to-point protocol over ATM) est un protocole utilisé par les connexions haut débit ADSL et câble destinées aux particuliers.

– **PPPoE** (en anglais point-to-point protocol over Ethernet) est un protocole d'encapsulation de PPP sur Ethernet. Il permet de bénéficier des avantages de PPP, notamment sa compatibilité avec les protocoles d'authentification (PAP, CHAP, etc.) et le contrôle de la connexion (débit, etc.), sur un réseau Ethernet. Il est beaucoup employé par les connexions haut débit à Internet par ADSL et câble destinées aux particuliers.

3.6 Exercices

Exercice 1 Délimitation des trames

1. On doit émettre sur une liaison le texte suivant :

   "La couche liaison est la couche numéro 2."

   Sachant que la méthode de délimitation des trames utilisée est le comptage de caractères et que la taille du bloc est de 4 caractères, donner la chaine de caractères réellement émise.

2. On doit émettre sur une liaison les données binaires suivantes (4 octets) :

   0011 0111 0111 1110 0001 0001 1011 1110 soit encore en hexadécimal 377E11BE

   – La délimitation des trames utilisée est la transparence binaire ("bit stuffing"). Rappelez brièvement son principe.

   – Quelles données observerait-t-on alors sur la voie physique ?

Exercice 2 Parité

Soit le message composé de la chaîne : "NET", le contrôle de transmission de chaque caractère est assuré par un bit de parité impair, donner la représentation binaire du message transmis. On suppose que les caractères sont codés selon le code ASCII, en utilisant 7 bits.

Rappel : Le code ASCII des caractères transmis sont : N : 1001110, E : 1001001, T : 1010100

Exercice 3 Code CRC

– Soit le message suivant : 0011111101. On rajoute à ce message un CRC calculé par le polynôme générateur $g(x) = x^2 + x + 1$. Quel est le message codé ?

– Le message 101011000110 est reçu. Le polynôme utilisé pour la détection des erreurs est le suivant $x^6 + x^4 + x + 1$. La transmission s'est-elle faite correctement et quel est le message émis.

Exercice 4 Procédure HDLC

On désire émettre une suite d'informations d'une Station A vers une Station B en utilisant le protocole de liaison de niveau 2 HDLC (High level Data Link Control) défini par l'ISO. En supposant que la taille de la fenêtre = 8 (0..7) et que la Station Émettrice A n'envoie que 04 trames d'informations I numérotées puis se place en attente d'accusé de réception,

1. On vous demande de déterminer la trame de supervision générée par la station B selon les cas suivants :
   - Cas1 : toutes les trames ont été bien reçues .
   - Cas 2 : la trame I N°2 a été mal réceptionnée .
   - Cas 3 : les trames I N°1 et N°3 contiennent des erreurs .
   - Cas 4 : la Station réceptrice B ne répond pas. (étudier les différentes raisons possibles)
2. On vous demande de déterminer la suite de trames émises de la Station A en fonction de la suite des trames de supervision S/U suivantes envoyées par la Station réceptrice B :

t_0	t_1	t_2	t_3	t_4	t_5	t_6	t_7	t_8
UA	RR-04	REJ-06	RR-02	SREJ-04	SREJ-07	RR-04	UA	fin

   t_i : à l'instant t_i

   Commenter votre réponse.

Exercice 5 Procédure HDLC

1. Soit la suite de données binaires située dans le champ d'information d'une trame HDLC :

   011110111110011111100011

   - Quelle est la suite réellement fournie au support de transmission (pour ces données seulement) ?
   - Que se passe-t-il si le douzième bit de la suite réellement transmise a été mal reconnu du récepteur ?
2. Décoder les trames HDLC représentées en hexadécimal suivantes en extrayant les différents champs et donnant leur signification :
   - "7E C0 48 4D 41 47 49 53 54 45 52 D3 E1 7E", "7E 80 BC 02 2D 7E", "7E C0 A6 FF 7E", "7E 80 95 FF 7E"

Chapitre 4

Réseaux locaux

Un réseau local est un ensemble de moyens autonomes de calcul (micro-ordinateurs, stations de travail, téléphones portables, tablettes, appareils ou autres) reliés entre eux pour s'échanger des informations et partager des ressources matérielles (imprimantes, espace disque...) ou logicielles (programmes, bases de données...). Ils utilisent des protocoles simples car les distances couvertes sont courtes (de quelques centaines de mètres à quelques kilomètres) et les débits importants (jusqu'à plusieurs centaines de Mbit/s). Ces réseaux sont souvent appelés RLE (Réseaux Locaux d'entreprise), car ils répondent, le plus , aux besoins des entreprises

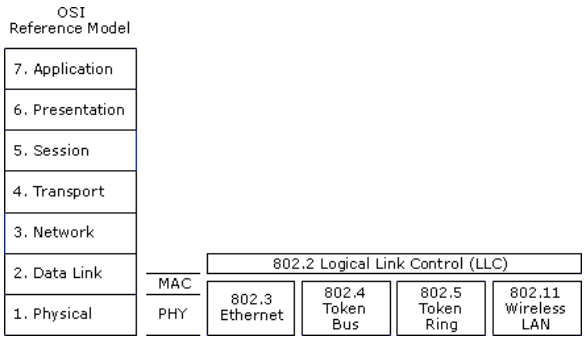
4.1 Standardisation

Le comité 802 de l'IEEE (Institute of Electrical and Electronics Engineers), essentiellement constitué de représentants des constructeurs américains, s'est occupé de l'architecture des réseaux locaux. Plusieurs documents définissent l'architecture proposée :

- Le standard 802.1 définit le contexte général des réseaux locaux informatiques.
- Le standard 802.2 définit la couche Liaison de données.
- Les standards 802.3, 802.4, 802.5 et 802.6 définissent différents protocoles d'accès au support, pour plusieurs types de supports physiques : paire métallique, câble coaxial ou fibre optique.
- Le standard 802.11 définit un protocole d'accès pour les réseaux locaux sans fil (WLAN, Wireless LAN).

Par rapport au modèle OSI, l'architecture normalisée dans les réseaux locaux découpe la couche Liaison en deux sous-couches : MAC (Medium Access Control) et LLC (Logical Link Control). La première règle l'accès au support partagé. Elle filtre les trames reçues

pour ne laisser passer que celles réellement destinées à l'équipement concerné. La seconde gère l'envoi des trames entre équipements, quelle que soit la technique d'accès au support.



4.2 Topologies des réseaux locaux

La topologie d'un réseaux définit la manière selon laquelle sont reliés ses différents composants entre eux. Les réseaux locaux utilisent les topologies de base comme le bus, l'anneau et l'étoile ou des combinaisons de celles-ci (étoile de bus, grappe d'étoiles...). Il faut distinguer la topologie physique de la topologie logique. La première caractérise la manière dont est réalisé le câblage du réseau local (la structure des chemins de câbles, le type de raccordement...) ; la seconde décrit comment on attribue le droit à la parole entre toutes les stations. La topologie logique définit la méthode d'accès au support (ou niveau MAC) utilisée.

4.2.1 Topologies physiques

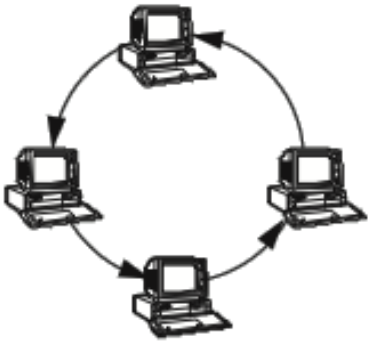
Il existe trois topologies physiques de base :

4.2.1.1 Topologie en bus

La topologie en bus consiste à utiliser un long câble, sur lequel les différents équipements se raccordent en série, pour qu'il n'y ait qu'un seul chemin sans boucle entre deux équipements du réseau local. Chaque station peut accéder à tout moment au support commun pour émettre. Les données sont diffusées à toutes les stations.

4.2.1.2 Topologie en anneau

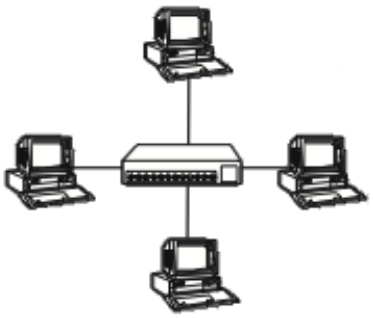
Dans la topologie en anneau, chaque station est connectée au support par un port d'entrée et transmet les données à la station suivante par son port de sortie. Les différentes stations sont reliées en cascade et les données circulent d'une station à l'autre, toujours dans le même sens : chaque station traversée prend le message, l'analyse puis le retransmet sur son port de sortie.



L'anneau manque de fiabilité en cas de rupture du support. On le double parfois pour réaliser deux anneaux qui peuvent transmettre soit dans le même sens soit en sens inverse. La seconde solution est préférable car elle permet de reconstituer le réseau, même en cas de rupture des deux anneaux au même endroit.

4.2.1.3 Topologie en étoile

La topologie en étoile est, en fait, la généralisation des liaisons point à point : chaque équipement est relié par une liaison spécifique à un équipement central.

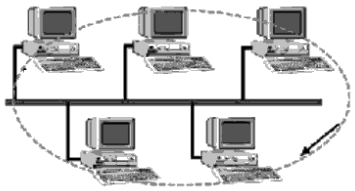


4.2.2 Topologie Logique

La topologie logique s'appuie sur la manière dont les équipements échangent leurs données sur le réseau local. Elle ne dépend que du niveau MAC choisi et non de la façon

de raccorder les équipements entre eux. Pratiquement, deux topologies logiques sont à considérer : le bus et l'anneau.

On peut en effet utiliser différentes topologies physiques pour réaliser une topologie logique donnée. Par exemple, une topologie logique en anneau peut utiliser un câblage physique en bus :



4.3 Constituants d'un réseau local

Architecture informatique dédiée à l'échange d'information et au partage de ressources physiques, un réseau local est essentiellement constitué par :

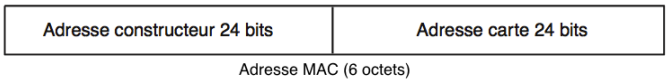
1. un câblage reliant les différents nœuds selon une certaine topologie ;
2. une méthode d'accès au support pour assurer son partage ;
3. une méthode d'adressage pour identifier chaque nœuds ;
4. un ensemble cohérent de protocoles(pile) pour permettre la communication ;
5. un système d'exploitation spécifique (NOS,Network Operating System) capable de prendre en charge les périphériques distants partagés et d'en contrôler l'utilisation (administration et sécurité) ;
6. un ensemble de programmes utilisant les ressources mises en commun.

4.4 Sous couche MAC

4.4.1 Adressage

Dans les réseaux locaux, l'adresse utilisée est une adresse physique qui se gère au niveau du matériel. Elle possède un format défini par l'IEEE sur 48 bits. Ce format constitue l'adressage universel des équipements : il correspond à un numéro de série dont un premier champ de 24 bits donne le constructeur de la carte (champ attribué par l'IEEE). Le second champ de 24 bits, librement choisi par le constructeur, est le numéro de la carte elle-même. De cette façon, toute carte réseau d'un ordinateur possède une adresse physique unique

dans le monde. Le format universel est généralement appelé adresse MAC, du nom de la couche.



L'adresse MAC est généralement représentée par six valeurs hexadecimales séparées par " :", par exemple : " 52 :54 :05 :fd :de :e5". Une adresse avec tous les bits à 1 est utilisée pour la diffusion vers toutes les stations du réseau.

L'adresse MAC est utilisée par les machines dans un LAN pour se reconnaitre. Une machine qui trouve son adresse MAC dans un message, elle le récupère et l'utilise, sinon elle l'ignore.

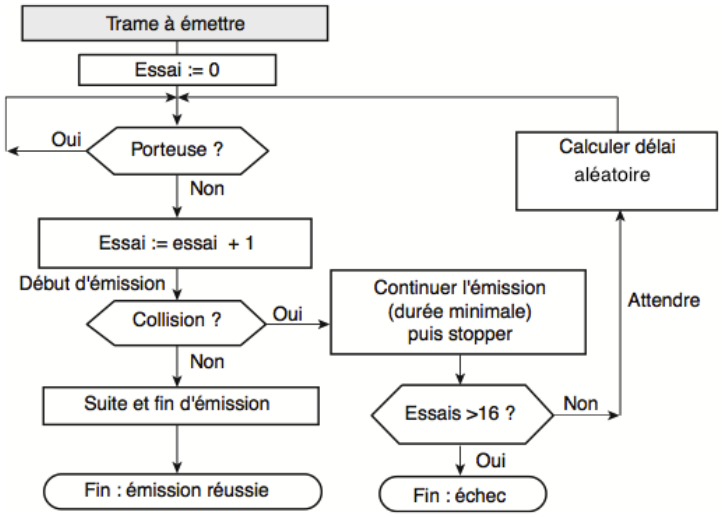
4.4.2 Techniques d'accès au support

Dans un réseau local, les machines partagent la même bande passante, ce qui nécessite une technique d'arbitrage pour résoudre les conflits. Les constructeurs informatiques ont proposé de nombreuses techniques d'accès :

4.4.3 CSMA/CD

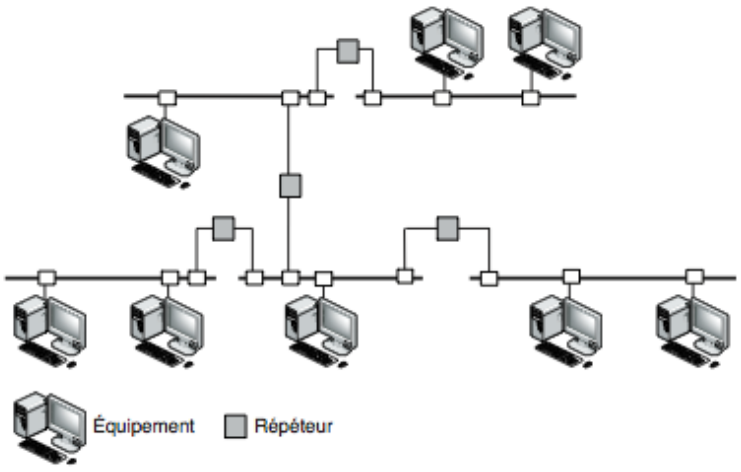
CSMA (Carrier Sense Multiple Access with Collision Detection), est une technique d'accès dite aléatoire. Le principe de base repose sur la diffusion des messages à toutes les stations (réseau à diffusion). Lorsqu'une station désire émettre, elle écoute le réseau, si aucun message n'est en cours de diffusion (silence) elle émet, sinon, elle diffère son émission jusqu'à ce que le support soit libre (attente active). Cette méthode ne peut garantir que deux stations n'émettront simultanément leur message. Dans ce cas, chaque message est pollué par l'autre (collision) et devient inexploitable.

Pour détecter les collisions, chaque station écoute le support durant son émission pour une durée égale au moins la durée d'aller retour du signal entre les deux stations les plus éloignées. Si elle détecte une perturbation de son message, elle arrête son émission et arme un temporisateur aléatoire. À l'échéance du temporisateur la station écoute le support, s'il est libre, elle retransmet le message tout en surveillant son émission (détection de collision). L'organigramme suivant illustre le principe de la méthode CSMA/CD :

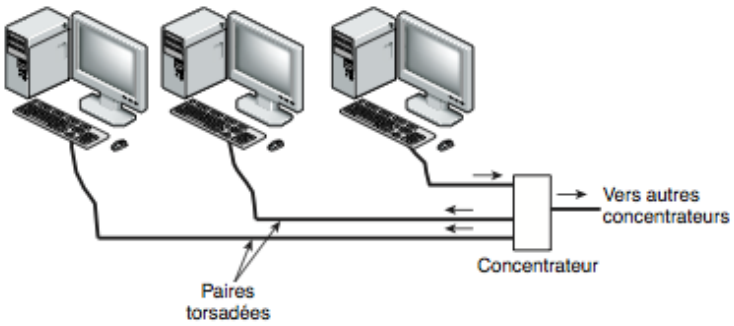


4.4.3.1 Réseaux Ethernet

Ethernet est d'une des application réussies de la technique CSMA/CD. C'est un protocole de réseaux locaux développée par Xerox en 1976. Il a été normalisé par la suite par IEEE sous la norme 802.3 et représente aujourd'hui la technologie la plus utilisée. Un réseau Ethernet (IEEE 802.3) utilise une transmission en bande de base avec un code Manchester sur un bus physique en RJ45 ou câble coaxial, organisé en un ou plusieurs segments.



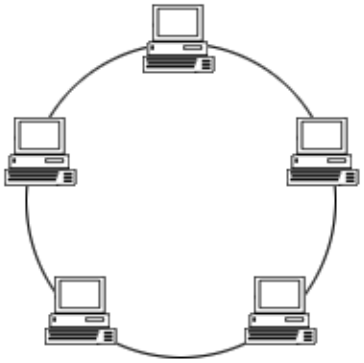
Afin que tous les équipements reçoivent un signal de puissance suffisante, la longueur de chaque segment est limitée. Pour des longueurs supérieures, il faut utiliser des répéteurs (hubs ou concentrateur), qui décodent et amplifient les signaux reçus sans les interpréter.



Le réseau Ethernet est une solution rapide et peu coûteuse, destinée principalement à la bureautique. La force de Ethernet est dans sa simplicité : il n'y a aucun équipement centralisant le contrôle du réseau. L'ajout et le retrait d'un équipement se font sans interruption de fonctionnement, que ce soit avec un câblage en bus ou en étoile sur le concentrateur. Si le trafic est faible, l'accès au support est quasiment immédiat. En revanche, le réseau supporte mal les fortes charges qui peuvent provoquer un effondrement du débit utile, car le temps d'accès au support n'est pas borné.

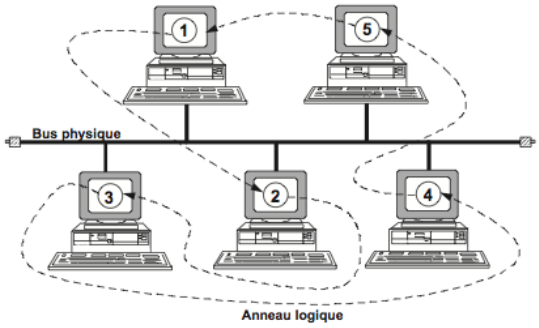
4.4.4 Token Ring

L'anneau à jeton (en anglais token ring) est une technologie d'accès au réseau basé sur le principe de la communication au tour à tour, c'est-à-dire que chaque ordinateur du réseau a la possibilité de parler à son tour. C'est un jeton (un paquet de données), circulant en boucle d'un ordinateur à un autre, qui détermine quel ordinateur a le droit d'émettre des informations. Lorsqu'un ordinateur est en possession du jeton il peut émettre pendant un temps déterminé, après lequel il remet le jeton à l'ordinateur suivant.



Cette technique est utilisée également sur un réseau en bus, le jeton, circule de la station de plus faible adresse à celle de plus forte adresse, formant ainsi un anneau virtuel sur le

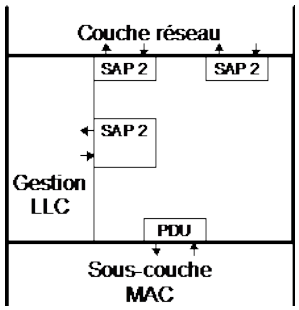
bus (anneau logique/bus physique).



Puisque le nombre de stations est connu, le temps d'accès d'une station au réseau peut être borné et la technique est dite déterministe. Généralement, cette technique est utilisée dans les réseaux industriels.

4.5 Sous couche LLC

La sous couche LLC (Logical Link Control) permet un ensemble de fonctions de services entre la sous couche MAC et les couches supérieures. Elle masque à la couche supérieure le type de réseau utilisé (Ethernet, Token Ring...). Les services de la sous-couche LLC sont accessibles à partir d'un point d'accès LSAP (Link Service Access Point ou point d'accès au service de liaison). Pour distinguer les deux extrémités de la relation, ces points sont respectivement appelés DSAP pour la machine destination (Destination Service Access Point) et SSAP pour la machine source (Source Service Access Point).



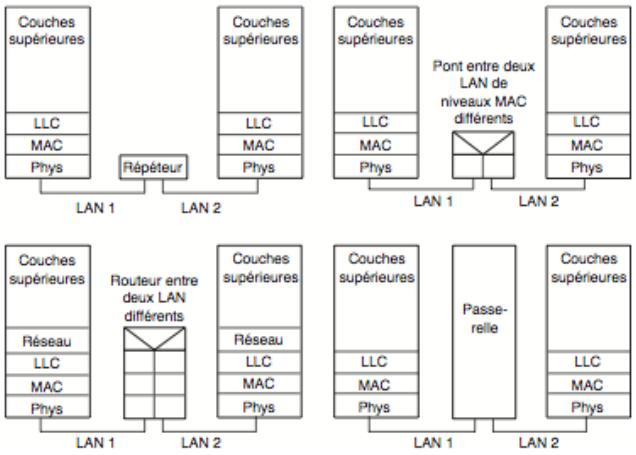
Les unités de données délivrées par ou à la couche supérieure forment des LSDU (Link Service Data Unit), celles-ci transmettent à la couche liaison les informations nécessaires à l'envoi des données (adresses MAC source et destination, niveau de priorité, données...). Les sous-couches LLC s'échangent des LPDU (Link Protocol Data Unit) dont le format est similaire à celui des trames d'HDLC

La sous couche LLC offre, selon les besoins, trois types de services : LLC1, LLC2 et LLC3.

1. **LLC1** fournit un service simple sans connexion ni contrôle, en point à point, en multipoint ou en diffusion. C'est le protocole le plus courant dans les réseaux locaux informatiques. Il se réduit pratiquement à une seule trame : UI (Unnumbered Information), trame d'information non numérotée, correspondant à la notion de datagramme. Le service rendu par le protocole LLC1 est minimal : il se contente de formater les messages à émettre et de leur ajouter un bloc de contrôle d'erreur. Le récepteur vérifie le bloc de contrôle et détruit les messages reçus erronés. Il n'y a aucun accusé de réception, ni aucune demande de retransmission. Un tel fonctionnement est acceptable dans l'environnement des réseaux locaux car les distances ainsi que les taux d'erreur sont très faibles. Les messages manquants sont éventuellement détectés puis réémis au niveau de la couche Transport.
2. **LLC2** assure un service avec connexion entre deux points d'accès et possède les fonctionnalités complètes du niveau Liaison du modèle OSI (contrôle de flux et contrôle d'erreur). C'est un protocole complet, analogue à la norme HDLC.
3. **LLC3**, adapté au monde des réseaux industriels, rend un service sans connexion avec acquittement.Il ajoute à LLC1 la notion d'accusé de réception. Dans les réseaux locaux industriels ou la commande de processus, il est important de garantir la fiabilité des transmissions, d'où l'idée d'un protocole sans connexion qui permette la bonne réception des messages sans la lourdeur imposée par la gestion des connexions.

4.6 Interconnexion des LANs

Physiquement, deux réseaux ne peuvent être reliés que par l'intermédiaire d'un équipement connecté à chacun d'eux, sachant acheminer des messages de l'un à l'autre. Plusieurs dispositifs d'interconnexion se mettent en place, selon le degré de similitude des réseaux. L'équipement d'interconnexion peut être selon les cas un répéteur (concentrateur), un pont (commutateur), un routeur ou une passerelle



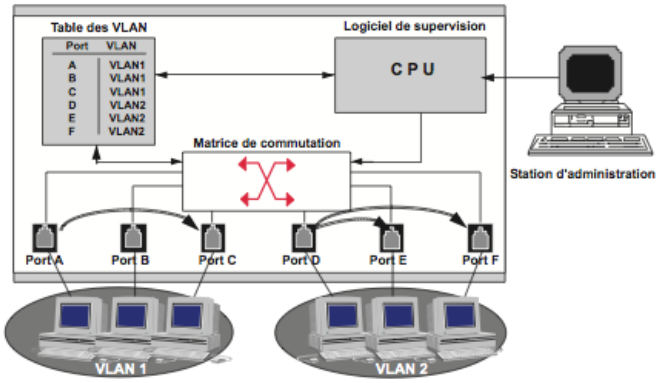
– **Répéteur :** réalise une connexion physique entre deux segments d'un même réseau logique. Agissant au niveau physique, les réseaux interconnectés doivent être homogènes. Un répéteur ne fait que retransmettre d'un côté les bits reçus sur l'autre, il agit par diffusion. Le nombre de répéteurs maximum dans un réseau est généralement limité à quelques répéteur lié au temps de transmission global de la trame. Le concentrateur (hub) est un répéteur multiport.
– **Pont :** (ou bridge) est un élément d'interconnexion de niveau 2. Ils permet d'interconnecter deux ou plusieurs réseaux (ponts multiports ou switch) dont les couches physiques sont dissemblables. Un pont stocke les trames et les analyse pour les envoyer à leurs destinations. Il permet de scinder un réseau local en deux et réduire ainsi le trafic dans chaque partie.

  Des algorithmes très poussés sont implémentés dans les switchs basés sur l'auto-apprentissage qui permettent de construire des tables de correspondances entre les adresses des stations et les différentes sorties du switch.
– **Routeur :** (routers) sont destinés à relier plusieurs réseaux de technologies différentes. Ils opèrent essentiellement au niveau de la couche 3 du modèle OSI, c'est-à-dire qu'ils assurent le routage des informations à travers l'ensemble des réseaux interconnectés. Le routeur possède au moins deux interfaces réseau et contient un logiciel très évolué, administrable à distance.
– **Passerelle :** (gateway) opère sur les sept couches du modèle OSI et effectue les conversions nécessaires pour interconnecter des réseaux totalement différents n'utilisant pas les mêmes protocoles de communications. Une passerelle est dans la majorité des cas constituée d'un ordinateur doté de deux cartes réseaux et un logiciel spécifique pour convertir les données entre les deux réseaux.

4.7 Réseaux locaux virtuels (VLAN)

Les réseaux locaux virtuels ou VLAN (Virtual LAN) sont des réseaux logiques indépendants les uns des autres qui sont définis en fonction des centres d'intérêt de leurs utilisateurs, et non en fonction de la situation géographique des équipements.

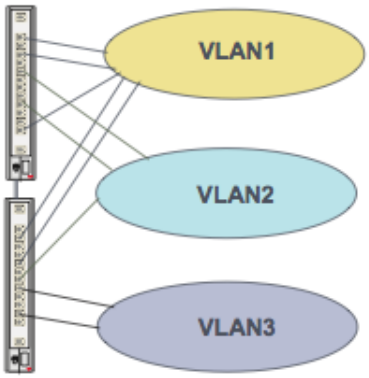
Un réseau virtuel regroupe une communauté d'usagers répartis dans toute l'entreprise, comme s'ils appartenaient au même réseau physique. Les échanges à l'intérieur d'un VLAN sont sécurisés et les communications entre VLAN contrôlées. Par exemple, le réseau virtuel réservé à la direction de l'entreprise fournit un espace de communication sécurisé à l'équipe directoriale. Ce réseau est logiquement distinct du réseau virtuel affecté aux services de production, même si les machines des deux départements sont reliées physiquement aux mêmes commutateurs.



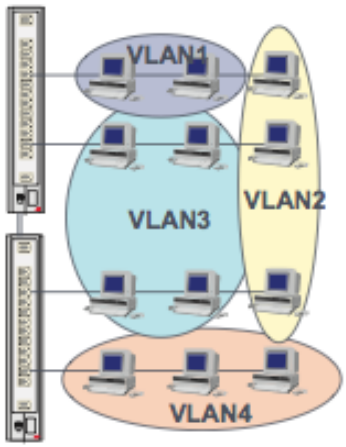
En définissant des domaines de diffusion (domaine de broadcast) indépendamment de la situation géographique des systèmes, les VLAN autorisent une répartition et un partage optimal des ressources de l'entreprise.

On utilise plusieurs techniques de différentiation des équipements pour créer un VLAN.

– La première opère au niveau physique 1 c-à-d niveau des ports du commutateur : un sous-ensemble des ports correspond à un VLAN donné. Cette solution a l'inconvénient de ne pas gérer la mobilité des utilisateurs.



– La deuxième opère au niveau MAC 2 : elle consiste à identifier les équipements d'un VLAN par leurs adresses MAC, quel que soit le port du commutateur sur lequel l'équipement est raccordé. Cette solution est plus souple que la précédente, mais elle lie encore l'appartenance à un VLAN particulier au matériel utilisé.



– La troisième opère au niveau Réseaux 3 en utilisant les adresses IP.

Le commutateur contient une table de correspondance entre les VLAN et la liste des ports associés. Pour gérer le VLAN avec un maximum de souplesse (quelle que soit la technique de différentiation), il faut qu'il soit étiqueté (tagged), c'est-à-dire que les trames portent un identificateur du VLAN auquel elles appartiennent. Cette étiquette se résume par deux octets ajoutés dans la trame, selon les recommandations du comité 802 (standard 802.1Q).

4.8 Réseaux locaux sans fil WLAN

Les WLANs sont des réseaux locaux qui utilisent les ondes radio pour échanges les données. Selon l'utilisation on distingue deux types :

– réseaux sans fil (WPAN, Wireless Personal Area Network), reliant des téléphones, périphériques, etc. Standardisés par 802.15, ils sont plus connus sous le nom de Bluetooth.
– réseaux sans fil (WLAN) compatibles Ethernet, standardisés par 802.11 ;

Norme WLAN	Nom commercial	Débit théorique (Mbit/s)	Portée max
802.11a	Wi-Fi	54	40 m
802.11b	Wi-Fi	11	90 m
802.11g	Wi-Fi	54	70 m

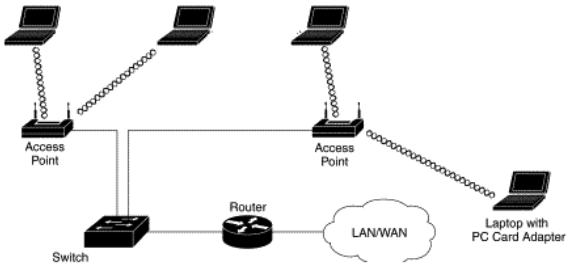
4.8.1 Architecture des WLANs

Deux modèles d'architecture sont à considérer : les réseaux ad-hoc et les réseaux à infrastructure.

– Dans les réseaux ad- hoc, les communications s'effectuent en point à point entre les stations. C'est le modèle de fonctionnement des WPAN. Les réseaux ad-hoc s'affranchissent de toute infrastructure. La communication à lieu directement de machine à machine. Une machine pouvant éventuellement servir de relais pour diffuser un message vers une station non vue (au sens électromagnétique du terme) par la station d'origine (routage).

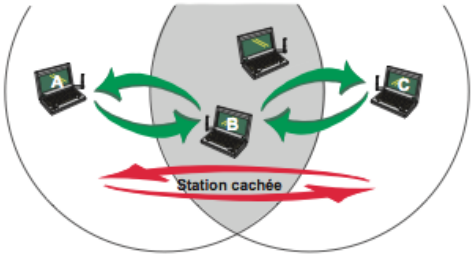
Actuellement, les réseaux ad-hoc ne fonctionnent qu'en mode point à point. Les protocoles de routage font l'objet de nombreuses recherches.

– Dans les réseaux à infrastructure, le réseau est géré par une ou plusieurs bases (ou bornes ou points d'accès). Lorsqu'un réseau comprend plusieurs bornes, celles-ci sont raccordées par un réseau Ethernet filaire. Les réseaux de la norme 802.11 en sont un exemple. Le réseau peut comporter une ou plusieurs cellules autonomes ou être le prolongement d'un réseau Ethernet traditionnel.



4.8.2 Technique d'accès

À l'instar d'Ethernet, les stations d'un réseau sans fil se partagent le même média. Le protocole CSMA utilisé dans les réseaux Ethernet n'est pas applicable tel quel, à cause du problème de la station cachée. Dans la figure suivante, un envoie de A vers B est en cours, si C veut émettre, il écoute le réseau et il le trouve libre. La station A et dite cachée par rapport à C.



La technique d'accès utilisé dans les WLANs est une version adaptée du CSMA, le CSMA/CA (Carrier Send Multiple Access with Collision Avoidance, signifiant à prévention de collision). Une station qui veut émettre écoute le support (CSMA). Si le support est occupé, elle diffère son émission. Si le support est libre, elle émet un petit paquet (RTS, Request To Send) qui contient les adresses source et destination. Si le support est libre, la station destination répond (CTS, Clear To Send), le message comporte les mêmes informations que le RTS. Ainsi, la station C (station cachée de A) qui n'a pas reçu le message de A, reçoit celui de B qui comporte les mêmes informations, elle est donc informée de la demande de réservation de bande formulée par A. La probabilité de collision est d'autant plus faible que le message est court. À cet effet, la norme IEEE 802.11 introduit la segmentation au niveau MAC.

4.9 Exercices

Exercice 1 CSMA/CD

Sur un câble coaxial en cuivre utilisée dans un réseaux Ethernet de 10Mbits/s, la vitesse de propagation du signal électrique est de $2*10^8$ m/s. Sachant que la longueur minimale d'une trame est de 64 octets, quelle est la longueur maximale d'un segment d'un tel medium pour que le principe CSMA/CD soit respecté ?

Exercice 2 CSMA/CD

On considère un réseau local dont le partage de la voie est géré selon un algorithme CSMA/CD persistant. Ce réseau gère les transmissions entre 4 stations A, B, C et D. Dans cet exercice on utilise comme mesure de temps le "slot time". Les délais d'espacement intertrames ainsi que les durées de détection de voie libre sont négligées. Le temps de détection de collision est égal à 1 slot.

A l'instant t = 0 la station A acquiert la voie et commence à transmettre un message. A l'instant t = 5 les stations B, C, et D recoivent une demande de transmission de message. Puis, pendant toute la durée considérée dans l'exercice aucune autre demande de transmission n'est soumise aux stations. Tous ces messages sont de taille fixe et la durée de leur transmission est égale à 6 slots.

La retransmission en cas de collision est effectuée après un certain temps calculé en fonction du nombre de tentatives d'accès, selon l'algorithme suivant :

```
Attente(attempts)
begin
  if attempts = 1 then maxbackoff := 2
  else
    if attempts = 10 then maxbackoff := backofflimit
    else maxbackoff := maxbackoff * 2
    endif
  endif
  delay := int (random * maxbackoff)
  Wait (delay * slot_time)
end
```

attempts est le nombre de tentatives pour accéder à la voie y compris celle en cours.

backoff_limit vaut 1024

int est une fonction qui rend la valeur entière par défaut

random est un générateur de nombres aléatoires compris entre 0 et 1.

Dans l'exemple on considèrera que la fonction random rend successivement pour chaque station les valeurs données par le tableau suivant :

Tirage/Stations	B	C	D
1^{er} tirage	1/2	1/4	3/4
2^{e} tirage	3/4	1/6	5/8
3^{e} tirage	1/3	2/3	1/2

Questions

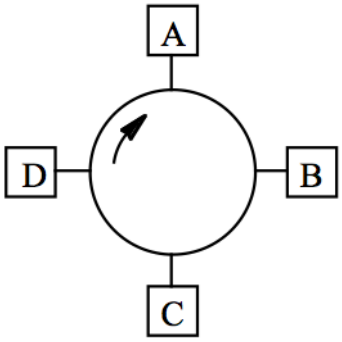
1. Compléter le diagramme suivant en indiquant pour chaque slot l'état de la voie.
   - Un slot occupé par la transmission d'un message correctement émis par la station A est représenté par "A"
   - Un slot occupé par une collision est représenté par "X"
   - Un slot correspondant à une absence de transmission est représenté par " ?"

Temps (slots)	0	1	2	3	4	...
Trames						...

2. Calculer le taux d'utilisation de la voie sur la période allant de t = 0 à la fin de la transmission du dernier message.

Exercice 3 Token Ring

On considère un réseau local en anneaux comportant quatre stations désignées par A, B C et D. Chaque station accède au support en utilisant le protocole de l'anneau à jeton. Elle peut transmettre au plus une trame de données. Le jeton est relâché par une station après que sa trame lui soit intégralement revenue. Le temps de propagation entre chaque station est de 1 ms, le temps de transmission d'une trame est de 4 ms (entête incluse). On néglige le temps de traitement de chaque station. Un jeton libre correspond à une trame plus petite dont on négligera le temps de transmission.



1. Dessiner un diagramme des temps gradués en ms décrivant le déroulement des différentes transmissions de trames suivant le scénario suivant :

   à t = 0, D possède le jeton ;

   à t = 0, B veut transmettre 2 trames ;

   à t = 4, A veut transmettre 1 trame ;

   à t = 8, D veut transmettre 1 trame ;

   à t = 23, C veut transmettre 2 trames.

2. Quelle est la durée totale de l'exécution de ce scénario ?

3. Quel est le temps d'accès moyen au support pour ce scénario ?

Exercice 4 Interconnexion

On considère deux réseaux locaux de type Token Ring d'IBM. Le LAN1 est formé de 4 stations A, B, C, D et le LAN2 est composé de 5 stations 1, 2, 3, 4 et 5. Ces stations sont ordonnées selon l'ordre inverse du sens de rotation d'une montre. Ces deux réseaux sont interconnectés par un pont simple (bridge) qui est situé entre D et C du LAN1 et entre 2 et 3 du LAN2.

Chaque réseau possède son propre Jeton (J1 et J2). Les caractéristiques de ce réseau sont :

- Le jeton circule selon le sens de rotation d'une montre
- la sous-couche LLC utilise un protocole de type 3 (service sans connexion et avec Acquittement LLC3) .
- Les trames de données sont de tailles fixes
- Les temps de transfert de station à la station suivante sont (y compris le pont) :
- t0 : temps de transfert d'un jeton libre
- t1 : temps de transfert d'une trame de données
- t2 : temps de transfert d'une trame d'acquittement

Sachant qu'à l'instant initial t=0 :

- Le jeton libre J1 de LAN1 se trouve au niveau de la station A
- Le jeton libre J2 de LAN2 se trouve au niveau de la station 5
- La station B désire envoyer à la station 4 une trame de données
- La station 2 désire envoyer deux (2) trames de données à la station 3

On vous demande de :

1. Décrire par un schéma l'architecture du réseau.
2. Donner les principales fonctions d'un pont simple d'une manière générale
3. Donner les étapes du comportement du pont pour réaliser le transfert d'une trame de données d'une station du LAN1 vers une station du LAN2.
4. Déterminer le temps T1 nécessaire à la station 2 pour transférer ses données
5. Déterminer le temps T3 d'attente à la trame émise par la station B avant qu'elle ne puisse circuler dans le LAN2
6. Déterminer le temps T2 nécessaire à la station B pour transférer ses données

Chapitre 5

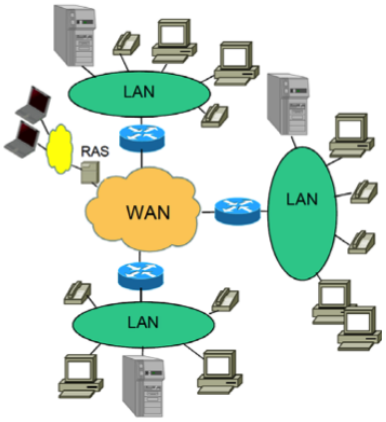
Réseaux grande distance

5.1 Définition

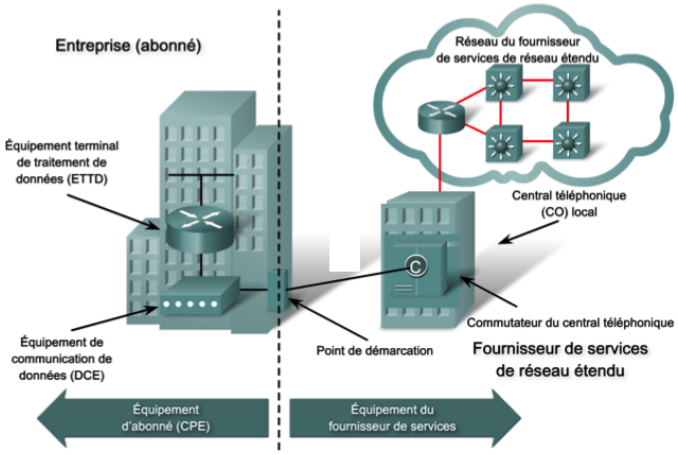
Les réseaux à grande distance (WAN) reposent sur une infrastructure très étendue, nécessitant des investissements très lourds. Contrairement aux réseaux locaux d'entreprise, les usagers ne sont pas propriétaires des réseaux, lesquels appartiennent à des opérateurs qui doivent respecter la législation en cours dans les pays où ils sont implantés. Ils fournissent aux usagers un service de transport de données, soit par des lignes spécialisées louées, soit par des lignes commutés à travers des réseaux à commutation de circuits ou à commutation de paquets. Les accès peuvent être permanents et commutés avec une plus ou moins grande fiabilité.

5.2 Organisation physique

Les réseaux WAN sont utilisés pour interconnecter plusieurs réseaux locaux, ou même permettre aux utilisateurs de se connecter à travers des réseaux publiques tel que internet.



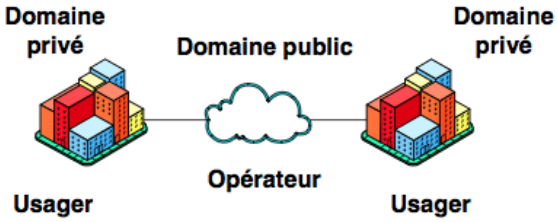
À l'intérieur, un réseau WAN est composé des moyens de transmission et les organes nécessaires à l'acheminement des informations (réseau téléphoniques fixes et cellulaires, lignes spécialisées , liaisons satellites,...) et son optimisation (fournisseurs de services, commutateurs, taxation, statistiques, sécurité, ...)



5.3 Connexion

5.3.1 Les opérateurs

Dans le domaine public, le transport des informations est assuré par des opérateurs (publics ou privés, en situation de monopole ou non).



Ils fournissent des services de transport de données aux usagers. Quelquefois, les services peuvent s'étendre au delà du transport, et prendre en compte les applications, voire leur gestion. En fonction de la technologie utilisée, la rémunération peut être basée sur la distance, la vitesse, le volume, la sécurisation ... Elle dépend donc de la qualité du service demandé.

5.3.2 Les lignes spécialisées (ou louées)

Elles réalisent des communications point-à-point, où chaque point de connexion est identifié par l'opérateur. En général, le coût à la minute est plus faible que celui d'une

liaison commutée, mais en volume, il est plus important puisque la liaison est permanente. Elle est rentable si le trafic est intense (plusieurs heures par jour). En contre partie, à débit physique égal, la liaison est plus rapide puisqu'on économise les durées de connexion et de déconnexion. On peut faire une analogie avec une manufacture qui dispose d'un site de fabrication, et d'un un site commercial éloigné. Si la production à écouler est permanente et volumineuse, il est plus rentable de louer une ligne ferroviaire entre ces 2 sites. Le temps de transit est alors plus faible (Il n'est pas nécessaire d'organiser une livraison). Dans le cas contraire, il vaut mieux expédier la production à travers le réseau ferroviaire de l'opérateur. Chaque livraison devra être organisée, et la production sera acheminée avec le reste du trafic de l'opérateur. Le délai de livraison sera plus long (aiguillages, temporisation dans les gares de triage ...), mais le coût de la livraison sera moindre.

5.3.3 Les lignes multiplexées

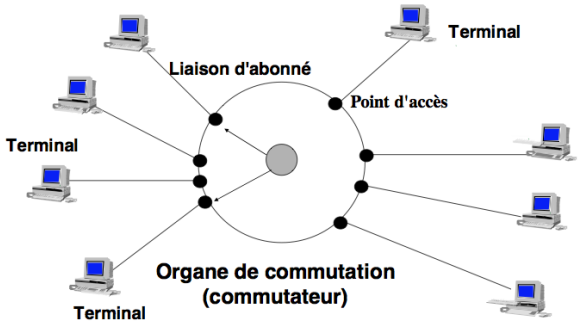
L'objectif économique d'une ligne multiplexée est l' utilisation rationnelle d'une ligne qui peut être partagée entre plusieurs usagers. En effet,il est rare qu'un seul usager utilise en permanence la totalité des capacités d'une ligne. Les ressources de la ligne peuvent être partagées soit en fréquence, soit dans le temps.

- Le multiplexage fréquentiel consiste à diviser la bande passante de la ligne en sous-bandes, chacune d'elle étant affectée à une communication. Tout se passe comme si la ligne était constituée de plusieurs lignes en parallèle (canaux), chacune d'elle occupant une fraction de la bande passante totale de la ligne. A la source, l'opération de multiplexage consiste à transposer les signaux de chaque canal dans la bande de fréquence qui lui a été attribuée. Ainsi les différents signaux peuvent être transmis ensemble sur la ligne sans interférer. Pour éviter les interférences, on prévoit des bandes de fréquence de sécurité afin que les spectres de 2 canaux voisins ne se recouvrent pas.
- Le multiplexage temporel est utilisé pour les signaux numériques. Si le signal est analogique à la source, il subit une conversion analogique/numérique.

5.4 Commutation

La commutation consiste à mettre en relation de façon temporaire 2 points de connexion, créant ainsi une liaison temporaire entre les 2 terminaux connectés. L'organe de commutation s'appelle un commutateur. Cette solution résout le problème du nombre de lignes

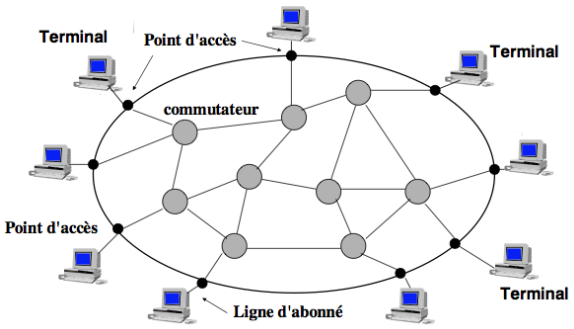
d'abonnés (une ligne par abonné). Par contre, si le commutateur est unique, les lignes d'abonnés doivent être très longues, et de plus, à un instant, seuls 2 abonnés peuvent être connectés.



Pour résoudre ce problème, il faut rapprocher les points de connexion des abonnés, offrir la possibilité de construire des chemins multiples entre les points de connexion : il faut créer un maillage entre des commutateurs, c'est à dire un réseau de commutation.

5.4.1 Réseaux de commutation

Les terminaux sont reliés au réseau de commutation par une ligne d'abonné locale (courte). Plusieurs liaisons peuvent être établies simultanément. Plusieurs terminaux peuvent accéder au réseau de commutation par le même point d'accès (non représenté sur le schéma). Les commutateurs réalisent une fonction d'aiguillage et participent au routage des données, pour constituer des connexions entre les terminaux.



Dans ce contexte où la ressource est rare vis-à-vis de la demande potentielle (si simultanément tous les abonnés du réseau désiraient joindre un autre abonné...), il est indispensable de rechercher des techniques particulières pour optimiser le partage des ressources, c'est l'objectif des techniques de commutation.

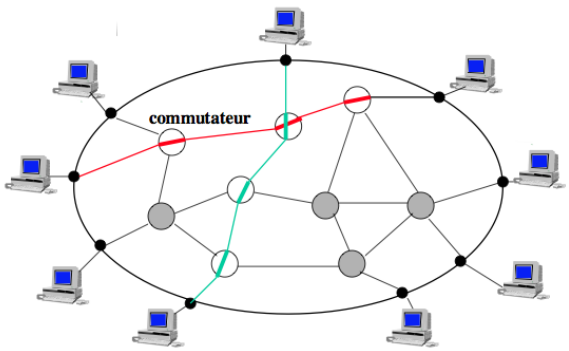
5.4.2 Techniques de commutation

Selon la technique employée pour relier deux utilisateurs, on distingue la commutation de circuits, de messages ou de paquets.

5.4.2.1 La commutation de circuits

Elle est issue des techniques utilisées dans les réseaux téléphoniques (RTC). Elle se déroule en 3 phases :

1. **La connexion :** un chemin est établi entre l'appelant et l'appelé, par commutations successives. Les commutateurs ne remplissent qu'une fonction d'aiguillage. Tout se passe comme s'il n'y avait qu'une seule liaison entre les extrémités.
2. **Le transfert :** Les données (ou la voix) sont transmises de bout en bout sur le "circuit de données". Les ressources (lignes) sont attribuées en permanence, et en volume constant, pendant toute la durée de la communication (les "silences" sont pénalisés).
3. **La libération :** après le transfert, les ressources sont restituées au réseau de commutation, et sont disponibles pour d'autres communications.

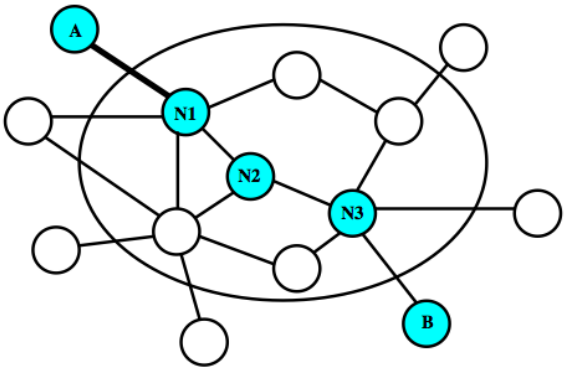


Cette technique soufre de trois inconvénients :

- Chevelure analogique (débit limité)
- Délais de connexion importants
- Signalisation indistincte des données, et mal adaptée

5.4.2.2 La commutation de message

Le principe est très différent de la commutation de circuits. Les données sont structurées en messages. Un message est une suite logique de données qui forment un tout (fichier, enregistrement ...).



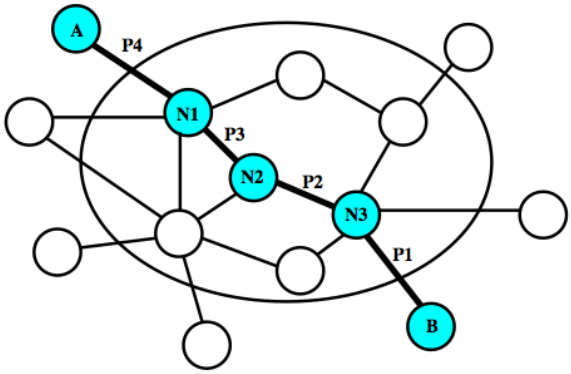
Un message est acheminé vers sa destination au fur et à mesure des commutations :

- Le message délivré par A est envoyé vers N1, où il est stocké et vérifié,
- La liaison A-N1 est libérée
- Il est transmis à N2, où il est stocké et vérifié,
- La liaison N1-N2 est libérée,
- Le processus est itératif jusqu'à la livraison du message à B
- Ainsi, les commutateurs (ou nœuds de commutation) sont dotés de mémoire et de capacité de traitement de données (leur fonction va au-delà d'un simple aiguillage).
- Quand un message est enregistré dans un nœud de commutation, la liaison par laquelle il est arrivé est libérée, et ses ressources sont disponibles pour le réseau de commutation.

L'avantage de cette technique est que sur le chemin AB, on n'utilise qu'une seule liaison de données à la fois, les autres étant disponibles pendant ce temps pour d'autres communications. Cependant, si la taille des messages est trop importante, il y a des risques de débordement des tampons de stockage puisqu'un nœud de commutation peut recevoir des messages depuis plusieurs stations). En plus, le délai d'acheminement de bout en bout est excessif (il faut attendre qu'un message soit entièrement stocké dans un nœud avant de le retransmettre vers le nœud suivant),

5.4.2.3 Commutation de paquets

Pour palier aux inconvénients engendrés par les messages de taille trop importante, on fragmente les messages en paquets de taille moyenne. Les paquets sont acheminés de nœud en nœud : après avoir été vérifiés, ils sont réexpédiés, sans attendre la totalité du message.



Cette fragmentation élimine les inconvénients engendrés par la commutation de messages trop longs :

- A débit constant, le délai d'acheminement de bout en bout est plus court,
- La capacité de stockage des nœuds de commutation est moindre,
- A taux d'erreur constant, la probabilité d'erreur sur un paquet (un bit erroné) est plus faible, et en cas d'erreur, seul le paquet erroné doit être retransmis.
- De plus, les paquets peuvent plus facilement être multiplexés sur des liaisons à haut débit.

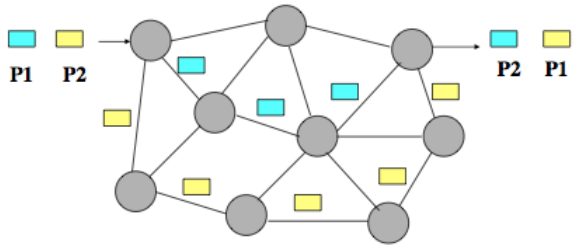
La taille des paquets est fixée par un compromis entre 2 contraintes :

- Il faut réduire leur taille pour profiter au maximum des avantages de la fragmentation,
- Il ne faut pas trop la réduire, à cause de l'encapsulation des données (pour ne pas réduire le débit utile, il faut que la taille des données utiles soit très supérieure à celle de la signalisation et des informations protocolaires).

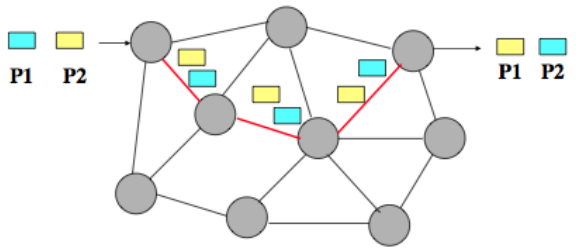
En pratique, elle est fixée par les protocoles de transfert de paquets : Elle est généralement de l'ordre de grandeur du koctet (sauf pour les réseaux à commutations rapides, pour lesquels les messages sont fragmentés en cellules de quelques dizaines d'octets).

La commutation de paquets peut se faire en deux modes :

- Mode non connecté : les paquets (appelés datagrammes) sont transmis de nœud en nœud, au fur et à mesure que la connexion est établie, sans s'assurer que les ressources soient disponibles de bout en bout. Les paquets d'un même message, sont indépendants. Ils peuvent suivre des chemins différents, car les algorithmes de routage sont adaptatifs (chaque paquet subit un routage, et son parcours dépend du trafic). Ils sont livrés dans le désordre.



– En mode connecté, un circuit est établi de bout en bout, avant de transférer le message, comme pour la commutation de circuits. Mais il s'agit bien de la commutation de paquets (le circuit est virtuel). Avant de transférer les paquets de données, un paquet (appelé paquet d'appel) subit un routage adaptatif, pour parcourir un chemin optimal. Au fur et à mesure de son parcours, les ressources sont réservées, et les tables de routage des nœuds traversés sont fixées. Ainsi, tous les paquets suivants d'un même message suivront le même chemin (appelé circuit virtuel commuté ou CVC), et sont livrés dans l'ordre d'émission. Après le transfert des données, un paquet (de libération) parcourt le CVC, et le ferme en restituant ses ressources.



Le transfert des paquets de données est plus rapide, car ils ne sont pas retardés par l'exécution d'un algorithme de routage.

Le contrôle d'erreur dans les réseaux à commutation de paquets peu se faire en deux manières :

1. Un contrôle d'erreur par liaison de données : Le paquet, encapsulé dans une trame, est contrôlé dans chaque nœud de commutation. Cette méthode augmente la fiabilité, mais aussi le délai de transit.
2. Un contrôle d'erreur de bout en bout : Il n'y a pas de contrôle d'erreur dans les nœuds de commutation. Le contrôle est effectué aux extrémités par les usagers du réseau de commutation. Le transfert est moins fiable, mais plus rapide.

5.5 Exercices

Exercice 1 Commutation

Soit un réseau à commutation au sein duquel deux stations A et B ont établi une communication. A doit envoyer un fichier de taille L bits à B. Le transfert de données présente les caractéristiques suivantes :

- S est le nombre de commutateurs traversés pour la communication entre A et B. Toutes les liaisons de données utilisées ont un débit D bit/s.
- Le protocole de liaison est le même sur toutes les liaisons ; il ajoute un en-tête de H bits à chaque unité de données transférée.
- On néglige les temps de propagation et les temps de traitement dans les commutateurs du réseau. On néglige de même les temps de gestion des accusés de réception.

1. Le réseau est un réseau à commutation de messages. Le fichier est transmis dans un seul message, d'une liaison à l'autre, jusqu'au destinataire. Donnez l'expression T_{fic1} du temps de transmission de ce fichier dans le réseau.
2. Le réseau est un réseau à commutation de paquets. Le fichier est découpé en paquets contenant P bits de données (pour simplifier, on supposera que les paquets sont tous de taille identique). Donnez l'expression T_{fic2} du temps de transmission du fichier
3. Calculez et comparez les temps obtenus dans les deux premières questions en prenant : L = 64000 octets ; H = 9 octets ; S = 2 ; D = 64 kbit/s. On prendra trois valeurs possibles pour la taille des paquets : P = 128 octets ; P = 16 octets ; P = 48 octets (dans ce dernier cas, il s'agit d'une cellule ATM dont l'en-tête H utilise 5 octets).

Chapitre 6

Couche Réseaux

Pour pouvoir échanger des informations entre les utilisateurs de plusieurs réseaux locaux, les entités intermédiaires jouent un rôle capital. Elles doivent contenir les moyens nécessaires à l'acheminement des informations entre deux stations quelconques dans le réseaux. Ces moyens sont situés, selon le modèle OSI, au niveau de la couche 3 : la couche réseaux.

La couche réseaux est appelée, donc, à fournir les procédures et les moyens fonctionnels nécessaires à l'échange des informations données par la couche transport. C'est un service de bout en bout qui est responsable de l'acheminement des paquets de données qui peuvent traverser plusieurs nœuds intermédiaires. Le paquet est l'unité de transport de données dans la couche réseaux.

Cette couche est surtout nécessaire dans les réseaux maillés où les paquets doivent traverser plusieurs nœuds avant d'arriver à, leurs destinations ; elle n'est pas prise en compte dans les réseaux constitués par une seule liaison. Les caractéristiques de cette couche ont été déterminées par la réalisation effective de réseaux d'ordinateurs généraux (Internet).

Le rôle de la couche réseau est de transporter d'une extrémité à l'autre du réseau des blocs de données provenant d'une fragmentation des messages du niveau supérieur, le niveau transport.

Pour pouvoir échanger des informations entre deux entités communicantes quelconques à travers un ou plusieurs réseaux, de nombreux services sont fournis par la couche réseau :

1. **Commutation :** pour mettre en relation les deux correspondants.
2. **Adressage et nommage :** pour identifier et localiser chaque correspondant de manière unique sur le réseau.
3. **Routage :** pour acheminer les blocs d'information vers le destinataire.

4. **Segmentation :** pour adapter la taille des unités de données transférées aux capacités du réseau.
5. **Contrôle de congestion :** pour contrôler le trafic admis dans le réseau pour empêcher son effondrement.

En plus de ces grands services, la couche réseau assure l'intégrité du transport des paquets. Pour ce faire, il est nécessaire de définir un format de paquet et de se donner des moyens pour détecter les erreurs.

Des services facultatifs peuvent être rendus par la couche réseau. Par exemple, la livraison en séquence des paquets reçus par la couche transport, le transfert accéléré de paquets de supervision, le multiplexage de connexions réseau... etc.

La commutation (vue dans le chapitre précédent) est une tâche de base de la couche réseaux, elle peut être de circuit de message ou de paquet. Dans le dernier cas, souvent utilisé, les paquets peuvent être transférés en mode connecté ou non connecté.

6.1 Adressage et nommage

Le but de l'adressage est de fournir un service de communication universel permettant à toute machine de communiquer avec toute autre machine. Les machines doivent être accessibles aussi bien par des humains que par d'autres machines. Une machine doit pouvoir donc être identifiée par :

- une adresse qui doit être un identificateur universel de la machine,
- un nom (mnémotechnique pour les utilisateurs),
- une route précisant comment la machine peut être atteinte.

Les noms sont plus faciles à utiliser par les utilisateurs, mais ne permettent pas l'identification des machines et nécessitent un moyens de faire la correspondance avec les adresses.

Les adresses forment le moyen d'identifier de manière unique chacun de ses utilisateurs.

6.1.1 Adressage

On utilise dans les réseaux, selon la cas, deux types d'adressage :

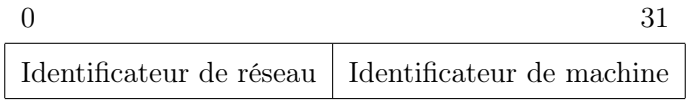
- Adressage hiérarchique : l'adresse est décomposée en différentes parties qui permettent d'identifier :
  - le réseau auquel l'utilisateur est rattaché
  - le point d'accès par lequel il est raccordé au réseau

– l'utilisateur dans l'installation locale Le champ adresse diminue au fur et à mesure de la progression des blocs dans le réseau. L'exemple courant de ce type est la numérotation téléphonique
– Adressage à plat : le format de l'adresse n'a aucune signification particulière quant à la localisation de l'entité communicante. L'exemple est l'adresse MAC.

6.1.1.1 Principe de l'adressage IP

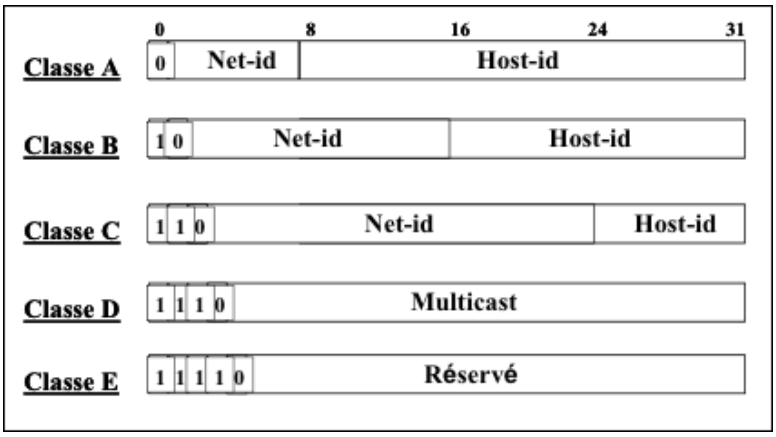
Les adresses IP permettent d'identifier à la fois les réseaux et les machines. Une adresse IP est constitué de 32 bits structuré en deux parties : identificateur de réseau et identificateur de machine.

Une adresse IP version 4 est constituée de 32 bits structurés en deux parties : identificateur de réseau et identificateur de machine.



Les identificateurs des réseaux sont contrôlés par le NIC (Network Information Center) en Californie mais les identificateurs des machines sont contrôlés localement.

Les adresses IP sont organisées en cinq classes :



– La classe A est la classe des très gros réseaux tel que ARPANET et MILNET, elle comporte 126 réseaux de 17 millions de machines chacun.
– La classe B est la classe des réseaux moyens, elle comporte 16384 réseaux de 65000 machines.
– La classe C est la classe des réseaux locaux, c'est la classe la plus utilisé dans l'Internet, elle comporte deux millions de réseaux de 254 machine chacun.

– La classe D est la classe de diffusion multiple (Multicast).
– La classe E est une classe expérimentale, réservée à des usages d'essai ou des usages futurs.

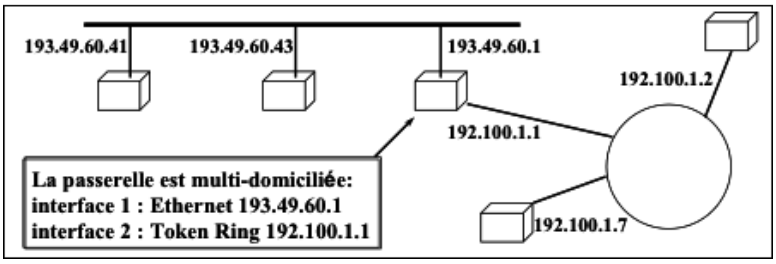
6.1.1.2 Notation décimale

Les adresses IP binaires sont difficiles à manipuler, on utilise alors la notation décimale qui représente l'adresse IP sous la forme de quatre valeurs décimale comprises entre 0 et 255 représentant les valeurs des quatre octets de l'adresse binaire.

10000000		00001010		00000010		00011110
128	.	10	.	2	.	30

On écrit : 128.10.2.30

Exemple



6.1.1.3 Adresses particulières

Dans chaque classe, il existe des adresses réservés pour une utilisation particulière et qui ne peuvent être attribuées à aucune machine et qui ont une signification particulière. En général :

– Un champ d'adresse (Netid ou Hostid) tout à 1 signifie tous les objets (réseaux ou machines) (utilisé pour la diffusion)
– Un champ d'adresse (Netid ou Hostid) tout à 0 signifie cet objet (réseau ou machine) (utilisé en cas d'ignorance des identificateurs)

Exemples

– L'adresse du réseau a une valeur d'indentificateur de machine où tous les bits sont nuls (0)
– Une adresse contenant les bits de réseau à 0 signifie ce réseau
– Une adresse de diffusion dans le réseau d'attachement (local) comporte les 32 bits IP à 1 (plein 1 ou all 1s) (Utilisée lors du démarrage lorsqu'on ignore son adresse IP).

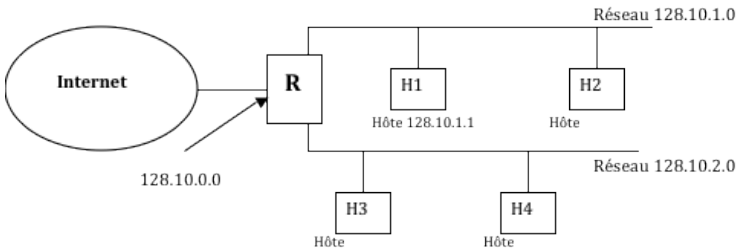
– Une adresse tout à 0 veut dire cet ordinateur n'est autorisé que lors du processus de démarrage.
– Une adresse qui à le premier octet égale à 01111111 (127) est dite adresse de Rebouclage, elle est utilisé pour les communications intra-machine pour des besoins de tests ou pour la communication entre les applications dans la même machine. Les adresses de classe A de 10.0.0.0 à 10.255.255.255, de classe B de 172.16.0.0 à 172.31.255.255 et de classe C de 192.168.0.0 à 192.168.255.255 sont réservées à la constitution de réseaux privés autrement appelés intranet 1.
– Les adresses de classe A de 10.0.0.0 à 10.255.255.255, de classe B de 172.16.0.0 à 172.31.255.255 et de classe C de 192.168.0.0 à 192.168.255.255 sont réservées à la constitution de réseaux privés autrement appelés intranet

6.1.1.4 Sous adressage

Les concepteurs de l'adressage IP, travaillant dans un monde de gros systèmes coûteux, ont pensé à un Internet de quelques dizaines de réseaux et de quelques centaines de machines. Ils n'ont pas prévu l'explosion du nombre de petits réseaux individuels, la croissance était exponentielle et on a vu un doublement de taille tous les neuf mois. Le grand nombre de réseaux élémentaires a fini par poser des problèmes :

– La tâche de gestion des adresses IP est énorme
– Les tables de routage deviennent gigantesques voire saturés.
– La classe C (2 millions de réseaux) est devenue rapidement insuffisante.
– L'utilisation de la classe B engendre aussi des problèmes : le nombre de réseaux est insuffisant et la gestion de 65000 machines au sein de chaque réseau est très difficile.

D'où la nécessité de subdiviser. Le sous adressage (subnet adressing ou subnetting) est une technique standardisée dans l'adressage IP, elle permet d'utiliser une seule adresse réseau avec plusieurs réseaux (sous-réseaux) en découpant la partie réservée à l'adresse des machines sur un réseau en deux parties dont la première sera un identificateur de sous-réseau. Ainsi un seul réseau de classe B, sur lequel on pourrait nommer 65536 machines pourra être décomposé en 254 sous-réseaux de 254 machines.



Pour l'Internet, il n'existe q'un seul réseau 128.10.0.0 et tous les routeurs traitent les datagrammes à destination de ce réseau de la même façon. Par contre, le routeur R se sert du troisième octet (égal à 1 ou 2) de l'adresse contenue dans les datagrammes qui lui proviennent pour les diriger vers le sous-réseau auquel ils sont destinés assurant ainsi un routage hiérarchique.

<table>
<tr><td>0</td><td colspan="2">31</td><td></td></tr>
<tr><td>NetID</td><td colspan="2">HostID</td><td>Ancienne adresse IP</td></tr>
<tr><td>Partie Internet</td><td colspan="2">Partie locale</td><td></td></tr>
<tr><td>Partie Internet</td><td>Sous réseau</td><td>Machine</td><td>Nouvelle adresse IP</td></tr>
</table>

Le choix du nombre de bits représentant l'identificateur de sous réseaux est laissé à l'administrateur local. Si ce nombre est fixe pour tous les sous-réseaux, on parle alors de sous adressage fixe, sinon on parle de sous adressage variable. Le sous adressage variable est utilisé dans le cas ou une entreprise par exemple compte à la fois de petits réseaux et de grands réseaux. Dans l'adressage fixe (utilisé souvent), on doit faire un compromis entre le nombre de réseaux et le nombre de machines.

Nombre de bits de sous réseau	Nombre de sous réseau	Nombre d'hôtes
2	2	16382
3	6	8190
4	14	4094
.	.	.
.	.	.
.	.	.

- Les masques de sous réseaux

Le standard TCP/IP indique q'un site qui utilise le subnetting doit choisir un masque (subnet mask) pour chaque sous réseau qui sera enregistré sur chaque machine. Le masque

permet à une machine de connaître le nombre de bits attribués à l'identificateur du sous-réseau et à celui de la machine.Un masque de sous réseau est un mot de 32 bits contenant des bits à 1 au lieu de l'identificateur de réseau et de sous-réseau et des bits à 0 au lieu de l'identificateur de machines.

Exemples de masques

11111111	11111111	11111111	00000000
Réseau			Hôte
255	255	255	0

11111111	11111111	11110000	00000000
Réseau			Hôte
255	255	240	0

11111111	11111111	11111111	11110000
Réseau			Hôte
255	255	255	240

- Appartenance d'une machine à un sous réseau

Donc, à partir de l'adresse d'un datagramme et de son masque de sous-réseau une machine peut déterminer si le datagramme est destiné à une machine sur son propre sous-réseau, à une machine sur un autre sous-réseau de son réseau ou à une machine extérieure à son sous-réseau.

Pour vérifier que la machine d'adresse IPDest appartient au sous-réseau d'adresse IPRes ayant le masque N, on calcule

$$V = IPdest \wedge N$$

Si $V = IPres$ alors la machine se trouve dans le même sous réseau et les messages lui sont envoyés, sinon les messages sont envoyés à une passerelle (routeur) qui les transmet au reste du réseau qui se charge de les acheminer vers leur destination.

Par exemple, dans le cadre du réseau présenté au debut de cette section où le masque de sous-réseau est 255.255.255.0 supposons que notre machine soit celle identifiée par l'adresse IP 128.10.1.2 (H2).

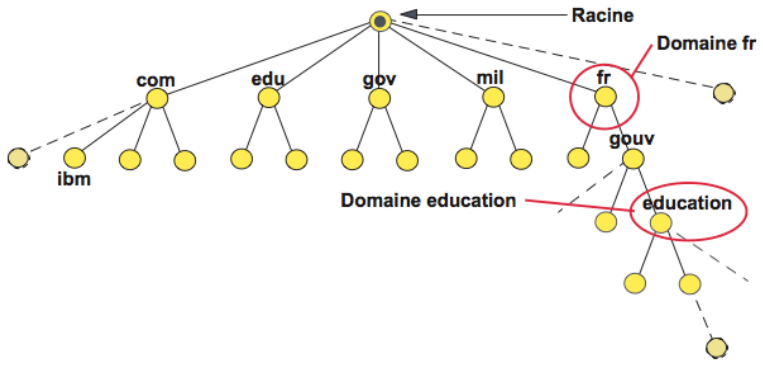
– Si l'adresse de destination est 128.10.1.1, un "et" entre la représentation binaire de cette adresse est de celle du masque de sous-réseau donne 128.10.1.0 à savoir l'adresse du sous-réseau de notre machine, donc le datagramme est destiné à une machine de ce même sous-réseau.

– Si l'adresse de destination est 128.10.2.1, un calcul du même genre donne 128.10.2.0 c'est-à-dire l'adresse d'un autre sous-réseau du même réseau.
– Si l'adresse de destination est S.T.U.V (avec (S,T) $\neq$ (128,10)) le résultat sera l'adresse d'un réseau différent de celui auquel appartient notre machine.

6.1.2 Nommage

La notion de nommage est complémentaire de celle d'adressage, l'un désigne l'objet, l'autre précise sa localisation. Indépendamment qu'il est plus aisé de manipuler des noms que des adresses, l'avantage du nommage est essentiellement de dissocier l'objet de sa localisation géographique. Le déplacement de l'objet nommé est transparent à l'utilisateur. De manière similaire à l'adressage, le nommage utilise deux modes de représentation :

– Le nommage à plat ou horizontal, ce type de nommage impose une démarche rigoureuse pour garantir l'unicité d'un nom sur l'ensemble du réseau. NetBios, protocole allégé mis en œuvre dans les réseaux locaux, utilise un nommage à plat.
– Le nommage hiérarchique ou arborescent, plus souple, organise le nommage en domaines. Cette technique autorise une représentation des objets calquée sur l'organisation de l'entreprise. Chaque nœud peut être un domaine dont la gestion peut être confiée à une autorité particulière. Ce mode de représentation et d'administration convient parfaitement à la gestion d'un annuaire très important comme celui d'Internet.



DNS (Domain Name System) est un système d'annuaire permettant de faire la correspondance entre le nom symbolique et l'adresse IP. Les serveurs de noms, ou serveurs DNS, sont des machines qui assurent la traduction des noms en adresses IP et réciproquement. On parle de résolution d'un nom ou d'une adresse. Pour cela, ils possèdent des informations sur l'architecture de l'arbre et sur les données associées.

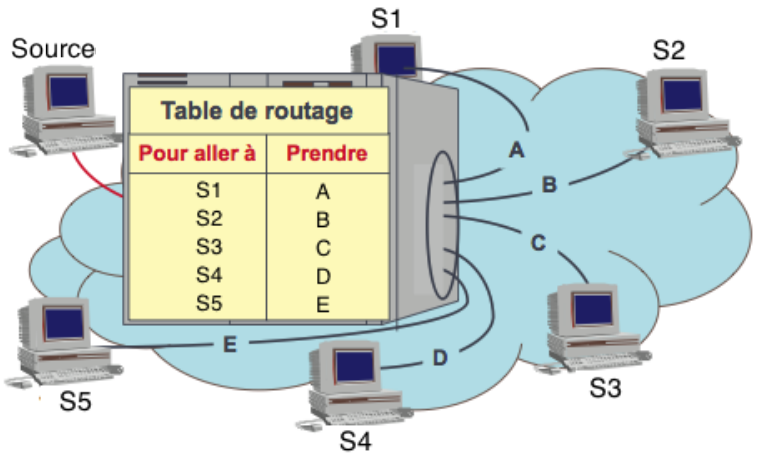
6.2 Routage

6.2.1 Principe

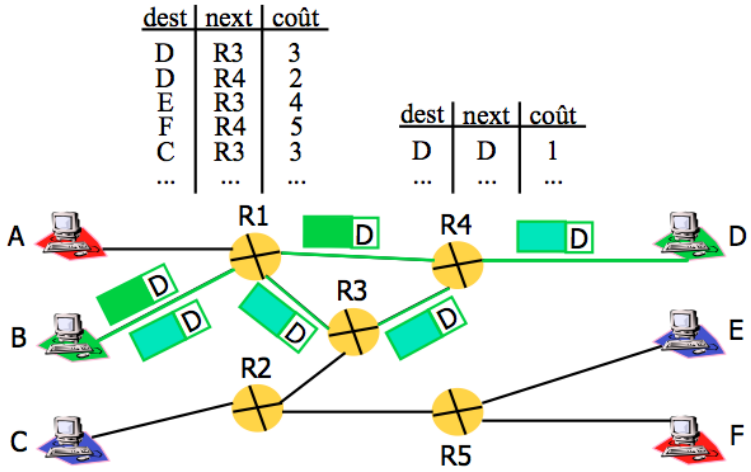
Le but du routage est la détermination d'un chemin à travers le réseau entre une machine émettrice et une machine réceptrice, toutes deux identifiées par leur adresse. Les protocoles de routage établissent des règles d'échange entre routeurs pour mettre à jour leurs tables d'informations selon des critères de coût comme, par exemple, la distance, l'état de la liaison, le débit. Ils améliorent ainsi l'efficacité du routage.

Il y a de très nombreux problèmes à résoudre. L'un des problèmes fondamentaux à éviter réside dans les boucles de routage (le message peut "tourner en rond" dans le réseau et ne jamais atteindre son destinataire). L'autre apparait lorsqu'il y a une panne dans le réseau et qu'il faut optimiser le calcul des nouvelles routes : une fois la panne détectée, il faut transmettre l'information sur l'évènement le plus rapidement possible pour que les différents routeurs recalculent par où faire passer leurs messages en contournant la liaison en panne.

Chaque nœud du réseau comporte des tables, dites tables d'acheminement couramment appelées tables de routage, qui indiquent la route à suivre pour atteindre le destinataire. En principe, une table de routage est un triplet <Adresse destination>/<Route à prendre>/<Coût>.



Chaque paquet doit contenir une information qui permet d'identifier le destinataire pour que chaque routeur puisse prendre une décision (@destination). Le "coût" permet de choisir la route appropriée si plusieurs routes sont possibles (coût pour atteindre la destination). Par exemple dans la figure suivante, le coût et représenté par le nombre de sauts (de routeurs) pour atteindre la destination.



Un protocole de routage commence par la construction des tables de routage au niveau de chaque nœud, ensuite utilise ces tables pour l'acheminement des paquets entre les stations. À priori, aucun routeur n'a une vision globale de la route que prendront les paquets : les paquets sont relayés de proche en proche jusqu'au destinataire. L'émetteur du paquet doit connaître le premier routeur relais, ensuite, chaque routeur est chargé d'acheminer le paquet vers le routeur suivant jusqu'à la destination finale.

Un protocole de routage efficace doit assurer :

- une taille minimale pour les tables de routage,
- Une consultation rapide des tables,
- Une consommation acceptable de mémoire
- Le moins possible d'informations à échanger
- minimiser la fréquence des messages de contrôle générés par l'échange des informations de routage
- être robuste en évitant les boucles,la surcharge de certains routeurs...
- trouver une route optimale

En général des types de routage existent :

6.2.2 Routage statique

Dans le routage statique (ou non adaptatif), la décision de routage ne dépend pas de l'état du réseau ; le choix de la route est défini par l'administrateur une fois pour toute lors de l'initialisation et elles sont mises à jour uniquement quand la topologie du réseau change (cas de panne).

Le routage statique est simple mais ne recherche pas la route optimale et n'est pas adapté à la défaillance d'un lien. Il est généralement adapté aux petits réseaux et aux

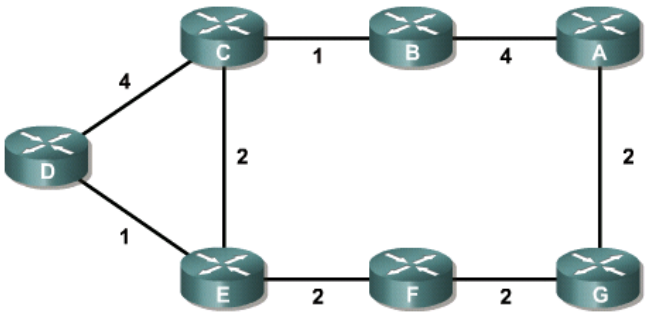
réseaux dans lesquels le choix de la route est limité (routes rentrées manuellement). Cependant, il assure le séquencement des paquets même en mode non connecté car tous les paquets prennent la même route.

Deux variantes de routage statique sont utilisées :

6.2.2.1 Plus court chemin

Dans ce type de routage, l'administrateur calcule les chemins minimums entre chaque deux stations (réseaux) puis introduits les tables correspondant à ces chemins dans chaque routeur. Le réseaux tout entier est représenté par un graphe pondéré. Le coût (métrique) de chaque arrête peut être calculé selon :

- le nombre de saut (nombre de routeurs traversés)
- la distance réelle (en km) entre deux routeurs
- le délai de transmission (temps de latence)
- le nombre de paquets moyen dans les files d'attente
- le taux d'erreurs moyen
- le trafic moyen observé, ...



Le calcul des chemins est effectué en utilisant des algorithmes connus en théorie des graphes tel que Dijkstra.

6.2.2.2 Inondation

Dans le routage par inondation, chaque nœud envoie le message sur toutes ses lignes de sortie, sauf celle d'où provient le message. Pour éviter une surcharge du réseau, chaque message comporte un compteur de sauts. Le compteur est initialisé à l'émission (nombre de sauts autorisés) et décrémenté par chaque nœud. Le message est détruit quand le compteur de sauts est à zéro. Pour éviter les bouclages, les messages sont numérotés, chaque nœud

mémorise cet identifiant et détruit les messages déjà vus.

Ce système est très robuste, il résiste à la destruction de plusieurs lignes et garantit de trouver toujours le plus court chemin ; il est utilisé dans certaines communications militaires et par certains protocoles de routage pour diffuser les informations d'états du réseau. Il est utilisé, également pour découvrir le chemin optimal et en déduire une route statique.

6.2.3 Routage dynamique

Dans le Routage dynamique, les tables de routage sont construites automatiquement sans l'intervention de l'administrateur. Les routeurs échangent régulièrement leurs états et mettent à jour leurs tables de routage. Ce routage est plus complexe que le routage statique et surcharge le réseau par l'échange d'informations de routage et ne garantit pas le séquencement en mode non connecté. Cependant, il permet de choisir la route optimale.

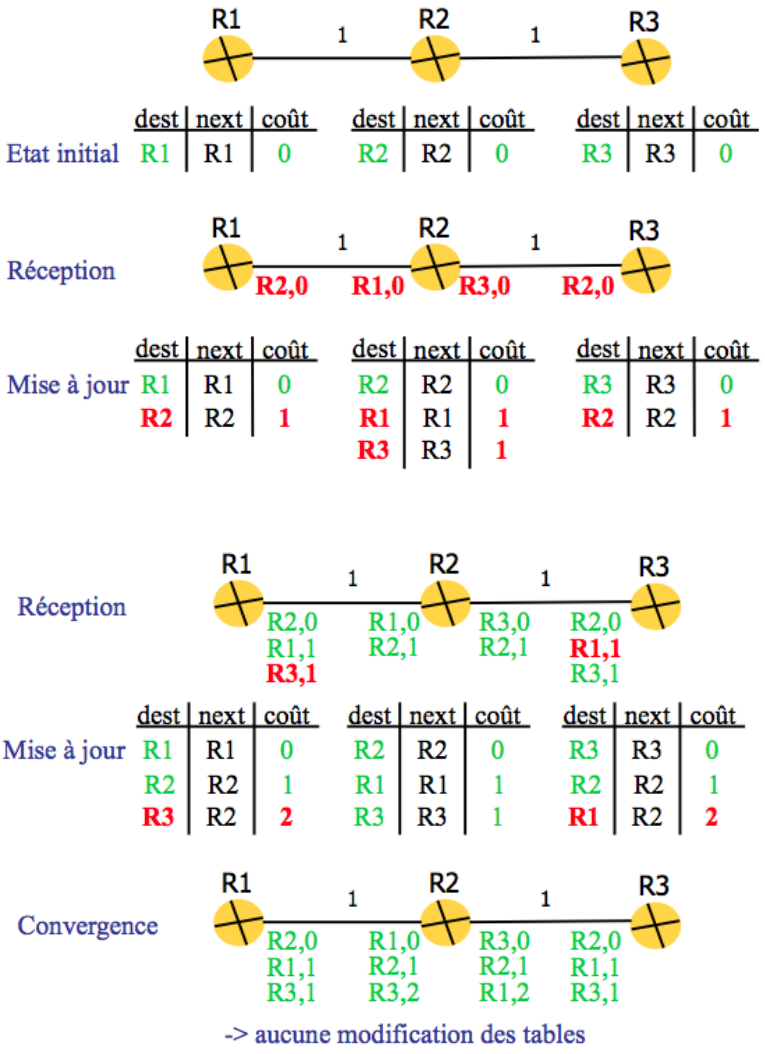
Il existe trois algorithmes de routage dynamique :

6.2.3.1 Routage à Vecteur de distance

Dans le routage à vecteur de distance ou routage de Bellman-Ford (distance vector routing), chaque nœud du réseau maintient une table de routage qui comporte une entrée par nœud du réseau et le coût pour joindre ce nœud. Périodiquement chaque nœud diffuse sa table de routage à ses voisins. Le nœud destinataire apprend ainsi ce que son voisin est capable de joindre. À réception, le nœud compare les informations reçues à sa propre base de connaissance :

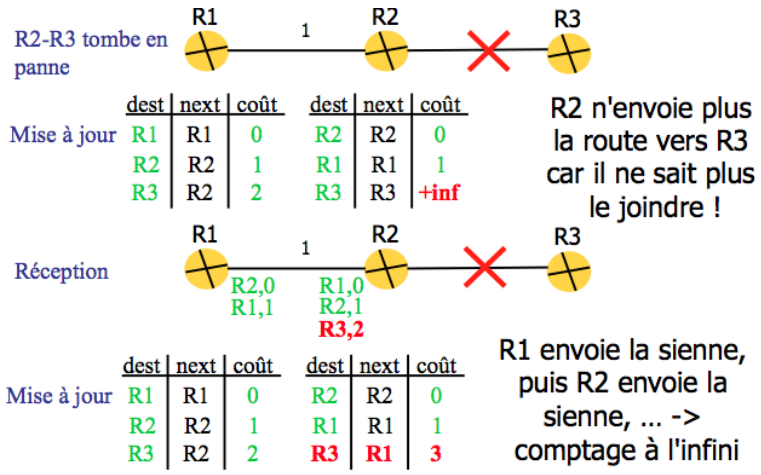
- La table reçue contient une entrée qui n'est pas déjà dans sa propre table, il incrémente le coût de cette entrée du coût affecté au lien par lequel il vient de recevoir cette table et met cette entrée dans sa table. Il a ainsi appris une nouvelle destination.
- La table contient une entrée qu'il connaît déjà. Si le coût calculé (coût reçu incrémenté du coût du lien) est supérieur à l'information qu'il possède, il l'ignore sinon il met sa table à jour de cette nouvelle entrée.

De proche en proche chaque nœud apprend la configuration du réseau et le coût des différents chemins. La convergence des différentes tables peut être assez longue. Les deux figures suivantes en représentent un exemple.



Deux problèmes majeurs peuvent survenir dans cet algorithme en cas de panne d'un lien entre deux routeurs :

1. Les boucles de routage : la panne d'un lien peut conduire à une bouclage infini des paquets dans le réseau. La figure suivante illustre ce phénomène :tous les paquets à destination de R3 oscillent entre R1 et R2



2. l'algorithme ne converge plus : à l'échange suivant, R1 apprend de R2 que désormais le coût pour joindre R3 en passant par R2 est de 3 -> il met sa table à jour (R3, R2, 4) ; de même, R2 va apprendre de R1 que désormais le coût pour joindre R3 est de 4...

Les solutions utilisées consistent à :

- interdire à un nœd de signaler une destination qu'il connaît au routeur par lequel il l'a apprise (split horizon)
- limiter la valeur infinie du coût à une petite valeur (16 dans RIP) -> convergence dés que l'infini est atteint

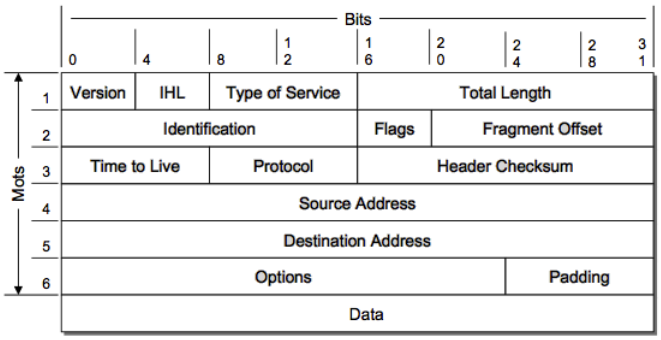
6.3 Protocole IP

Le protocole IP fait partie de la couche Internet de la suite de protocoles TCP/IP. C'est un des protocoles les plus importants d'Internet car il permet l'élaboration et le transport des datagrammes IP (paquets), sans toutefois en assurer la livraison. En réalité, le protocole IP traite les datagrammes IP indépendamment les uns des autres en définissant leur représentation, leur routage et leur expédition.

Le protocole IP détermine le destinataire d'un paquets grâce à trois informations disponible au niveau de chaque machine : l'adresse IP, le masque de sous-réseau, l'adresse de la passerelle par défaut. Les tables de routages établies au niveaux des routeurs permettent de déterminer les routes à suivre par les paquets. Le protocole RIP (routing information protocol) utilisant un algorithme de type vecteur à distance permet de construire et mettre à jour les tables de routage.

6.3.1 Structure d'un paquet IP

Le datagramme IP contient un en-tête IP suivi des données IP provenant des protocoles des couches supérieures.



- Par défaut, la longueur de l'en-tête est de 5 mots de 32 bits (soit 20 octets) ; le sixième mot est facultatif. Puisque la longueur de l'en-tête est variable, elle inclut un champ appelé Internet Header Lenght (IHL - longueur de l'en-tête Internet) en mots.
- Le champ Version fait quatre bits et indique le format de l'en-tête IP (IPv4 ou IPv6).
- Le champ Type of Service (TOS) informe les réseaux de la qualité de service désirée, spécifiant ainsi les délais, le débit et la fiabilité. Les implémentations actuelles ignorent ce champ.
- Le champ Total length (longueur totale) contient la longueur de l'en-tête et des données IP, en octets.
- La durée de vie (Time To Live) représente la durée maximale de vie d'un datagramme sur le réseau. Cette valeur est décrémentée à chaque routeur. Lorsque le champ TTL tombe à 0, datagramme IP est écarté par le routeur.

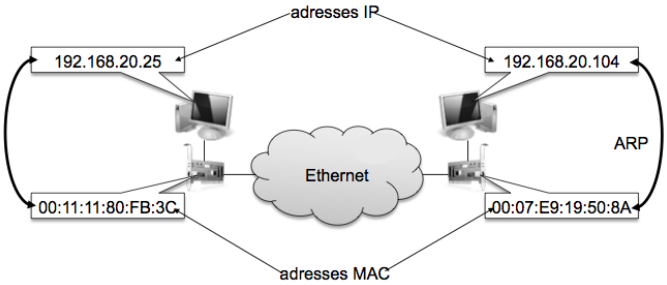
Plusieurs autres protocoles sont utilisés avec le protocole IP dans la couche réseaux notamment :

6.3.2 RIP

RIP (Routing Information Protocol) est un protocole de routage IP de type vecteur distance basé sur l'algorithme de routage décentralisé Bellman-Ford. Il utilise le nombre de sauts (hops) comme métrique de distance entre les machines. Chaque routeur diffuse sa table de routage à ses voisins toutes les 30 secondes. En recevant une table de routage d'un voisin, un routeur met à jour la sienne. Le TTL max étant fixé à 16. Un routeur supprime une information de sa table si elles n'est pas confirmée pour 180 secondes. Il existe deux versions de RIP, la deuxième étant une amélioration de la première : RIPv1 et RIPv2.

6.3.3 ARP

En TCP/IP les interfaces du réseau sont modélisées par un unique identificateur à 32 bits, l'adresse IP. Or la transmission des datagrammes IP sur le réseau physique nécessite que ces datagrammes soient encapsulés dans des trames de couche de liaison de données (couche 2), telles que Ethernet ou Token-Ring, qui elles contiennent des adresses "physiques" (adresses MAC).



Un mécanisme souple, implémenté sous forme d'un protocole distinct et appelé ARP (Address Resolution Protocol) permet de déterminer dynamiquement l'adresse MAC à partir de l'adresse IP d'un hôte.

Pour déterminer l'adresse matérielle de l'hôte B avant de lui envoyer son message, la station A envoie sur le réseau une trame MAC de diffusion, appelée trame ARP de requête. Celle-ci contient les adresses IP et MAC de l'hôte A émetteur, ainsi que l'adresse IP de la destination B. La trame inclut un champ destiné à contenir l'adresse MAC de B. Tous les nœuds du réseau physique reçoivent la trame ARP. Seul l'hôte dont l'adresse IP correspond à l'adresse requise dans la trame de requête ARP répond en encodant sa propre adresse matérielle dans une trame de réponse ARP. L'hôte A initialise alors sa table cache ARP (conservée en mémoire) en utilisant la réponse fournie. Les entrées dans cette table expirent après une temporisation donnée qui peut être configurée dans certaines implémentations de TCP/IP (généralement 15 mn). Le cache ARP est consulté par un hôte juste avant l'envoi d'une requête ARP ; si la réponse se trouve dans le cache, la requête n'est pas effectuée.

6.3.4 RARP

RARP (Reverse ARP) est un mécanisme utilisé par les stations sans disques (terminaux) pour obtenir leur adresse IP auprès d'un serveur distant. Le nœud qui veut connaître sa propre adresse envoie en diffusion une requête RARP. S'il existe plusieurs serveurs RARP, chacun d'eux tente de traiter la requête RARP. Généralement, le client RARP accepte la première réponse reçue et ignore silencieusement les suivantes.

6.3.5 ICMP

Le protocole ICMP (Internet Control Message Protocol) envoie des messages qui réalisent des fonctions de contrôle, de détection des erreurs, et de transmission d'informations pour TCP/IP. Il existe 18 types de messages ICMP.

La commande *traceroute*, par exemple, utilise également des messages ICMP ; elle permet de connaître la route exacte empruntée par les datagrammes. traceroute envoie 3 paquets UDP avec un TTL égal à 1 puis recommence en augmentant le TTL de 1 à chaque envoi. A chaque fois que le TTL arrive à 0, le routeur renvoie un message ICMP d'erreur.

6.3.6 IGMP

IGMP (Internet Group Management Protocol) permet aux machines de déclarer leur appartenance à un ou plusieurs groupes auprès du routeur multipoint dont elles dépendent soit spontanément soit après interrogation du routeur. Celui-ci diffusera alors les datagrammes destinés à ce ou ces groupes. IGMP comprend essentiellement deux types de messages : un message d'interrogation (Host Membership Query), utilisé par les routeurs, pour découvrir et/ou suivre l'existence de membres d'un groupe et un message de réponse (Host Membership Report), délivré en réponse au premier, par au moins un membre du groupe concerné.

6.4 Exercices

Exercice 1 Adresses IP

1. Déterminer les classes des adresses IP suivantes. En déduire les identifiants de réseau et de machine correspondants.

   192.18.97.39 (www.javasoft.com), 138.96.64.15 (www.inria.fr), 18.181.0.31 (www.mit.edu), 226.192.60.40, 91.216.107.152

2. Dites si les adresses IP suivantes sont correctes ou fausses. Justifier votre réponse.

   192.168.262.10, 200.30.1.5.2, 1.12.200.13, 55.255.255.255, 153.12.6, 172.24.15.7, 0.0.0.0

3. Dites si les adresses IP suivantes sont utilisables pour adresser des machines sur Internet. Justifier votre réponse.

   205.0.0.1, 192.168.104.0, 127.17.128.2, 172.125.38.224, 172.217.23.196, 10.148.255.255, 195.14.172.255, 128.0.143.2

Exercice 2 Sous adressage IP

1. Dites si les masques suivant sont corrects ou faux. Justifier votre réponse.

   255.255.11.0, 255.255.255.240, 255.200.255.16, 255.255.255.255, 0.0.0.0, 255.255.255.252

2. On veut émettre un message à tous les hôtes d'un réseau local d'Id 1024. Quelle adresse IP utiliser en format binaire et décimal ?
3. Une machine peut-elle avoir plus d'une adresse IP ? Justifier.
4. Une adresse IP peut-elle être attribuée à plus d'une machine ? Justifier.
5. Donner les plages d'adresses (adresses basse et haute) des différentes classes et préciser le nombre de machines adressables.

Exercice 3 Sous adressage IP

Une entreprise dispose de l'adresse IP 192.168.124.0 pour l'utiliser dans l'adressage de son réseau, et pour une meilleure gestion, l'entreprise décide de le subdiviser en six sous réseaux.

Pour chaque sous réseau, donner en format décimal :

- L'adresse de sous réseau.
- Le nombre de machines adressables.
- La plage d'adresses.
- Le masque de sous réseau.
- L'adresse de diffusion dans le sous-réseau.

Exercice 4 Sous adressage IP

Une machine utilise l'adresse IP **172.16.112.31** et le masque **255.255.224.0**

- Donner l'adresse du réseau auquel appartient cette machine,
- Combien de machines peut-on adresses dans ce réseau ?
- Donnes les adresses la plus basses et la plus haute.
- Donner l'adresse de diffusion.

Exercice 5 Sous adressage IP

Votre entreprise vient d'obtenir l'adresse IP 214.123.155.0. Vous devez créer 10 sous-réseaux distincts pour les 10 succursales de l'entreprise, à partir de cette adresse IP :

- Quel est la classe de ce réseau ?
- Quel masque de sous-réseau devez vous utiliser ?
- Combien d'adresses IP distinctes est-il possible d'utiliser avec un tel masque, tout sous-réseaux possibles confondus ?

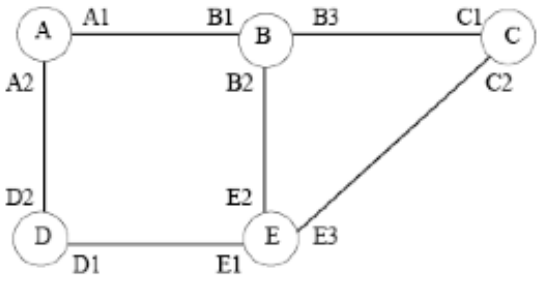
– Combien d'adresses IP (machines ou routeurs) pourra recevoir chaque sous-réseau ?

– Quelle est l'adresse réseau et de broadcast du 5ème sous-réseau utilisable ?

Exercice 6 Sur un réseau Ethernet (Topologie Bus), comment peut-on envoyer une trame à destination de toutes les machines du réseau ? Est-ce que cela charge plus le réseau que d'envoyer une trame à destination d'une seule machine ? (Justifier la réponse).

Exercice 7 Routage à vecteur de distance

Soit le mini-réseau représenté dans la figure ci-dessous :



A, B, C, D et E sont 5 routeurs dont les interfaces sont A1, A2, ... E3 et on suppose qu'ils possèdent les tables de routage suivantes.

table de A

destination	interface	distance
A	locale	0
B	A1	1
D	A2	1

table de B

destination	interface	distance
A	B1	1
B	locale	0
C	B3	1
D	B1	2

table de C

destination	interface	distance
A	C1	2
B	C1	1
C	locale	0
D	C1	3

table de D

destination	interface	distance
A	D2	1
B	D2	2
D	locale	0

table de E

destination	interface	distance
A	E2	2
B	E2	1
C	E3	1
D	E1	1
E	locale	0

– Expliquer brièvement le principe du routage RIP.

– En respectant l'algorithme RIP de construction des tables de routage, donnez l'état des 5 tables de routage une fois que le routeur E aura diffusé sa table à ses voisins. On ne prendra pas en compte d'autres diffusions de tables.

Exercice 8 Routage à vecteur de distance

Un inter-réseau est constitué de réseaux locaux Li et de routeurs Gi. Le tableau suivant indique les liaisons entre les réseaux et les routeurs.

Routeur	Relié à
G1	L1, L3 et L4
G2	L1 et L2
G3	L4 et L5
G4	L2 et L5

On représentera également une station A sur le réseau L1 et une station B sur L3

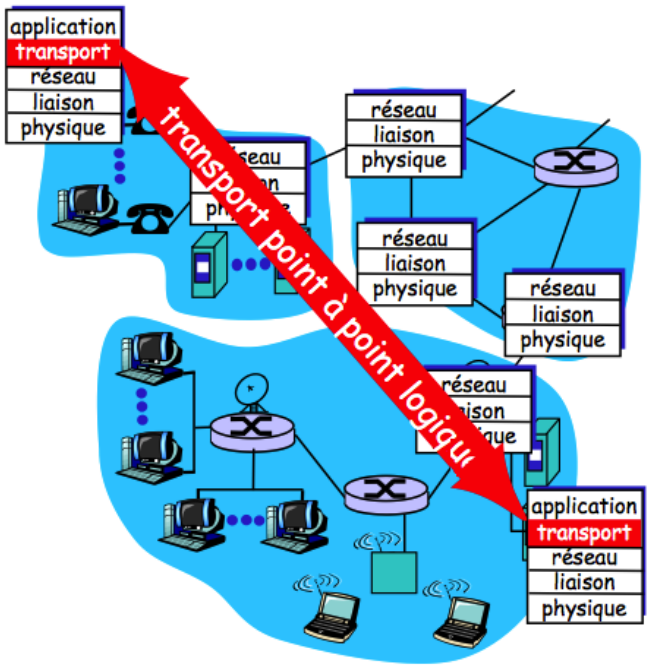
- Faire un schéma du réseau
- Indiquer l'évolution des tables de routage de chaque routeur. Le coût est calculé en nombre de sauts ; il est nul si le réseau est directement accessible. En cas d ?égalité de coût, le chemin vers le routeur de plus petit identificateur sera choisi.
- Au bout de combien d'itérations le procédé converge-t-il ?
- Comment évoluent les tables si G3 tombe en panne ?

Chapitre 7

Couche Transport

Le service fourni par les protocoles de la couche réseaux (IP par exemple) n'étant pas fiable, il faut implanter par dessus un protocole supplémentaire, en fonction de la qualité de service dont les applications ont besoin. Ce protocole est appelé protocole de transport et appartient à la couche OSI numéro 4, la couche transport.

La couche transport assure une communication entre deux machines dans un réseau quelque soit leur localisation en masquant les détails vus dans la couche réseaux tel que le routage. Elle fournit donc une communication logique de bout en bout entre processus tournant sur des machines différentes. Les protocoles de transport tournent sur les hôtes et non pas sur les routeurs.



Il est important de noter qu'il existe une grande ressemblance entres les fonctionnalités de la couche transport 4 et la couche liaison 2. Cependant, la couche liaison adresse las machines tandis que la couche transport adresse les applications. Les tâche essentielles de la couche transport sont les suivantes :

- Segmentation des messages,
- Séquencement des messages,
- Multiplexage et démultiplexage des données des applications,
- Protection contre les éventuelles erreurs,
- Assurer les qualité de service souhaitée par les applications.

7.1 Segmentation des messages

La couche transport émettrice divise (fragmente) le message reçu de la couche supérieure (session pour OSI et application pour TCP/IP) en segments qui les passe à la couche réseau. L'unité de données manipulée par le ouche transport est donc le segment. La couche transport réceptrice, reforme le message à partir des segments obtenus de la couche réseau.

7.2 Séquencement des messages

Si le service offert par la couche réseau n'est pas fiable, la couche transport doit le fiabiliser en garantissant la reconstruction correcte du message pour les application ayant besoin. Pour cela les segments doivent être numérotés et acquittés exactement comme dans la couche liaison, mais ici entre deux applications distantes.

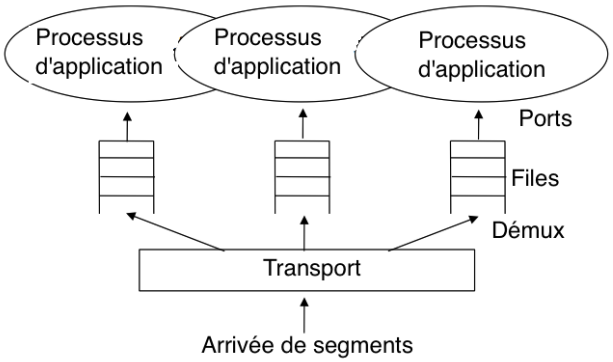
7.3 Multiplexage et démultiplexage

Puisque plusieurs application peuvent tourner sur une machine et peuvent toutes envoyer et recevoir des messages, la couche transport doit pouvoir :

- lors de l'émission, collecter ces données et et les encaplsuler dans le même médium : service multiplexage,
- lors de la réception, livrer les segments reçus aux bonnes applications : service de démultiplexage.

Pour pouvoir distinguer les applications (processus) des unes des autres, elles doivent être identifiées par des adresses. Chaque processus utilisant le réseau doit obtenir une adresse. Par exemple, dans le protocole TCP d'Internet on utilise les numéro de port pour

adresser les applications. Si les trames portent des adresses MAC et les paquets des adresses IP, les segments portent des numéros de port.



Dans le protocole TCP, le numéro de port est un entier représenté sur deux octets. Par exemple, les applications http utilisent le port numéro 80.

7.4 Protection contre les erreurs

En plus de la protection contre les erreurs effectuée à chaque liaison, la couche transport en effectue une autre de bout en bout. Généralement, c'est une somme (checksum) effectuée sur la totalité du segment envoyé. Le champ Checksum est codé sur 16 bits et représente la validité du paquet de la couche 4 TCP.

Pour TCP, le Checksum est constitué en calculant le complément à 1 sur 16 bits de la somme des compléments à 1 des octets de l'en-tête et des données pris deux par deux (mots de 16 bits).

Par example, soit le segment à envoyer est "0x450000304422400080060000 8c7c19acae241e2b". On commence par diviser le segment en blocs de 16 bits chacun puis calculer leurs somme :

$$4500 + 0030 + 4422 + 4000 + 8006 + 0000 + 8c7c + 19ac + ae24 + 1e2b = 2BBCF$$

Puis mettre le résultat en 16 bits par l'ajout du reste au résultat :

$$2 + BBCF = BBD1 = 1011101111010001$$

Finalement, on calcule le complément à 1 du résultat

$$\text{checksum} = \text{complement à un } (1011101111010001) = 0100010000101110 = 442E$$

La vérification chez le récepteur est faite en utilisant le même algorithme avec l'initialisation du checksum à la valeur 442E.

2BBCF + 442E = 2FFFD, alors 2 + FFFD = FFFF

On prend le complément à un de FFFF = 0.

Le segment est correct si le checksum est à 0.

7.5 Protocoles de transport

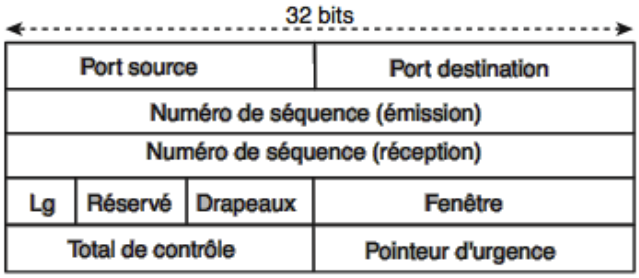
Les applications utilisant les réseaux peuvent avoir besoin de deux type de service : connecté et non connecté. Le service connecté peut être utilisé lorsqu'on connait l'adresse du destinataire au préalable tel que les serveurs http, ou ftp. Tandis que le service non connecté peut être utilisé par exemple pour la diffusion. Le monde d'Internet (TCP/IP) utilise les deux protocoles TCP et UDP correspondant chacun à un service.

7.5.1 TCP

TCP (Transport Control Protocol) assure un service de transmission de données de bout en bout, connecté, fiable avec détection et correction d'erreurs .

7.5.1.1 Format d'un segment TCP

Un segment TCP est constitué comme suit :



- Port Source (16 bits) : Numéro du port utilisé par l'application en cours sur la machine source.
- Port Destination (16 bits) : Numéro du port relatif à l'application en cours sur la machine de destination.
- Numéro d'ordre (32 bits) : numéro du premier octet du flux de données qui sera transmis (Initial Sequence Number)
- Numéro d'accusé de réception (32 bits) : Numéro d'ordre du dernier octet reçu par le récepteur (par rapport à tous les octets du flot de données reçues).

- Longueur en-tête (4 bits) : Il permet de repérer le début des données dans le segment. Ce décalage est essentiel, car il est possible que l'en-tête contienne un champ d'options de taille variable. Un en-tête sans option contient 20 octets, donc le champ longueur contient la valeur 5, l'unité étant le mot de 32 bits (soit 4 octets).
- Réservé (6 bits) : Champ inutilisé.
- Drapeaux ou flags (6 bits) Ces bits sont à considérer individuellement :
  - URG (Urgent) : Si ce drapeau est à 1, le segment transporte des données urgentes dont la place est indiquée par le champ Pointeur d'urgence (voir ci-après).
  - ACK (Acknowledgement) : Si ce drapeau est à 1, le segment transporte un accusé de réception.
  - PSH (Push). Si ce drapeau est à 1, le module TCP récepteur ne doit pas attendre que son tampon de réception soit plein pour délivrer les données à l'application. Au contraire, il doit délivrer le segment immédiatement, quel que soit l'état de son tampon (méthode Push).
  - RST (Reset) : Si ce drapeau est à 1, la connexion est interrompue.
  - SYN (Synchronize) : Si ce drapeau est à 1, les numéros d'ordre sont synchronisés (il s'agit de l'ouverture de connexion).
  - FIN (Final) : Si ce drapeau est à 1, la connexion se termine normalement.
- Fenêtre (16 bits) : Champ permettant de connaître le nombre d'octets que le récepteur est capable de recevoir sans accusé de réception.
- Total de contrôle ou checksum (16 bits). Le total de contrôle est réalisé en faisant la somme des champs de données et de l'en-tête. Il est calculé par le module TCP émetteur et permet au module TCP récepteur de vérifier l'intégrité du segment reçu.
- Pointeur d'urgence (16 bits). Indique le rang à partir duquel l'information est une donnée urgente.
- Options (taille variable).

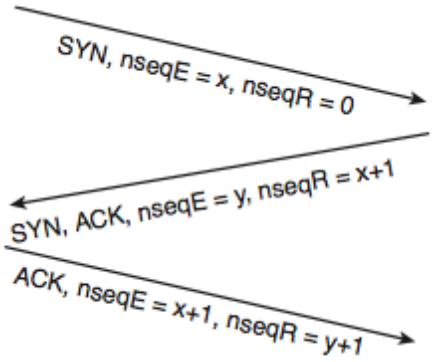
7.5.1.2 Connexion

TCP est un protocole qui fonctionne en mode client/serveur : l'un des utilisateurs est le serveur offrant des services (serveur http : site web), l'autre est le client (client http : navigateur web) qui utilise les services proposés par le serveur.

Le serveur doit être initialisé le premier ; on dit qu'il exécute une ouverture passive. Dès qu'il est opérationnel, il attend les demandes des clients, qui peuvent alors faire une ouverture active. Pour ouvrir une connexion, les clients doivent connaître le numéro de

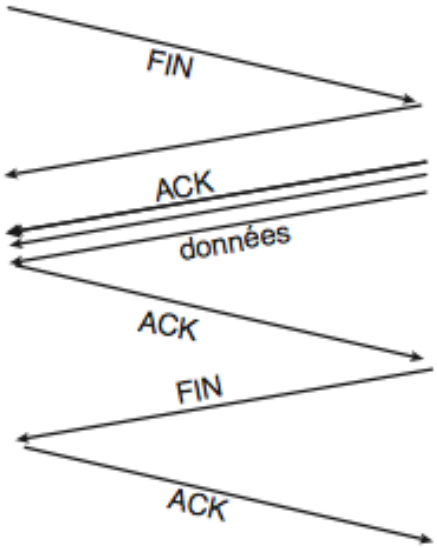
port de l'application distante. En général, les serveurs utilisent des numéros de ports bien connus, mais il est possible d'implanter une application sur un numéro de port quelconque. Il faut alors prévenir les clients pour qu'ils sachent le numéro de port à utiliser.

Le client ouvre la connexion en envoyant un premier segment, parfois appelé séquence de synchronisation. La connexion est établie en trois phases (*three-way-handshake*) en spécifiant les numéro de séquences des octets à échanger.



Une fois la connexion établie, elle peut être utilisée pour échanger les segments dans les deux sens.

La déconnexion est indépendante pour les deux sens ; un échange dans un sens peut être interrompu en gardant celui de l'autre sens. Pour fermer la connexion dans les deux sens, on utilise quatre phases.



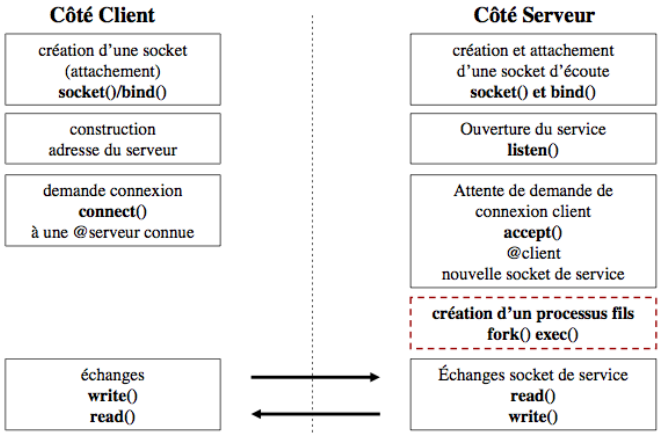
Les applications utilisent un concept appelé socket (initialement développé dans UNIX), permettant d'identifier les différentes communication sur la même machine. Le socket est constitué de la paire :

< adresse IP locale, numéro de port local >

Pour identifier de manière unique l'échange de données avec le processus applicatif distant, le protocole de transport utilise un ensemble de cinq paramètres formé par le nom du protocole utilisé, le socket local et le socket distant :

< protocole, adresse IP locale, numéro de port local ; adresse IP distante, numéro de port distant >

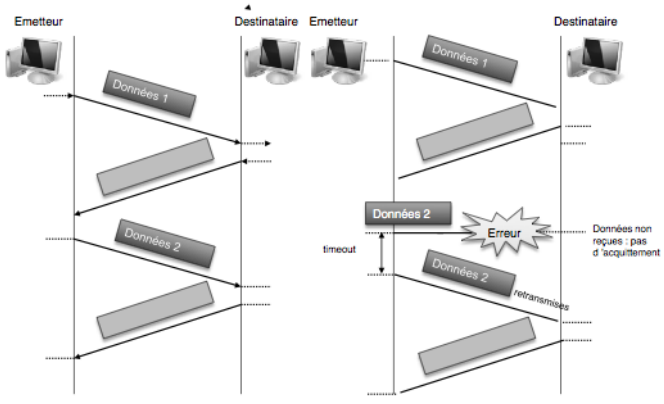
Les serveur peut accepter plusieurs connexions simultanément en créant pour chacune son propore soket avec un processus différent pour sa gestion.



Dans le modèle OSI, les sockets sont gérés par la couche session.

7.5.1.3 Fiabilité

L'utilisation d'un mécanisme appelé PAR (Positive Acknowlegment with Retransmission, Accusé de réception positif avec la retransmission) permet à TCP de garantir des transmissions fiables.



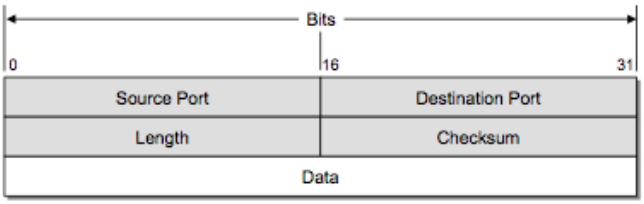
Chaque segment envoyé contient un checksum que le destinataire utilise pour vérifier que les données n'ont pas été endommagées pendant leur transmission. Si le segment est correctement reçu, le récepteur renvoie un accusé de réception positif à l'émetteur. Dans la négative, le récepteur élimine ce segment de données. Après un délai d'attente déterminé, le module TCP d'envoi retransmet les segments pour lesquels aucun accusé de réception positif n'a été reçu.

7.5.2 UDP

Le protocole UDP permet aux applications d'accéder directement à un service de transmission de datagrammes, tel que le service de transmission qu'offre IP. UDP est caractérisé par :

- UDP possède un mécanisme permettant d'identifier les processus d'application à l'aide de numéros de port UDP.
- UDP est orienté datagrammes (sans connexion), ce qui évite les problèmes liés à l'ouverture, au maintien et à la fermeture des connexions.
- UDP est efficace pour les applications en diffusion/multidiffusion. Les applications satisfaisant à un modèle du type "interrogation-réponse" peuvent également utiliser UDP. La réponse peut être utilisée comme étant un accusé de réception positif à l'interrogation. Si une réponse n'est pas reçue dans un certain intervalle de temps, l'application envoie simplement une autre interrogation.
- UDP ne séquence pas les données. La remise conforme des données n'est pas garantie.
- UDP peut éventuellement vérifier l'intégrité des données (et des données seulement) avec un total de contrôle.
- UDP est plus rapide, plus simple et plus efficace que TCP mais il est moins robuste.

Le datagramme UDP est organisé comme suit :



- Port source (16 bits) : Il s'agit du numéro de port correspondant à l'application émettrice du paquet. Ce champ représente une adresse de réponse pour le destinataire.
- Port destination (16 bits) : Contient le port correspondant à l'application de la

machine à laquelle on s'adresse.

– Longueur (16 bits) : Précise la longueur totale du datagramme UDP, exprimée en octets.
– Total de contrôle ou checksum (16 bits). Bloc de contrôle d'erreur destiné à contrôler l'intégrité de l'entête du datagramme UDP.

7.6 Les sockets

Au début des années 80, l'ARPA (Advanced Research Projects Agency du département de la défense américaine) a assigné à l'Université de Berkeley en Californie la responsabilité de construire un système d'exploitation qui pourrait être utilisé comme plate-forme standard pour l'ARPANet, le prédécesseur de l'actuel Internet.

Berkeley, déjà très connu pour son travail sur Unix, a ajouté une nouvelle interface au système d'exploitation pour implémenter les communications réseaux. Cette interface est généralement connue sous le nom de Berkeley-Socket. Sockets Interface (BSD : Berkeley Software Distribution) est à l'origine de presque tout ce qui existe comme interface pour TCP/IP, et à l'origine même des Windows Sockets (WinSock).

7.6.1 Définition d'une socket

Une Socket désigne l'extrémité d'un canal de communication bidirectionnel, elle ressemble beaucoup à un téléphone : En connectant deux sockets ensemble, on peut faire passer des données entre processus, même entre processus s'exécutent sur des machines différentes, exactement de la même façon qu'on parle à travers le téléphone une fois qu'on s'est connecté chez quelqu'un d'autre en l'appelant. Une socket est donc une interface entre les applications des utilisateurs et la couche transport.

Modèle des sockets	**Modèle OSI**
Application utilisant les sockets	Application Présentation Session
UDP/TCP	Transport
IP/ARP	Réseau
Ethernet, X25, ...	Liaison Physique

Les sockets peuvent être utilisée en deux modes de communication :

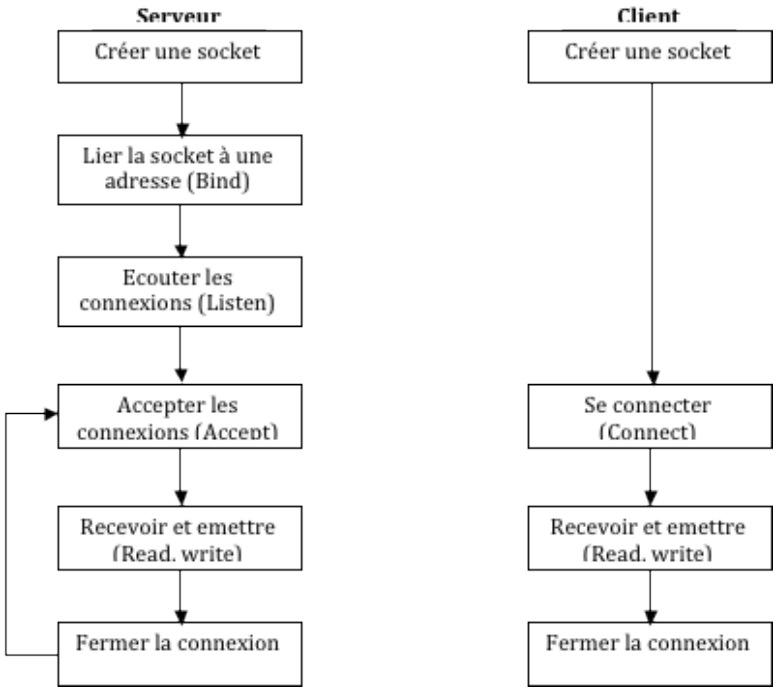
- Le mode connecté (comparable à une communication téléphonique), utilisant le protocole TCP. Dans ce mode de communication, une connexion durable est établie entre les deux processus, de telle façon que l'adresse de destination n'est pas nécessaire à chaque envoi de données.
- Le mode non connecté (analogue à une communication par courrier), utilisant le protocole UDP. Ce mode nécessite l'adresse de destination à chaque envoi, et aucun accusé de réception n'est donné.

Pour faciliter leur utilisation les sockets sont conçues en conservant la sémantique des primitives d'E/S système exactement comme les fichier (création, ouverture, lecture, écriture, fermeture).

Pour communiquer des données entre deux sockets, dans un mode connecté, on doit faire une distinction entre celle utilisée par le programme demandeur de connexion (Client) et celle utilisée par le programme qui accepte les connexions (Serveur).

- Un serveur est un programme qui attend les connexions à travers une Socket et qui gère ensuite toutes les connexions qui arrivent.
- Un client est un programme qui se connecte à un serveur à travers une socket.

Le schéma suivant montre les différentes étapes exécutées par un client et un serveur pour communiquer :



7.6.2 Utilisation des sockets

Les sockets sont généralement implémentés en langage C, et utilisent des fonctions et des structures disponibles dans la librairie <sys/socket.h>.

Pour recevoir des appels téléphoniques, il faut d'abord installer votre téléphone. Pour ce faire, il faut créer une socket pour écouter les connections, un procédé qui se passe en plusieurs étapes :

7.6.2.1 Création d'une socket → Socket()

Ce qui ressemble à se faire installer une ligne de téléphone par la compagnie des télécoms. La fonction socket() necéssite de Spécifier le type de la socket. Les deux types les plus connus sont SOCK_STREAM et SOCK_DGRAM. SOCK_STREAM indique que les données seront transportées par le protocole TCP, alors que SOCK_DGRAM indique que les données seront transportées par le protocole UDP. Nous ne nous intéresserons ici qu'aux sockets SOCK_STREAM, qui sont les plus courantes.

7.6.2.2 Lier la Socket à une adresse → Bind()

Après avoir créé une socket, il faut lui donner une adresse à écouter, de la même façon qu'on prend un numéro de téléphone pour pouvoir recevoir des appels, mais avant ça, on doit spécifier la famille d'adresse à utiliser. Dans le cas de TCP/IP, la famille d'adresse est "AF_INET" où chaque socket a une adresse unique composée de deux éléments : une adresse IP et un numéro de port.

- La première partie est l'adresse IP (comme 192.9.200.10), avec lequel on veut communiquer. Malheureusement, les nombres sont difficiles à retenir, surtout quand on doit travailler avec beaucoup de nombres différents. L'interface la plus utilisée pour retrouver une adresse est la fonction gethostbyname(), qui prend le nom d'un ordinateur et vous renvoie son adresse IP. De même, il est possible de retrouver le nom d'un ordinateur quand on a son adresse IP en utilisant la fonction gethostbyaddr().
- La seconde partie est le numéro de port, qui autorise plusieurs conversations simultanées sur chaque ordinateur. Une application peut soit prendre un numéro de port réservé pour son type d'application, soit en demander un au hasard du système lorsqu'il lie une adresse à sa socket ; une application peut en utiliser plusieurs (un serveur par exemple exploite une socket par client connecté). Les numéros de port sont uniques sur un système donné. Certains numéros sont réservés pour des appli-

cations (ou protocoles) précises, par exemple le port 80 est réservé aux serveurs web (HTTP). Ces ports réservés ont un numéro inférieur à 1024.

Application	Port	Application	Port
echo	7	telnet	23
www	80	pop3	110
ftp	21	smtp	25
kerberos	88	nntp	119
time	37	imap2	143
nameserver	42	irc	194
domain	53	imap3	220

Une connexion est identifiée, donc, de façon unique par la donnée de deux couples, une adresse IP et un numéro de port, un pour le client et un autre pour le serveur. Il est important de noter qu'un dialogue client/serveur n'a pas forcément lieu via un réseau. Il est en effet possible de faire communiquer un client et un serveur sur une même machine, via ce qu'on appelle l'interface de loopback, représentée par convention par l'adresse IP 127.0.0.1.

Pour lier une socket à une adresse on utilise la fonction bind() (to bind veut dire "lier"). Une adresse de socket Internet est spécifié en utilisant la structure sockaddr, qui contient les champs qui spécifient la famille d'adresse, l'adresse et sa longueur.

7.6.2.3 Ecouter les appels → Listen()

Les sockets de type SOCK_STREAM ont la capacité de mettre les requêtes de connexion en files d'attentes, ce qui ressemble au téléphone qui sonne en attendant que l'on réponde. Si c'est occupé, la connexion va attendre qu'on libère la ligne. La fonction listen() est utilisée pour donner le nombre maximum de requêtes en attente avant de refuser les connexions.

7.6.2.4 Accepter les appels → Accept()

Après avoir créé une socket pour recevoir des appels, il faut accepter les appels vers cette socket. La fonction accept() est utilisée pour se faire. Appeler la fonction accept() est équivalent à prendre le combiné lorsque le téléphone sonne. Accept() renvoie une nouvelle socket qui est connecté à celui qui appelle.

7.6.2.5 Appeler une socket → Connect()

Après avoir créé une socket, et après lui avoir donné une adresse, il faut utiliser la fonction connect() pour essayer de se connecter à une socket qui attend les appels ce qui est équivalent à composer numéro d'un téléphone.

7.6.2.6 Emettre et recevoir des données → Send() & Recv()

Maintenant qu'on a une connexion entre deux sockets, on peut envoyer des données entre elles. On utilise les fonctions send() and recv().

7.6.2.7 Fermer une connexion → closesocket()

De la même façon qu'on raccroche après avoir eu quelqu'un au téléphone, il faut fermer la connexion entre les deux sockets. La fonction closesocket() est utilisée pour fermer chaque extrémité de la connexion. Si une des extrémité est fermée et qu'on essaye d'utiliser la fonction send() à l'autre, la fonction send() renverra une erreur. Un recv() qui attend quand la connection à l'autre extrémité est fermé ne retournera aucun octet.

Chapitre 8

Solutions des exercices

8.1 Couche physique

Exercice 1 -

1. Calcule de T_1 et T_2 :
   - durée T_1

     Le Caractère est codé sur 8 bits :

     Taille du fichier $= 320 \times 1024 \times 8 = 2621440\ bits$

     $$9600\ bits \longrightarrow 1\ sec$$
     $$2621440 \longrightarrow T_1$$

     $T_1 = \frac{2621440}{9600} = 273,06 sec$
   - durée T_2 :

     Taille du caractère $= 8 + 1 + 1 + 1 = 11\ bits$

     Taille du fichier $= 320 * 1024 * 11 = 3604480 bits$

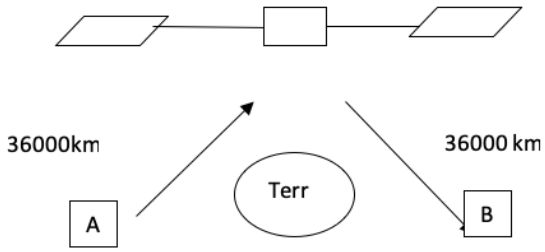
     $$9600\ bits \longrightarrow 1\ sec$$
     $$3604480 \longrightarrow T_2$$

     $T_2 = \frac{3604480}{9600} = 375,46 sec$
   - R= $\frac{T_2 - T_1}{T_2} = 0.27 = 27\%$

     2.
2. $N = 2$ c'est-à-dire on transfert 2 bits à la fois du fichier (valence = 4)

   $T_3 = \frac{3604480}{(2 \times 9600)} = 187.73$

Exercice 2 Transmission par satellite :



1. Calcul du temps T_1 (temps de propagation) :

$$300000\ km - - - - - - > 1\ s$$
$$36000\ km - - - - - - - > X\ s$$

$X = \frac{36000}{300000} = 0.12s$

$T_1 = 2 \times X = 0.12 \times 2 = 0.24\ s$

2. La réponse arrive en $(0.24 \times 2) = 0.48s$

$$64\ kbit \longrightarrow 1\ sec$$
$$Y \longrightarrow 0.48\ s$$

$Y = \frac{64kbits \times 0.48}{1} = 32\ kbits$

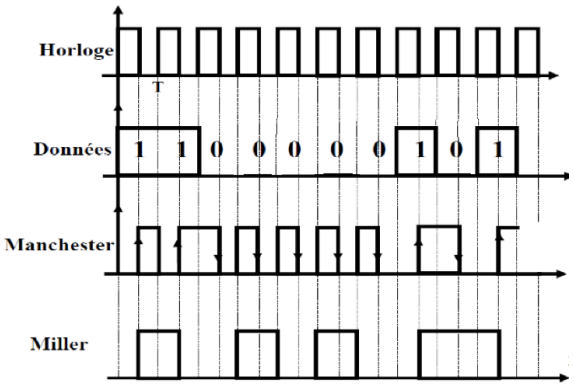
3. Sachant que la station A désire envoyer vers B une chaîne d'informations de taille égale à 96Kbits. Calculer le temps T2 total de transfert de cette chaîne.

Exercice 3 -

1. Capacité $= R = 2 \times W = 2 \times [3400 - 300] = 6200\ bauds$
2. Sachant que le débit de la ligne est de 62 Kbits/s :
   - Débit $= Log_2(V) * R \Rightarrow Log_2(V) = \frac{D}{R} = \frac{62 \times 10^3}{6200} = 10$

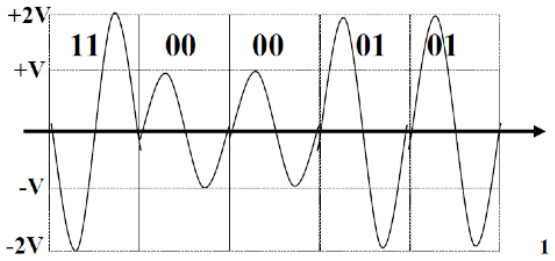
     $V = 2^10 = 1024$
   - $C = Wlog_2(1 + S/B) \Rightarrow S/B = 2^{\frac{C}{W}}?1 = 2^{\frac{6200}{3100}} = 2^2?1 = 3$

     $S/B_{db} = 10log_{10}(3) = 4.77\ db$
3. Code Manchester et Miller :

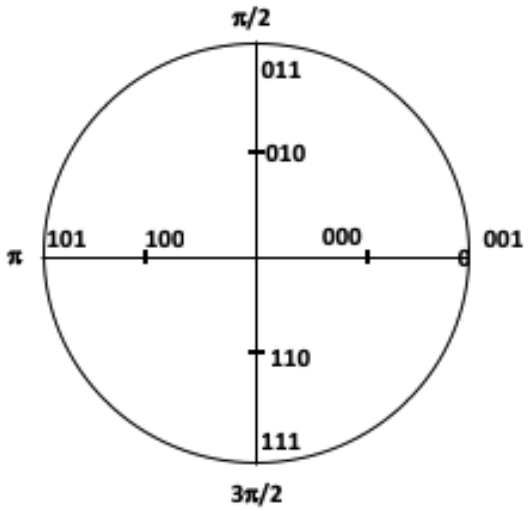


4. -

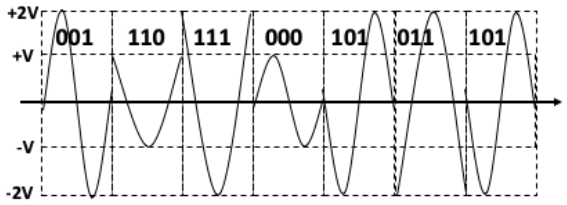
5. Sachant que le codage du signal sur la ligne téléphonique utilise une modulation à deux phases (0 et 180°) et deux amplitudes (V et 2V) :
   - Valence du signal $= 2 \times 2 = 4 \Rightarrow$ Nbre de bits / baud $= log_2(4) = 2$
   - Donner la forme du signal utilisé pour émettre la série de bits précédente de la station S2 au serveur d'accès Internet.



6. Sachant que le codage du signal sur la ligne téléphonique utilise une modulation à quatre phases (0, 90, 180 et 270°) et deux amplitudes (V et 2V) :
   - Valence du signal $= 4 \times 2 = 8 \Rightarrow$ Nbre de bits / baud $= log_2(8) = 3$
   - Cercle des phases et amplitudes



– Forme du signal



7. Débit moyen

   Soit un fichier de 1 Mbits :

   TEthernet $= \frac{1\ Mbits}{10\ Mbits/s} = 0.1\ s$

   Ttél $= \frac{1Mbits}{62\times1000} = \frac{1\times*106}{62\times1000} = \frac{1000}{62} = 16.12\ s$

   $T = 0.1 + 16.12 = 16.22\ s$

   Débit $= \frac{1\ Mbits/s}{16.22\ s} = \frac{106}{16.22} = 61652bit/s = 61.65\ Kbits/s$

Exercice 4 -

1. 02 terminaux sont seulement connectés en même temps.

   On distingue deux cas :

   – soit les deux terminaux ont le même débit (4800 b/s)

   De $= 4800 + 4800 = 9600\ b/s$

   $9600b \Rightarrow 1s$

   $2 \times 10 \Rightarrow T_1$

   $T_1 = \frac{20}{9600} = 2.08\ ms$

– soit le premier a un débit 9600b/s et le deuxième 4800b/s

De $= 9600 + 4800 = 14400$ b/s

$$14400b \Rightarrow 1\ s\ 2 \times 10 \Rightarrow T_1$$

$T1 = \frac{20}{14400} = 1.3\ ms$

2. Seulement 03 terminaux sont connectés en même temps.

– soit les trois terminaux ont le même débit (4800 b/s)

De $= 4800 + 4800 + 4800 = 14400\ b/s$

$$14400b \longrightarrow 1s$$

$$3 * 10 \longrightarrow T_1$$

$T_1 = \frac{30}{14400} 30/14400 = 2.08ms$

– soit le premier a un débit 9600b/s et le deux autre 4800b/s

De $= 9600 + 4800 + 4800 = 19200\ b/s$

$$19200b \longrightarrow 1s$$

$$3 * 10 \longrightarrow T_1$$

$T_1 = 30/19200 = 1.56\ ms$

3. Les 04 terminaux sont connectés en même temps.

De $= 9600 + 4800 + 4800 + 4800 = 24000\ b/s > 19200\ b/s$ impossible

On ne peut pas avoir ce cas car le débit des 4 terminaux dépasse celui de la ligne haute vitesse, il faut donc connecter au maximum 3 terminaux et quand un entre eux termine la transmission le quatrième peut se connecter. C ?est le principe du multiplexeur statistique car il améliore le multiplexage temporel en n ?attribuant la voie haute vitesse qu ?aux voies basses vitesse qui ont effectivement quelque chose à transmettre.

8.2 Couche Liaison de données

Exercice 1 -

1. La chaine de caractères réellement émise :

5	L	a		c	5	o	u	c	h	5	e		l	i	5	a	i	s	o	5	n		e	s
5	t		l	a	5		c	o	u	5	c	h	e		5	n	u	m	é	5	r	o		2
1	.																							

2. – Principe du bit stuffing :
   – À l'émission : ajouter à chaque cinq bits à 1 successifs un bit à 0
   – À la réception : retirer à chaque suite de cinq bits à 1 successifs un bit à 0

– Les données observées sur la voie physique :

0111 1110 0011 0111 0111 11**0**10 0001 0001 1011 111**0**0 **0111 1110**

Exercice 2 -

10011101 10010010 10101000

Exercice 3 -

– $P(X) = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1$

$P(x).x^2 = (x^7 + x^4 + 1).g(x) + (x + 1)$

Le message envoyé est : 001111110111

– Il faut diviser le message rec ?u par le polyno ?me ge ?ne ?rateur : 1010011

Le reste est nul.

La transmission s'est faite correctement. Sachant que le polynôme générateur est de degré 6 donc le reste est de degré 5 (6 bits). Le message émis est 101011.

Exercice 4 -

1. – RR-04
   – SREJ-02
   – REJ-01
   – B ne répond pas : Perte des trames ou perte de la réponse

   Dans les deux cas, après l'écoulement du temps max A retransmet.
2. SABM

   I00, I01, I02, I03

   I04, I05, I06, I06

   I06, I07, I00, I01

   IO2, I03, I04, I05

   I04, I06, I07, I00

   I07, I00, I01, I02

   DISC

Exercice 5 -

1. – Pour garantir la transparence, la suite réellement émise est : 01111011111**0**0011111**0**10001 (nous avons indiqué en gras les bits de transparence).
   – Par suite de l'erreur de transmission, la suite réellement transmise devient ? : 01111 01111110 011111010001. Le récepteur reconnaît un fanion dans la zone grisée : il

considère donc que la trame se termine à cet endroit ! L'erreur est détectée car la trame ne respecte pas le format d ?une trame I (de même, ce qui est pris pour la trame suivante n'a pas d'adresse valide). En outre, les 16 bits précédant le faux fanion sont considérés comme les bits du FCS, qui a toute chance d'être faux. Enfin, un récepteur ignore toute trame comptant moins de cinq octets.

2. **"7E C0 48 4D 41 47 49 53 54 45 52 D3 E1 7E"**

   7E : Fanion (11111110)

   C0 : Adresse (station secondaire réceptrice)

   48 (0100 1000) :

   Trame de type Information : N° trame émise : 04 (100)

   N° trame attendue : 00 (000)

   P/F=1

   "4D 41 47 49 53 54 45 52" : données D3 E1 : champs FCS

   7E Fanion

   "7E 80 BC 02 2D 7E"

   7E : Fanion

   80 : Adresse ?station secondaire émettrice)

   BC : (1011 1100)

   Trame de type S : Commande 11 (rejet selectif SREJ)

   N° trame rejeté : 04 (100)

   P/F=1

   02 2D : FCS

   7E : Fanion

8.3 Réseaux locaux

Exercice 1 -

Il faut que la collision arrive avant que l'émetteur ait fini d'envoyer ses données.

- $T_{emission} = \frac{(64\times8)}{10\times10^2} = 512 \times 10^7 s$
- $T_{aller\ retour} = 2 \times \frac{d_{max}}{V}$
- $d_{max} = 512 \times 10^{-7} \times 2 \times \frac{10^8}{2} = 5120m$

Exercice 2 -

- Diagramme

Temps (slots)	0	1	2	3	4	5	6	7	8	9	10	11	12	13
Trames	A	A	A	A	A	A	$\mathbf{X_1}$	C	C	C	C	C	C	$\mathbf{X_2}$

14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
—	—	D	D	D	D	D	D	B	B	B	B	B	B	…

– Taux d'utilisation = $\frac{26}{28} = 92.85\%$

Exercice 3 -

1. À t=0, D possède le jeton et B veut transmettre 2 trames

   t=0 ⟶ D transmet le jeton

   t=1 ⟶ A reçoit le jeton et le transmet

   t=2 ⟶ B reçoit le jeton et transmet sa 1ère trame

   t=4 ⟶ A veut transmettre 1 trame

   t=6 ⟶ B a fini de transmettre sa 1ère trame

   t=8 ⟶ D veut transmettre 1 trame

   t=10 ⟶ B reçoit sa propre trame et la retire (elle a parcouru l'anneau) puis transmet le jeton

   t=12 ⟶ D reçoit le jeton et transmet sa trame

   t=20 ⟶ D reçoit sa propre trame et la retire puis transmet le jeton

   t=21 ⟶ A reçoit le jeton et transmet sa trame

   t=23 ⟶ C veut transmettre 2 trames

   t=29 ⟶ A reçoit sa propre trame et la retire puis translet le jeton

   t=30 ⟶ B reçoit le jeton et transmet sa 2ème trame

   t=38 ⟶ B reçoit sa propre trame et la retire pui transmet le jeton

   t=39 ⟶ C reçoit le jeton et transmet sa 1ère trame

   t=47 ⟶ C reçoit sa propre trame et la retire puis transmet le jeton

   t=51 ⟶ C reçoit le jeton (qui a parcouru l'anneau) et transmet sa 2ème trame

   t=59 ⟶ C reçoit sa propre trame et la retire puis transmet le jeton

2. d'où la durée du scenario 59s.

3. Quant au temps d'accès, il suffit de remarquer que

   A transmet sa trame à t=21 alors qu'elle était prête à t=4 donc 21-4=17 ms d'attente

   Pour la 1ère trame de B, le temps d'attente est 2-0=2 ms

Pour la 2ème trame de B, temps d'attente 30-0=30 ms

Pour la 1ère trame de C, temps d'attente 39-23=16 ms

Pour la 2ème trame de C, temps d'attente 51-23=28 ms

Pour la trame de D, temps d'attente 12-8=4 ms

d'où temps d'attente moyen (17+2+30+16+28+4)/6 = 16 ms

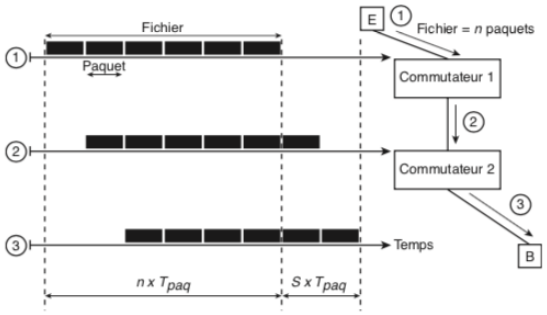
Exercice 4 -

1. T1 = 2 t1 + 8 t2
2. T2 = 2 t0 + T1 + t0 = 3 t0 + 2 t1 + 8 t2
3. T3 = 2 t2 + 3 t1

8.4 Réseaux grande distance

Exercice 1 Commutation

1. La durée de transmission du fichier sur une liaison est égale à : Tfic =(L + H)/D. La durée de transmission du fichier est égale au temps de transmission sur toutes les liaisons traversées, c'est-à-dire : Tfic1 = Tfic*(S + 1).
2. La durée de transmission d'un paquet sur une liaison de données vaut : Tpaq = (P + H)/D. La durée de transmission du fichier est égale à la durée de transmission des paquets jusqu'au premier commutateur, plus le délai nécessaire au dernier paquet pour parvenir jusqu'à B. Le nombre de paquets nécessaires pour transmettre le fichier vaut n = L/P. On en déduit : Tfic2 = (S + n)*Tpaq = (S + n)*(P + H)/D.



3. Applications numériques :

(a) Cas de la commutation de messages : P = L = 64 000*8 = 512 000 bits

Tfic1 = (2 + 1)*(64 000 + 9)*8/64 000 = 24 s.

(b) Cas de la commutation de paquets avec P = 128 octets = 128*8 = 1 024 bits ; n = L/P = 500 paquets

Tfic2 = (2 + 500)*(128 + 9)*8/64 000 = 8,6 s.

(c) Cas de la commutation de paquets avec P = 16 octets = 16*8 = 128 bits ; n = L/P = 4 000 paquets

Tfic2 = (2 + 4 000)*(16 + 9)*8/64 000 = 12,5 s.

(d) Cas de la commutation de cellules ATM avec P = 48 octets = 48*8 = 384 bits ; H = 5 octets ; n = L/P = 1 334 paquets (par excès)

Tfic2 = (2 + 1 334)*(48 + 5)*8/64 000 = 8,85 s.

8.5 Couche Réseaux

Exercice 1 Adresses IP

1. Déterminer les classes des adresses IP suivantes. En déduire les identifiants de réseau et de machine correspondants.

Adresse IP	1er octet binaire	Classe	ID réseau	Id machine
192.18.97.39	11000000	C	192.18.97	39
138.96.64.15	10001010	B	138.96	64.15
18.181.0.31	00010010	A	18	181.0.31
226.192.60.40	11100010	D	/	/
91.216.107.152	01011011	A	91	216.107.15

2. Dites si les adresses IP suivantes sont correctes ou fausses. Justifier votre réponse.
3. Dites si les adresses IP suivantes sont utilisables pour adresser des machines sur Internet. Justifier votre réponse.

Exercice 2 Sous adressage IP

1. Dites si les masques suivant sont corrects ou faux. Justifier votre réponse.

Adresse	Correcte/fasse	Justification
192.168.262.10	Fausse	Troisième octet > 255
200.30.1.5.2	Fausse	Composée de 5 octets
1.12.200.13	Correcte	
55.255.255.255	Correcte	
153.12.60	Fausse	composée de 3 octets
172.24.15.7	Correcte	
0.0.0.0	Correcte	particulière

Adresse	Utilisable/non	Justification
205.0.0.1	Utilisable	/
192.168.104.0	non	adresse réservée
127.17.128.2	non	adresse réservée
172.125.38.224	Utilisable	
172.217.23.196	Utilisable	
10.148.255.255	non	adresse réservée
195.14.172.255	Utilisable	
128.0.143.2	Utilisable	

Masque	Binaire	Correct/Faux	Justification
255.255.11.0	111111111.111111111.00001011.0000000	Faux	des zéros entre les uns
255.255.255.240	111111111.111111111.111111111.11110000	correct	
255.200.255.16	111111111.110011000.111111111.00010000	Faux	des zéros entre les uns
255.255.255.255	111111111.111111111.111111111.111111111	Faux	pas de partie machine
0.0.0.0	00000000.00000000.00000000.00000000	Faux	pas de partie réseaux
255.255.255.252	111111111.111111111.111111111.11111100	Correct	

2. On veut émettre un message à tous les hôtes d'un réseau local d'Id 1024. Quelle adresse IP utiliser en format binaire et décimal ?
   - Réseau local ⇒ Classe C (110) : Id réseau 3 octets et Id machine 1 octet
   - Id Réseau = 1024 = 10000000000
   - Message à toutes les machines du réseau ⇒ adresse de diffusion ⇒ Id machine = 11111111
   - Adresse IP = 110 00000.00000100.00000000.11111111 = 192.4.0.255

3. Une machine peut-elle avoir plus d'une adresse IP ? Justifier.

   Oui, si elle est connecté à plus d'un réseaux. Dans chaque réseaux, elle possède une adresse.

4. Une adresse IP peut-elle être attribuée à plus d'une machine ? Justifier.

   Non, puisque l'adresse sert à identifier une seule machine dans le réseau

5. Donner les plages d'adresses (adresses basse et haute) des différentes classes et préciser le nombre de machines adressables.

Classe	@ basse	@ haute	Nb réseaux	Nb machines/réseau	Nb machines adressables
A	0.0.0.0	127.255.255.255	$2^7 - 2$	$2^{24} - 2$	$(2^7 - 2) \times (2^{24} - 2)$
B	128.0.0.0	191.255.255.255	$2^{14} - 2$	$2^{16} - 2$	$(2^{14} - 2) \times (2^{16} - 2)$
C	192.0.0.0	224.255.255.255	$2^{21} - 2$	$2^8 - 2$	$(2^{21} - 2) \times (2^8 - 2)$

Exercice 3 Une entreprise dispose de l'adresse IP 192.168.124.0 pour l'utiliser dans l'adressage de son réseau, et pour une meilleure gestion, l'entreprise décide de le subdiviser en six sous réseaux.

Pour chaque sous réseau, donner en format décimal :

- L'adresse de sous réseau.
- Le nombre de machines adressables.
- La plage d'adresses.
- Le masque de sous réseau.
- L'adresse de diffusion dans le sous-réseau.
- Nombre de sous réseaux = 6 $\Rightarrow$ nbre de bits sous réseau = 3
- Nbre de bits machines = 8 - 3 =5

N°	@ sous-réseau	# Mach	@ basse	@ haute	masque	@ diffusion
1	192.168.124.32	30	192.168.124.33	192.168.124.62	255.255.255.224	192.168.124.63
2	192.168.124.64	30	192.168.124.65	192.168.124.94	255.255.255.224	192.168.124.95
3	192.168.124.96	30	192.168.124.97	192.168.124.126	255.255.255.224	192.168.124.127
4	192.168.124.128	30	192.168.124.129	192.168.124.158	255.255.255.224	192.168.124.159
5	192.168.124.160	30	192.168.124.161	192.168.124.190	255.255.255.224	192.168.124.191
6	192.168.124.192	30	192.168.124.193	192.168.124.222	255.255.255.224	192.168.124.223

Exercice 4 Une machine utilise l'adresse IP **172.16.112.31** et le masque **255.255.224.0**

- Donner l'adresse du réseau auquel appartient cette machine,

  - Adresse de la machine = 1010 1100.0001 0000.0111 0000.0001 1111
  - Masque = 1111 1111.1111 1111.1110 0000.0000 0000
  - @ réseau = @ machine && masque
  - @ réseau = 1010 1100.0001 0000.0110 0000.0000 0000
  - = 172.16.96.0
- Combien de machines peut-on adresses dans ce réseau ?
  - $2^{13} - 2 = 8190$ machines
- Donnes les adresses la plus basses et la plus haute.
  - @ basse : 1010 1100.0001 0000.0110 0000.0000 0001 = 172.16.96 .1
  - @ haute : 1010 1100.0001 0000.0111 1111.1111 1110 = 172.16.127 .254
- Donner l'adresse de diffusion.
  - @ de diffusion : 1010 1100.0001 0000.0111 1111.1111 1110 = 172.16.127 .255

Exercice 5 Votre entreprise vient d'obtenir l'adresse IP 214.123.155.0. Vous devez créer 10 sous-réseaux distincts pour les 10 succursales de l'entreprise, à partir de cette adresse IP :

- Quel est la classe de ce réseau ?
  - Classe C $\Rightarrow$ 24 bits pour réseau, 4 bits pour sous réseau et 4 bites pour machines
- Quel masque de sous-réseau devez vous utiliser ?
  - Masque = 255.255.255.11110000
  - Masque = 255.255.255.240
- Combien d'adresses IP distinctes est-il possible d'utiliser avec un tel masque, tout sous-réseaux possibles confondus ?
  - $(2^4 - 2) \times (2^4 - 2) = 14 \times 14 = 196$
- Combien d'adresses IP (machines ou routeurs) pourra recevoir chaque sous-réseau ?
  - $(2^4 - 2) = 14$
- Quelle est l'adresse réseau et de broadcast du 5ème sous-réseau utilisable ?
  - 214.123.155.0101 1111 = 214.123.155.97

Exercice 6 Sur un réseau Ethernet (Topologie Bus), comment peut-on envoyer une trame à destination de toutes les machines du réseau ?

- En mettant tous les bits de la partie machine à 1 ou en utilisant l'adresse all ones (255.255.255.255)

Est-ce que cela charge plus le réseau que d'envoyer une trame à destination d'une seule machine ? (Justifier la réponse).

– Non au contraire cela permet d'optimiser l'utilisation du réseau puisqu'on envoie une seule trame à toutes les machines au lieu d'en envoyer plusieurs.

Exercice 7 -

TC :

Destination	Interface	Distance
A	C1	2
B	C1	1
C	Locale	0
D	C2	2
E	C2	1

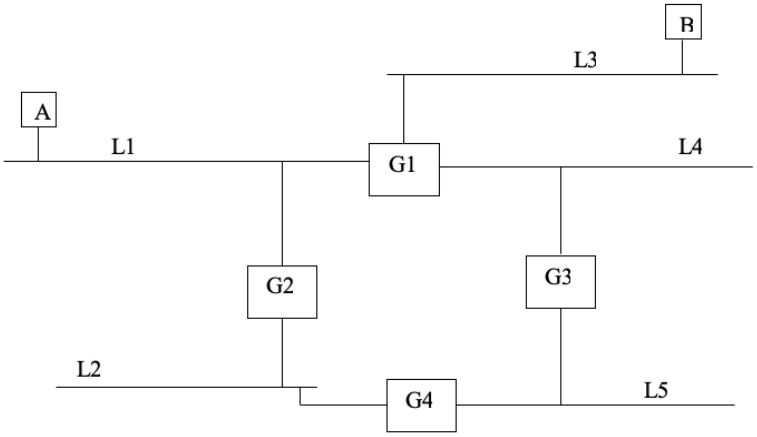
TB :

Destination	Interface	Distance
A	B1	1
B	Locale	0
C	B3	1
D	B1	2
E	B2	1

TD :

Destination	Interface	Distance
A	D2	1
B	D2	2
C	Locale	0
D	D1	2
E	D1	1

Exercice 8 -



–

– Initialement les tables sont les suivantes :

TG1 TG2

Destination	Interface	Distance	Destination	Interface	Distance
L1	Locale	0	L1	Locale	0
L3	Locale	0	L2	Locale	0
L4	Locale	0			

TG3 TG4

Destination	Interface	Distance	Destination	Interface	Distance
L4	Locale	0	L2	Locale	0
L5	Locale	0	L5	Locale	0

– Après la convergence :

TG1 TG2

Destination	Interface	Distance	Destination	Interface	Distance
L1	Locale	0	L1	Locale	0
L3	Locale	0	L2	Locale	0
L4	Locale	0	L3	G1	1
L2	G1	1	L3	G1	1
L5	G1	2	L3	G4	1

TG3 TG4

Destination	Interface	Distance	Destination	Interface	Distance
L4	Locale	0	L2	Locale	0
L5	Locale	0	L5	Locale	0
L1	G1	1	L1	G2	1
L2	G4	1	L3	G2	2
L3	G1	1	L4	G3	1

Chapitre 9

Sujets d'examens

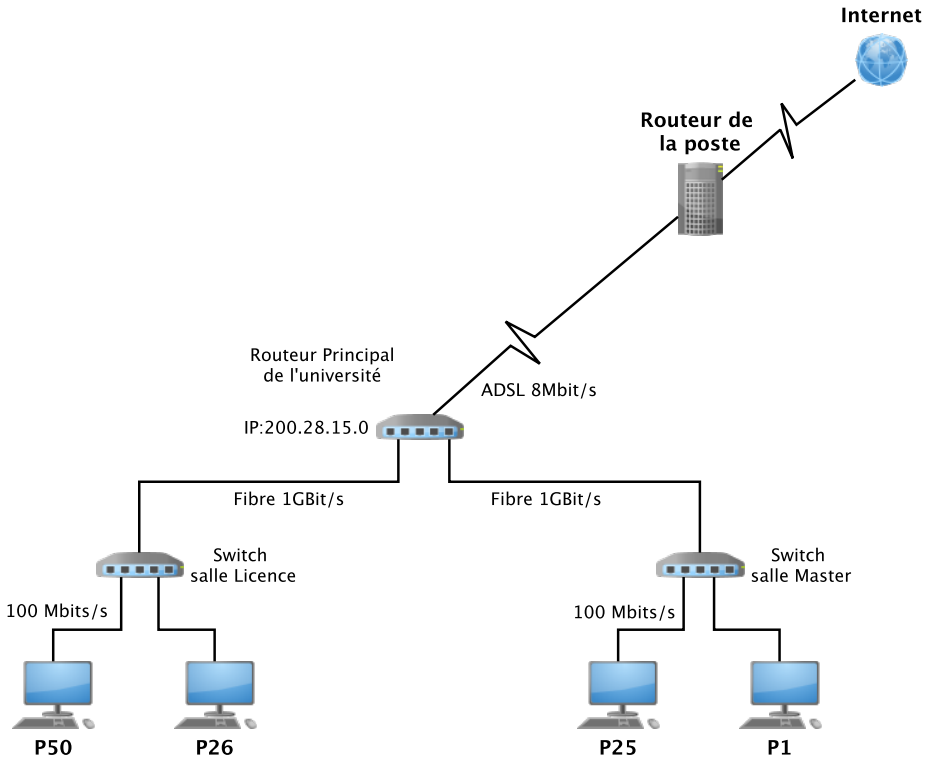
Université Mohamed Khider-Biskra
Faculté des Sciences Exactes et des Sciences de la Nature et de la Vie
Département d'informatique

$2^{ème}$ année LMD
13 Mai 2015

Réseaux de communication
08:00-09:30 A1, A2

Examen

Soit le réseau représenté dans la figure suivante :



Le réseau permet de relier les ordinateurs des deux salles d'un département d'informatique : la salle Master et la salle Licence. Les postes de chaque salle sont reliés par un réseau Ethernet de 100 Mbits/s à travers un switch. Chacun des deux switchs est relié au routeur de l'université par une liaison fibre optique de 1Gbit/s. Ce dernier est relié au routeur de la poste par une liaison ADSL de 8Mbits/s.

Exercice 1 Couche physique (8 pts : 2 + 4 + 2)

1. Le poste P1 envoie le message [**1000101101**] au poste P2 en utilisant le code Miller. Donner la forme du signal émis.
2. Le même message est retransmis du Routeur de l'université via la liaison téléphonique en utilisant une modulation en large bande combinant deux phases $(\frac{\pi}{2}, \frac{3\pi}{2})$ et deux amplitudes (A_1, A_2). Proposer un codage convenant puis donner la forme du signal émis.
3. Un fichier de 2 MOctets est envoyé du poste P1 vers le routeur de la poste (en utilisant une commutation de message)
   (a) Calculer le temps de transfert du fichier.
   (b) Calculer le débit moyen entre le poste P1 et le routeur de la poste.

Exercice 2 Couche Liaison (8 pts : 3 + 3 + 2)

1. Le réseau de la salle Master utilise le polynome générateur $G(x) = x^6 + x^4 + 1$ pour la protection contre les erreurs au niveau de la couche Liaison de données.
   (a) Le poste P1 veut envoyer le message [**100010110**] à P5. Donner le message réellement émis.
   (b) Le psote P1 reçoit le message [**110010101100**]. Que peut-il conclure ?
2. Le protocole HDLC (High level Data Link Control) défini par l'ISO est utilisé pour la gestion du dialogue dans le réseau de la salle Master. En supposant que la taille de la fenêtre = 8 (0..7) et que la station émettrice n'envoie que 04 trames d'informations I numérotées puis se place en attente d'un accusé de réception.
   (a) On vous demande de déterminer la suite de trames émises du poste P1 en fonction de la suite des trames de supervision S/U suivantes envoyées par le poste récepteur P5 :

t_0	t_1	t_2	t_3	t_4	t_5	t_6	t_7	t_8
UA	SREJ-01	RR-07	REJ-00	RR-04	SREJ-05	RR-06	UA	fin

   (b) Donner la représentation en hexadécimal des deux trames **REJ-00** et **RR-04** en supposant que le champs Adresse est "80" et FCS est "FF".

Exercice 3 Couche réseaux (4 pts : 0.5 + 1 + 2 + 0.5)

L'université dispose de l'adresse IP **200.28.15.0**

1. À quelle classe appartient cette adresse ?
2. Déterminer le masque de sous réseau permettant de subdiviser cette adresse sur les deux sous réseaux ; salle Master et salle Licence.
3. Pour chacun des deux sous réseaux déterminer son adresse de réseau, son adresse de diffusion et le nombre de machines adressables.
4. Combien de salles pareilles du département qui peuvent encore être connectées au réseau de l'université selon ce plan d'adressage ?

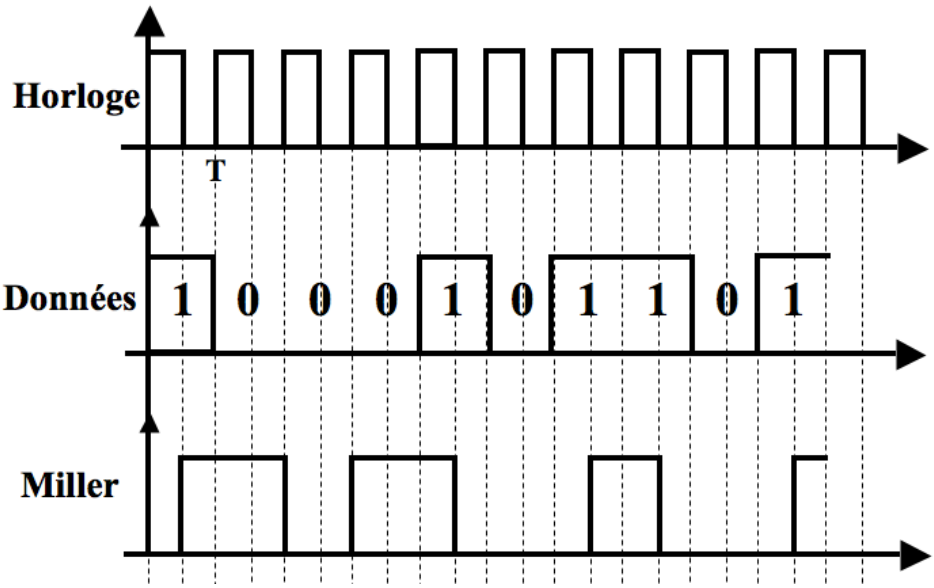
Bonne chance

Dr A.Djeffal, Dr A. Bachir, K. Djaber

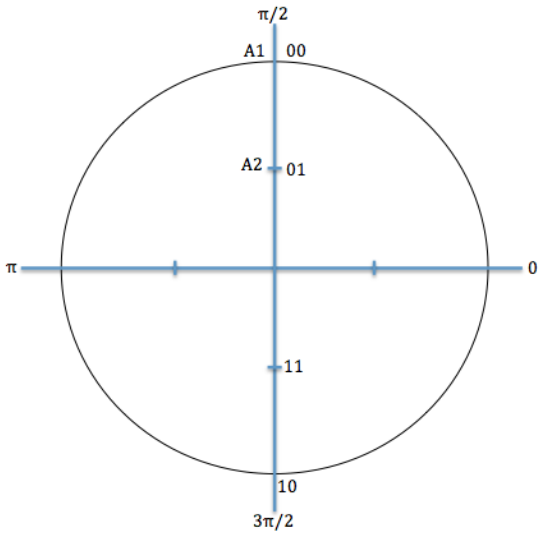
Corrigé type

Exercice 1 : Couche physique (8 pts : 2 + 4 + 2)

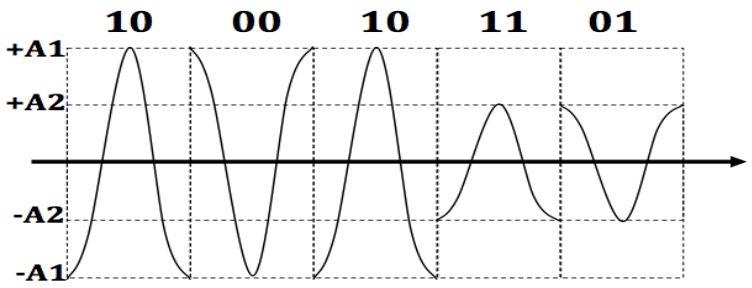
1. Code Miller (2 pts)



2. Proposition d'un codage combiné phase ($\frac{\pi}{2}$,$\frac{3\pi}{2}$) et amplitude (A1,A2) (2 pts)



Signal codé : Valence du signal = $2 \times 2 = 4 \Rightarrow$ nombre de bits d'un code = $log_2(4) = 2$



(2 pts)

3. – Temps de transfert de P1 vers le switch de la salle = $\frac{2\times8\times10^6 bit}{100\times10^6 bit/s} = 0.16s$

- Temps de transfert du Switch vers le routeur de l'université = $\frac{2\times8\times10^6 bit}{10^9 bit/s} = 0.016s$
- Temps de transfert du routeur de l'université vers le routeur de la poste = $\frac{2\times8\times10^6 bit}{8\times10^6 bit/s} = 2s$ (0.5 pt)
- **Temps total de transfert =** $0.16 + 0.016 + 2 = 2.176s$ (0.5 pt)
- **Débit moyen =** $\frac{2\times8\times10^6 bit}{2.176} \approx 7.35\ Mbit/s$ (1 pt)

Exercice 1 : Couche liaison (8 pts : 3 + 3 + 2)

1. Polynôme générateur $G(x) = x^6 + x^4 + 1$

   (a) Le poste P1 veut envoyer le message [**100010110**] à P5 :
   Message original = 100010110 $\Rightarrow M(x) = x^8 + x^4 + x^2 + x$
   $G(x) = x^6 + x^4 + 1$
   $M(x).x^6 = x^{14} + x^{10} + x^8 + x^7$

x^{14}	+	x^{10}	+	x^8	+	x^7		x^6	+	x^4	+	1
x^{14}	+	x^{12}	+	x^8			x^8	+	x^6	+	x	+ 1
x^{12}	+	x^{10}	+	x^7								
x^{12}	+	x^{10}	+	x^6								
x^7	+	x^6										
x^7	+	x^5	+	x								
x^6	+	x^5	+	x								
x^6	+	x^4	+	1								
x^5	+	x^4	+	x	+	1						

   $R(x) = x^5 + x^4 + x + 1 = (110011)_2$
   Le message à envoyer $T(x) = M(x).x^r - R(x) = x^{14} + x^10 + x^8 + x^7 + x^5 + x^4 + x + 1 = (100010110110011)_2$ (1.5 pt)

   (b) Le psote P1 reçoit le message [**110010101100**] :
   $T(x) = x^{11} + x^{10} + x^7 + x^5 + x^3 + x^2$

x^{11}	+	x^{10}	+	x^7	+	x^5	+	x^3	+	x^2		x^6	+	x^4	+	1		
x^{11}	+	x^9	+	x^5							x^5	+	x^4	+	x^3	+	x^2	+ 1
x^{10}	+	x^9	+	x^7	+	x^3	+	x^2										
x^{10}	+	x^8	+	x^4														
x^9	+	x^8	+	x^7	+	x^4	+	x^3	+	x^2								
x^9	+	x^7	+	x^3														
x^8	+	x^4	+	x^2														
x^8	+	x^6	+	x^2														
x^6	+	x^4																
x^6	+	x^4	+	1														
1																		

   Reste = $1 \neq 0 \Rightarrow$ Message erroné (1.5 pt)

2. Trames émises par P1 (1.5 pt)

t_0	SABM
t_1	I00,I01,I02,I03
t_2	I01,I04,I05,I06
t_3	I07,I00,I01,I02
t_4	I00,I01,I02,I03
t_5	I04,I05,I06,I07
t_6	I05 (P/F=1)
t_7	DISC

(3 pts)

3. Représentation hexadécimale des trames
   - **REJ-00 :**
     Fanion : 7E
     Adresse : 80
     Commande : 10 (trame S), 10 (REJ), 1 (P/F), 000 = $(10101000)_2 = (A8)_{16}$
     FCS : FF
     Fanion : 7E
     Trame : 7E80A8FF7E (1 pt)
   - **RR-04 :**
     Fanion : 7E
     Adresse : 80
     Commande : 10 (trame S), 00 (RR), 0 (P/F), 100 (04) = $(10000100)_2 = (84)_{16}$
     FCS : FF
     Fanion : 7E
     Trame : 7E8084FF7E (1 pt)

Exercice 3 : Couche réseaux (4 pts)

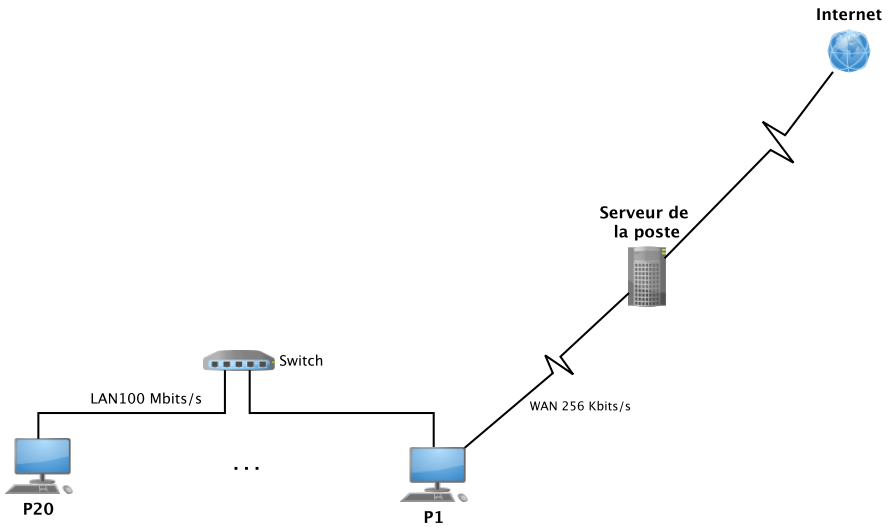
1. Classe C (0.5 pt)
2. Nombre de machines/sous-réseaux = 25 $\Rightarrow$ nombre de bits nécessaires pour les machines = $log_2(25) = 4, .. \Rightarrow 5$
   Nombre de bits pour les sous-réseaux = 8 - 5 = 3
   Masque = 255.255.255.$(11100000)_2$ = **255.255.255.224** (1 pt)
3. **Sous-réseau 1 :**
   Adresse : 200.28.15.32
   Adresse de diffusion : 200.28.15.63
   Nombre de machines adressables = $2^5 - 2 = 30$ (1 pt)
   Sous-réseau 2 :
   Adresse : 200.28.15.64
   Adresse de diffusion : 200.28.15.95
   Nombre de machines adressables = $2^5 - 2 = 30$ (1 pt)
4. Nombre de salles pareilles qui peuvent être encore ajoutées = $2^3 - 2 - 2 = 6$ (0.5 pt)

Université Mohamed Khider-Biskra
Faculté des Sciences Exactes et des Sciences de la Nature et de la Vie
Département d'informatique

$2^{ème}$ année LMD — Réseaux de communication
14 Mai 2016 — 10:00-11:30 A1, A2, A3, S1

Examen

Soit le réseau représenté dans la figure suivante :



Les postes de P1 à P20 sont reliés par le réseau LAN offrant un débit de 10 Mbits/s à travers le switch. Le poste P1 est relié aussi au réseau WAN de la poste offrant un débit de 256 Kbits/s à travers une carte modem.

Exercice 1 Couche physique (8 pts : 3 + 3 + 2)

1. La communication dans le réseau LAN utilise la transmission dite en bande de base :
   (a) Pourquoi cette appellation ?
   (b) Pourquoi nécessite-t-elle un codage ?
   (c) Le poste P20 désire envoyer à P1 la chaine binaire [**11001010**]. Donner la forme du signal émis sachant que le codage utilisé est celui de Manchester différentiel.
2. La communication dans le réseau WAN utilise la transmission dite large bande :
   (a) Donner une autre appellation de ce type de transmission.
   (b) Le poste P1 retransmet la même chaine reçue de P20 vers le serveur de la poste. Sachant que la modulation utilisée est de type FSK exploitant quatre fréquences, donner la forme du signal émis.
3. Calculer le temps de transfert d'un fichier de 3 MOctets du poste P20 au serveur de la poste (On néglige le temps de traitement au niveau des postes). En déduire le débit moyen entre P20 et le serveur de la poste.

Exercice 2 Couche Liaison (9 pts : 3 + 6)

1. La couche liaison de données du réseau LAN utilise le polynome générateur $G(x) = x^5 + x^2 + 1$ pour la protection contre les erreurs.
   (a) Le poste P1 veut envoyer le message [**100010110**] à P20. Donner le message réellement émis.
   (b) Le psote P1 reçoit le message [**110010101100**]. Que peut-il conclure ?
2. Le protocole HDLC (High level Data Link Control) défini par l'ISO est utilisé pour la gestion du dialogue dans le réseau LAN. En supposant que la taille de la fenêtre = 8 (0..7) et que la station émettrice n'envoie que 04 trames d'informations I numérotées puis se place en attente d'un accusé de réception.
   (a) Pourquoi la numérotation des trames est nécéssaire pour le bon fonctionnement du dialogue dans ce protocole ?
   (b) On vous demande de déterminer la suite de trames de supervision S/U émises par le poste P1 en fonction de la suite des trames d'information I suivantes envoyées par le poste P20 :

t_0	t_1	t_2	t_3	t_4	t_5	t_6
SABM	I0, I1, I2, I3	I4, I5, I6, I7	I6, I0, I1, I2	I1, I2, I3, I4	DISC	fin

   (c) Sachant que la trame d'information comporte 256 octets, déterminer le temps global de transmission dans le cas de la question précédente (On néglige le temps de traitement au niveau des postes).

Exercice 3 Couche réseaux (3 pts : 0.75 + 0.75 + 1.5)

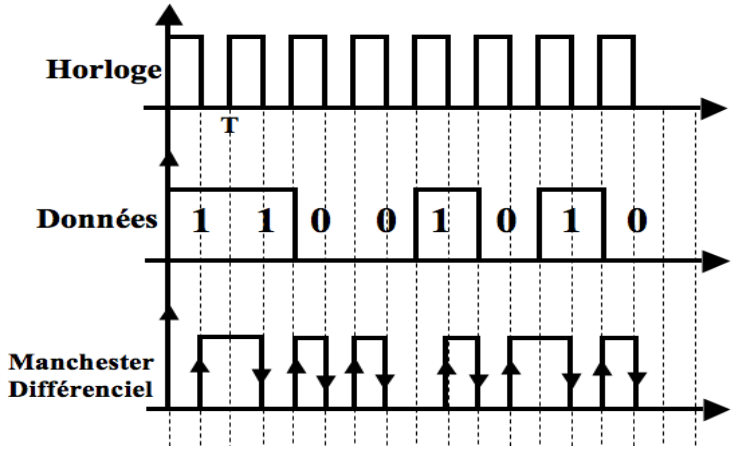
1. Citer trois missions de la couche réseaux.
2. Que contient la table de routage dans un routeur ?
3. Supposant que vous disposez de l'adresse IPv4 **146.17.0.0** pour adresser les postes du LAN :
   – Donner un masque raisonnable pour ce réseau.
   – En déduire la plage d'adresses.
   – En déduire l'adresse de diffusion.

Bonne chance

Corrigé type

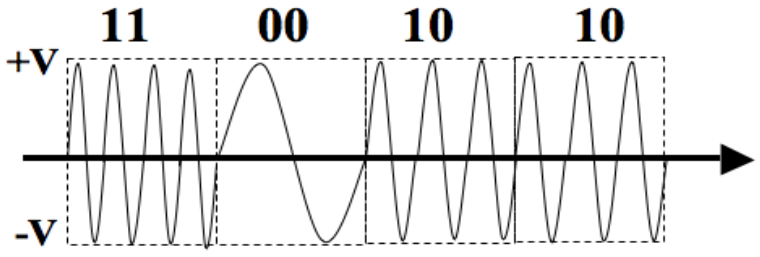
Exercice 1 : Couche physique (8 pts : 3 + 3 + 2)

1. La communication dans le réseau LAN utilise la transmission dite en bande de base :
   (a) Puisque le signal numérique est transmet dans sa fréquence de base. **0.5 pt**
   (b) Pour distinguer la valeur 0 de l'absence du signal et pour garder la synchronisation dans le cas de silences (longues suites de 0 et de 1) **0.5 pt**
   (c) -



2 pts

2. La communication dans le réseau WAN utilise la transmission dite large bande :
   (a) Une autre appellation : Bande transposée **0.5 pt**
   (b) $00 : f_1$
   $01 : f_2 = 2f_1$
   $10 : f_3 = 3f_1$
   $11 : f_4 = 4f_1$ **0.5 pt**



2 pts

3. Le transfert du fichier se fait de P20 vers P1 puis de P1 vers le serveur de la poste :
   - Taille du fichier = 3 MOctets $= 3 \times 8 = 24\ Mbits$ **0.5 pt**
   - Temps de transfert de P20 à P1 $= \frac{24\ Mbits}{10\ Mbits/s} = 2.4\ s$ **0.5 pt**
   - Temps de transfert de P1 au serveur de la poste $= \frac{24 \times 1024\ Kbits}{256\ Kbits/s} = 96\ s$ **0.5 pt**
   - Temps de transfert de P20 au serveur de la poste $= 2.4 + 96 = 98.4\ secondes$ **0.5 pt**
   - Débit moyen $= \frac{24\ Mbits}{98.4} = 0.2439\ Mbits/s = 249.75\ Kbits/s$ **0.5 pt**

Exercice 2 : Couche Liaison (9 pts : 3 + 6)

1. Polynôme générateur $G(x) = x^5 + x^2 + 1$
   (a) Le poste P1 veut envoyer le message [**100010110**] à P20 :
   Message original = 100010110 $\Rightarrow M(x) = x^8 + x^4 + x^2 + x$
   $G(x) = x^5 + x^2 + 1$
   $M(x).x^5 = x^{13} + x^9 + x^7 + x^6$

x^{13}	+	x^9	+	x^7	+	x^6		x^5	+	x^2	+	1
x^{13}	+	x^{10}	+	x^8				x^8	+	x^5	+	x^4	+ x^3
x^{10}	+	x^9	+	x^8	+ x^7	+ x^6						
x^{10}	+	x^7	+	x^5								
x^9	+	x^8	+	x^6	+	x^5						
x^9	+	x^6	+	x^4								
x^8	+	x^5	+	x^4								
x^8	+	x^5	+	x^3								
x^4	+	x^3										

   $R(x) = x^4 + x^3 = (11000)_2$
   Le message à envoyer $T(x) = M(x).x^r - R(x) = x^{13} + x^9 + x^7 + x^6 + x^4 + x^3 = (100010110\mathbf{11000})_2$ **(1.5 pt)**

   (b) Le psote P1 reçoit le message [**110010101100**] :
   $T(x) = x^{11} + x^{10} + x^7 + x^5 + x^3 + x^2$

x^{11}	+ x^{10}	+ x^7	+ x^5	+ x^3	+ x^2			x^5	+ x^2	+ 1		
x^{11}	+ x^8	+ x^6						x^6	+ x^5	+ x^3	+ x	+ 1
x^{10}	+ x^8	+ x^7	+ x^6	+ x^5	+ x^3	+ x^2						
x^{10}	+ x^7	+ x^5										
x^8	+ x^6	+ x^3	+ x^2									
x^8	+ x^5	+ x^3										
x^6	+ x^5	+ x^2										
x^6	+ x^3	+ x										
x^5	+ x^3	+ x^2	+ x									
x^5	+ x^2	+ 1										
x^3	+ x	+ 1										

   Reste = $x^3 + x + 1 \neq 0 \Rightarrow$ Message erroné **(1.5 pt)**

2. HDLC
   (a) Sans la numérotation des trames, le récepteur risque de recevoir des trames dupliquées. **(0.5 pt)**
   (b) La suite de trames de supervision S/U émises par le poste P1 :

t_0	t_1	t_2	t_3	t_4	t_5	t_6
UA	RR-04	SREJ-06	REJ-01	RR-05	UA	fin
0.5 pt	**0.5 pt**	**0.5 pt**	**0.5 pt**	**0.5 pt**	**0.5 pt**	

(c) Temps global de transmission :
- Nombre de trames d'informations émises = 16 trames
  Taille d'une trame I = 2 (Fanions) + 1 (adresse) + 1 (commande) + 256 (Information) + 2 (FCS) = 262 Octets
  Taille des trames d'informations = 262 x 16 = 4192 Octets
  Temps de transmission des trames I = $\frac{4192\times8}{10\times2^{20}}$ = **3.19 ms** **(1 pt)**
- Nombre de trames S émises = 4 trames
  Taille d'une trame S = 2 (Fanions) + 1 (adresse) + 1 (commande) + 2 (FCS) = 6 Octets
  Taille des trames S = 6 x 4 = 24 Octets
  Temps de transmission des trames S = $\frac{24\times8}{10\times2^{20}}$ = **0.018 ms** **(0.5 pt)**
- Nombre de trames U émises = 4 trames
  Taille d'une trame U = 2 (Fanions) + 1 (adresse) + 1 (commande) + 2 (FCS) = 6 Octets
  Taille des trames U = 6 x 4 = 24 Octets
  Temps de transmission des trames U = $\frac{24\times8}{10\times2^{20}}$ = **0.018 ms** **(0.5 pt)**
- Temps global de transmission = 3.19 + 0.018 + 0.018 = **3.226 ms** **(0.5 pt)**

Exercice 3 : Couche réseaux (3 pts : 0.75 + 0.75 + 1.5)

1. Missions de la couche réseau :
   - Commutation
   - Adressage
   - Nommage
   - Routage
   - Contrôle de congestion **(0.75 pt)**
2. La table de routage contient les réseau et leurs sorties correspondantes dans le routeur. **(0.75 pt)**
3. Supposant que vous disposez de l'adresse IPv4 **146.17.0.0** pour adresser les postes du LAN :
   - Le LAN contient 20 postes
     ⇒ le nombre de bits pour les machines = 5
     ⇒ le masque = 255.255.255.224 **(0.5 pt)**
   - Plage d'adresses : de 146.17.0.1 à 146.17.0.30 **(0.5 pt)**
   - Adresse de diffusion=146.17.0.31 **(0.5 pt)**

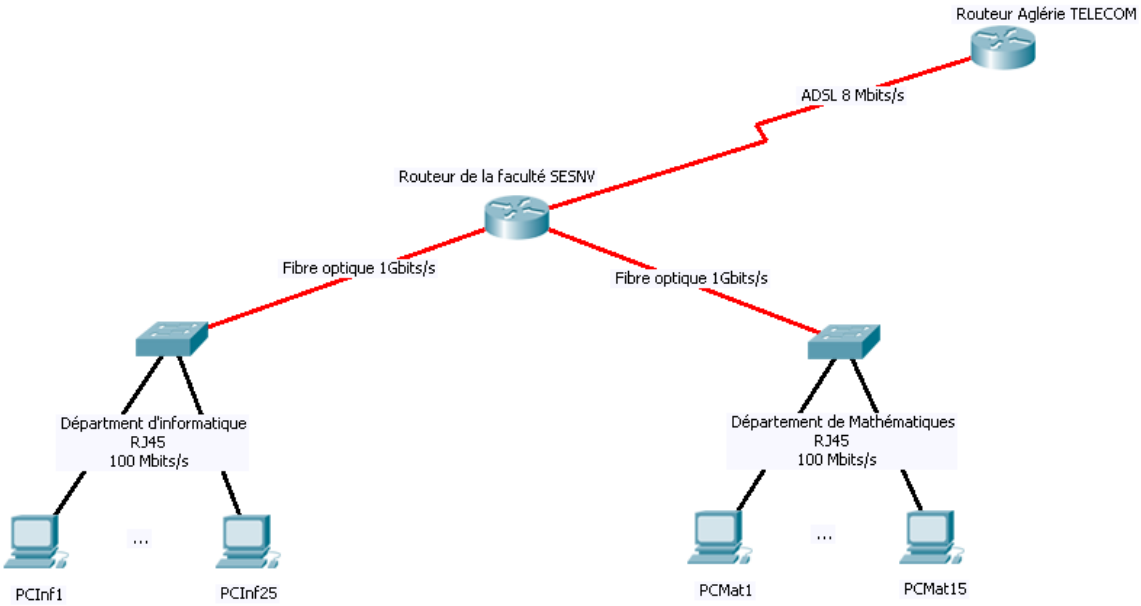
Université Mohamed Khider-Biskra
Faculté des Sciences Exactes et des Sciences de la Nature et de la Vie
Département d'informatique

$2^{ème}$ année LMD
15 Mai 2017

Réseaux de communication
10:00-11:30 A1, A2, A3, S1

Examen

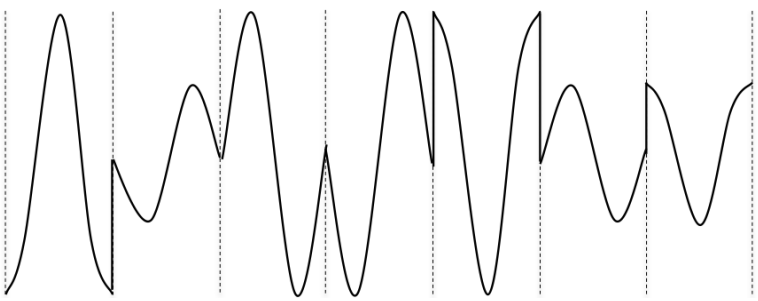
Soit le réseau représenté dans la figure suivante :



Un routeur au niveau de notre faculté FSESNV relie les réseaux des départments d'informatique et de mathématique à l'aide de liaisons en fibre optique d'un débit de 1 Gbits/s. Le réseau du department d'informatique comporte 25 postes tandis que le réseau du département de mathématique comporte 15 postes seulement. Chacun des deux réseau relie ses postes à travers un switch par une liaison en RJ45 offrant un débit de 100Mbits/s. Le routeur de la faculté est relié au routeur de la poste Algérie TELECOM par une liaison de type ADSL offrant un débit de 8 Mbits/s.

Exercice 1 Couche physique (6.5 pts : 1.5 + 3 + 2)

1. Calculer le débit moyen entre le poste PCInf1 et le routeur d'Algérie TELECOM en prenant comme exemple le transfert d'un fichier de 1 Méga Octets.
2. Le routeur de la poste décode la chaine binaire "**0100011100001001111101**" en recevant le signal suivant :



Tournez la page ../..

(a) Quel type de modulation utilise-t-il ? Justifier.

(b) Donner le diagramme des codes (cercle) correspondant.

3. Le réseau du département d'informatique utilise un codage en bande de base de type Manchester différentiel. Le poste PCInf1 veut envoyer la chaîne binaire "1001110010". Donner, sur un schéma la forme du signal émis.

Exercice 2 Couche Liaison (7.5 pts : 0.5 + 3 + 1.5 + 2 + 0.5)

Le protocole HDLC (High level Data Link Control) défini par l'ISO est utilisé pour la gestion du dialogue dans le réseau LAN du département d'informatique. En supposant que la taille de la fenêtre = 8 (0..7) et que la station émettrice n'envoie que 04 trames d'informations I numérotées puis se place en attente d'un accusé de réception. Pour la protection contre les éventuelles erreurs, on utilise la méthode CRC sur 8 bits avec un polynôme générateur $G(x) = x^8 + x^3 + 1$.

Une communication de type ABM est initialisée entre le poste PCInf1 d'adresse "00000001" et le poste PCInf2 d'adresse "00000010".

1. Donner la structure d'une trame d'information HDLC.
2. PCInf1 attend de PCInf2 la $1^{ère}$ trame et tente de lui envoyer la $9^{ème}$ trame l'information contenant l'information "00000110". Donner, en binaire, la trame envoyée par PCInf1.
3. Que peut conclure PCInf1 en recevant chacune des trames suivantes :
   - 01111110 00000001 10011110 00110101 01111110
   - 01111110 00000001 10000001 11101100 01111110
   - 01111110 00000001 01000101 01111110

Exercice 3 Couche réseaux (6 pts : 0.5 + 2 + 2 + 1.5)

L'administrateur réseau de la faculté dispose de l'adresse réseau **145.14.6.0** avec le masque **255.255.254.0** et veut l'utiliser pour sous-adresser les différents postes de la faculté.

1. À quelle classe appartient ce réseau ?
2. Sachant qu'il existe encore 8 départements à connecter comportant chacun au maximum 30 postes, proposer pour chacun des deux réseaux du schéma :
   - Une adresse réseau.
   - Un masque adéquat.
   - Une adresse de diffusion.
   - L'adresse IP la plus basse et la plus haute.
3. Donner pour les deux réseaux la configuration IP des interfaces représentées sur le schéma.

Bonne chance

Corrigé type

Exercice 1 : Couche physique (6.5 pts : 1.5 + 3 + 2)

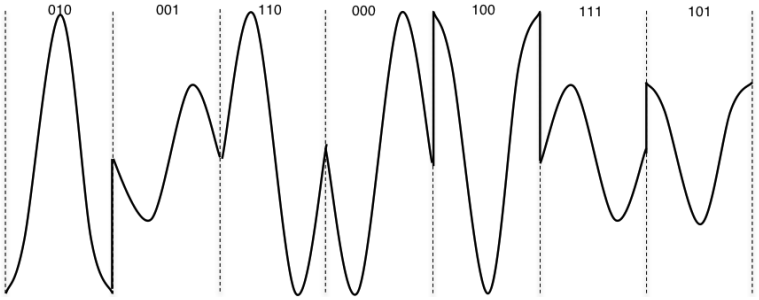
1. Débit moyen entre le poste PCInf1 et le routeur d'Algérie TELECOM
   - Temps de transfert du fichier entre PCInf1 et le Switch = $\frac{1\times 2^{20}\times 8}{100\times 2^{20}} = 0.08s$
   - Temps de transfert du fichier entre le Switch et le routeur de la faculté = $\frac{1\times 2^{20}\times 8}{\times 2^{30}} = 8\times 10^{-3}s$
   - Temps de transfert du fichier entre le routeur de la faculté et le routeur de la poste = $\frac{1\times 2^{20}\times 8}{8\times 2^{20}} = 1s$
   - Temps global de transfert = $0.08 + 0.008 + 1 = 1.088s$
   - Débit moyen = $\frac{1\times 2^{20}\times 8}{1.088s} = 7.35Mbits/s$

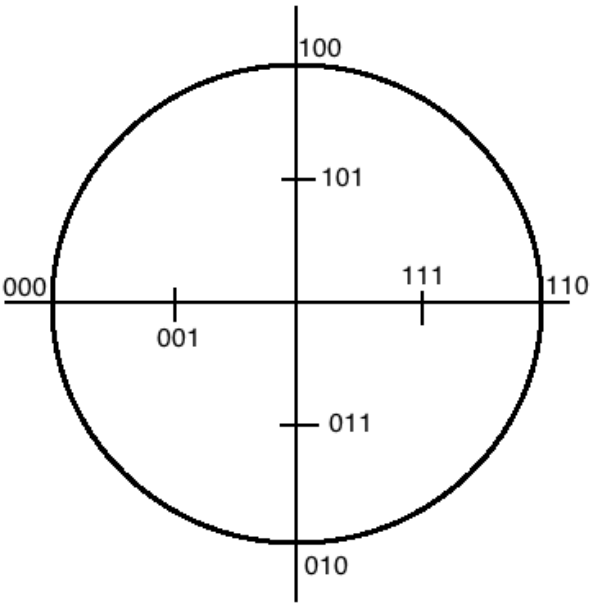
   1.5 pt

2. Le routeur de la poste décode la chaine binaire "**01000111000010011101101**" :

   (a) Il utilise la modulation combinée de phase et d'amplitude puisque uniquement l'amplitude et la phase qui change dans le signal. **0.5 pt**

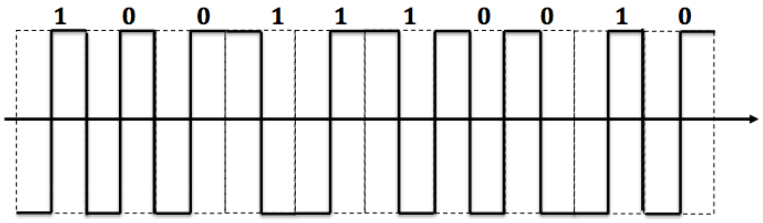
   (b) Le diagramme des codes





2.5 pts

3. Forme du signal émis en Manchester différentiel :



2 pts

Exercice 2 : Couche Liaison (7.5 pts : 0.5 + 3 + 1.5 + 2 + 0.5)

1. Structure d'une trame d'information HDLC.

8 bits	8 bits	1 bit	3 bits	1 bit	3 bits	n bits	16 bits	8 bits
fanion	adresse	0	N(s)	P/F	N(r)	information	FCS	fanion

0.5 pt

2. PCInf1 attend de PCInf2 la $1^{ère}$ trame et tente de lui envoyer la $9^{ème}$ trame l'information contenant l'information "00000110". Donner, en binaire, la trame envoyée par PCInf1.
   - Fanion = 01111110 **0.25 pt**
   - Adresse = 00000010 **0.25 pt**
   - N(s) = 000, N(r) = 000, P/F = 0 ⇒ CTRL = 00000000 **0.5 pt**
   - Info = 00000110 **0.25 pt**
   - Calcul du CRC sur 8 bits
     - $M(x) = 00000010000000000000110 = x^{17} + x^2 + x$
     - $G(x) = x^8 + x^3 + 1 \Rightarrow r = 8$
     - $M(x)x^r = x^{25} + x^{10} + x^9$
     - $M(x)x^r = G(x) \times (x^{17} + x^{12} + x^9 + x^7) + x^7$
     - $\Rightarrow R(x) = x^7 = 10000000$ **1.5 pt**
     - T(x) = 00000010000000000000011010000000
     - Trame = 01111110 00000010 00000000 00000110 10000000 01111110 **0.25 pt**
3. Conclusions de PCInf1 :
   - 01111110 00000001 10011110 00110101 01111110
     - T(x) = 00000001 10011110 00110101
     - Reste de (T(x)/G(x)) = 00111110 ≠ 0 ⇒ Trame erronée **1.5 pt**
   - 01111110 00000001 10000001 11101100 01111110
     - T(x) = 00000001 10000001 11101100
     - Reste de (T(x)/G(x)) = 0 ⇒ Trame correcte
     - Trame de type S, RR, P/F = 0, N(s) = 001

     2 pts
   - 01111110 00000001 01000101 01111110
     - Trame incomplète **0.5 pt**

Exercice 3 : Couche réseaux (6 pts : 0.5 + 2 + 2 + 1.5)

L'administrateur réseau de la faculté dispose de l'adresse réseau **145.14.6.0** avec le masque **255.255.254.0** et veut l'utiliser pour sous-adresser les différents postes de la faculté.

1. Le réseau appartient à la classe B **0.5 pt**
2. Nombre total de réseau = 8 + 2 = 10, Nombre de bits sous-réseaux = 4, Nombre max de machines par réseau = 30, Nombre de bits machines = 5
   Réseau du département d'informatique

- Adresse réseau = 145.14.6.32
- Masque adéquat= 255.255.255.224
- Adresse de diffusion : 145.14.6.63
- Adresse IP la plus basse = 145.14.6.33 et la plus haute = 145.14.6.62 **2 pts**

Réseau du département de mathématique

- Adresse réseau = 145.14.6.64
- Masque adéquat= 255.255.255.224
- Adresse de diffusion : 145.14.6.95
- Adresse IP la plus basse = 145.14.6.65 et la plus haute = 145.14.6.94 **2 pts**

3. Donner pour les deux réseaux la configuration IP des interfaces représentées sur le schéma.

	@IP	Masque	Passerelle	DNS
PCInf1	145.14.6.33	255.255.255.224	145.14.6.62	145.14.6.62
PCInf25	145.14.6.57	255.255.255.224	145.14.6.62	145.14.6.62
Routeur FSESNV Coté Informatique	145.14.6.62	255.255.255.224	145.14.6.62	145.14.6.62
PCMat1	145.14.6.65	255.255.255.224	145.14.6.94	145.14.6.94
PCMat15	145.14.6.79	255.255.255.224	145.14.6.94	145.14.6.94
Routeur FSESNV Coté Mathématiques	145.14.6.65	255.255.255.224	145.14.6.94	145.14.6.94

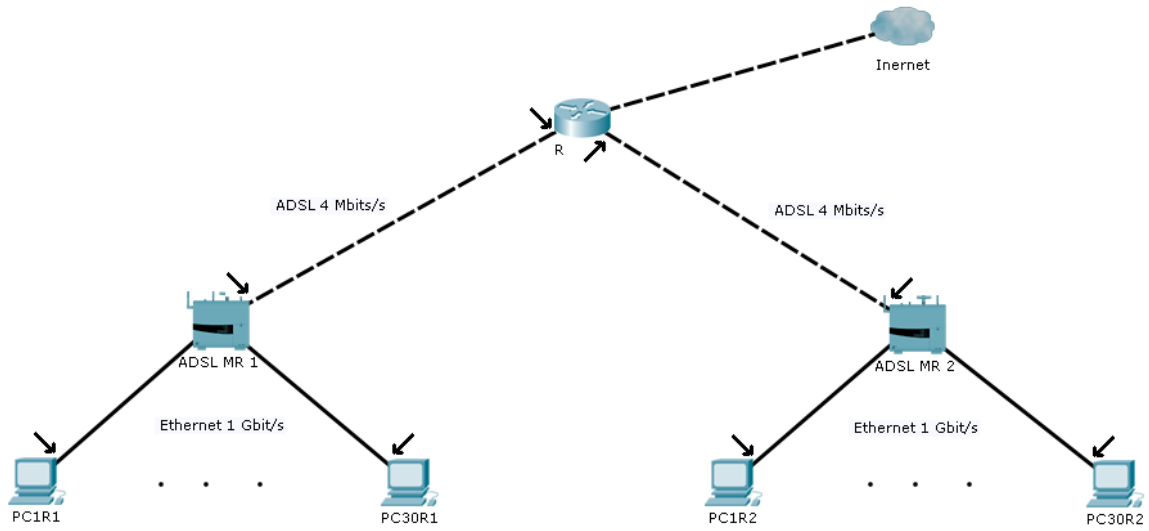
1.5 pt

Université Mohamed Khider-Biskra
Faculté des Sciences Exactes et des Sciences de la Nature et de la Vie
Département d'informatique

$2^{ème}$ année LMD | Réseaux de communication
23 Mai 2018 | 10:30-12:00 A1, A2, A3

Examen

Soit le réseau représenté dans la figure suivante :



Un routeur R relie deux réseaux R1 et R2 à travers des liaisons ADSL en utilisant deux modems-routeurs "ADSL MR 1" et "ADSL MR 2". Chaque modem-routeur comporte un switch de 48 interfaces Ethernet pour le réseau local et une interface téléphonique pour le réseau ADSL. Le réseau R1 relie 30 postes (PC1R1 à PC30R1) et le réseau R2 relie 30 postes (de PC1R2 à PC30R2). Les débit des liaisons ADSL est de 4 Mbits/s et celui des réseaux R1 er R2 est de 1 Gbit/s.

Exercice 1 Couche physique (8 pts : 2 + 3 + 3)

1. Calculer le débit moyen entre le poste PC1R1 du réseau R1 et le poste PC1R2 du réseau R2 en prenant un exemple de transfert d'un fichier de 100 Mégaoctets. Le fichier est transféré par commutation de de messages et les temps de traitement au niveau des nœuds et négligé.
2. Les réseau R1 et R2 utilisent le codage Miller au niveau de la couche physique, tandis que les liaison ADSL utilisent un codage PSK avec quatre phases (0°, 90°, 180°, 270°) . Le poste PC1R1 veut transmettre l'octet suivant : "**C9**" au poste PC1R2.
   Donner sur deux schémas :
   (a) La forme du signal véhiculé sur le réseau R1.
   (b) La forme du signal véhiculé sur la liaison ADSL du modem-routeur ADSL MR 1.

Exercice 2 Couche Liaison (6.5 pts : 2 + 1 + 2 + 1.5)

1. Pour la protection contre les éventuelles erreurs, la couche liaison du réseau R1 utilise la méthode CRC sur 8 bits avec un polynôme générateur $G(x) = x^8 + x + 1$.

(a) PC1R1 veut transmettre l'octet suivant : "**C9**" à PC2R1. Donner la chaine devant être réellement transmise.

(b) PC2R1 reçoit la chaine de deux octets suivante : "**C9A1**". Que conclut-il ?

2. Le protocole HDLC vue dans le cours est utilisé pour la couche liaison du réseau R1. PC1R1 veut transmettre la chaine "**C89B**" au poste PC2R1 en une seule trame.
   - Donner en format hexadécimal la trame HDLC émise. (*Le champs adresse est supposé égal à 1, et le champs FCS à FF*)
   - Que conclut PC1R1 en recevant comme réponse la trame : "**7E01B8FF7E**"

Exercice 3 Couche réseaux (5 pts : 0.5 + 3 + 1.5)

On dispose de le l'adresse réseau **202.16.148.0** pour l'utiliser pour adresser les différentes interfaces des différents réseaux.

1. À quelle classe appartient ce réseau ?
2. Proposer pour chacun des sous-réseaux du schéma une adresse réseau, un masque de sous réseaux, une adresse de diffusion, une plage d'adresses IP utilisables.
3. Pour chaque interface indiqué par une flèche sur le schéma, donner la configuration IP suivante :
   - L'adresse IP,
   - Le masque de sous-réseau,
   - L'adresse de la passerelle.

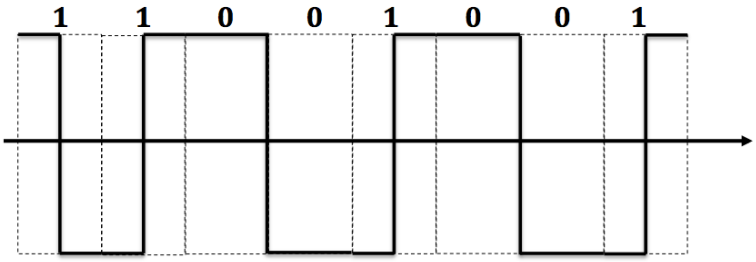
Bonne chance

Corrigé type

Exercice 1 Couche physique (8 pts : 2 + 3 + 3)

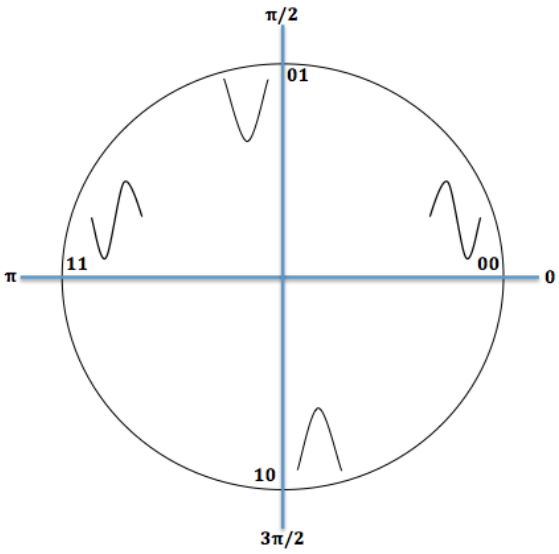
1. Débit moyen entre le poste PC1R1 et PC1R2
   - Temps de transfert du fichier entre PC1R1 et le MR1 = Temps de transfert du fichier entre MR2 PC1R2 = $\frac{100\times10^6\times8}{1\times10^9} = 0.8s$ **0.5 pt**
   - Temps de transfert du fichier entre MR1 et R = Temps de transfert du fichier entre R et MR2 = $\frac{100\times10^6\times8}{4\times10^6} = 200s$ **0.5 pt**
   - Temps global de transfert = $2 \times 0.8 + 2 \times 200 = 401.6s$ **0.5 pt**
   - Débit moyen = $\frac{100\times10^6\times8}{401.6s} = 1.99Mbits/s$ **0.5 pt**
2. Formes des signaux

   (a) La forme du signal véhiculé sur le réseau R1 (codage Miller).
   - Chaine binaire (C9) = 11001001



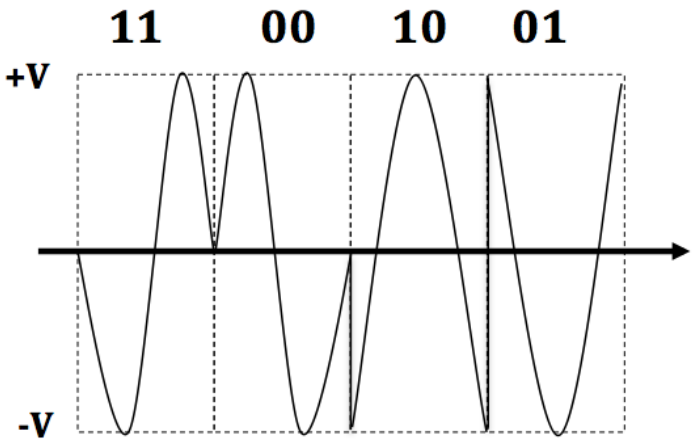
3 pts

   (b) La forme du signal véhiculé sur la liaison ADSL du modem-routeur ADSL MR 1 (PSK).
   - Codes



1 pt

– Signal



2 pts

Exercice 2 Couche Liaison (6.5 pts : 2 + 1 + 2 + 1.5)

1. Pour la protection contre les éventuelles erreurs, la couche liaison du réseau R1 utilise la méthode CRC sur 8 bits avec un polynôme générateur $G(x) = x^8 + x + 1$.
   (a) Chaine = $(C9)_{16} = (11001001)_2$
   - Chaine binaire = 11001001 $\Rightarrow M(x) = x^7 + x^6 + x^3 + 1 \Rightarrow r = 8$.
   - $M(x) \times x^r = x^{15} + x^{14} + x^{11} + x^8$.
   - $M(x) \times x^r = G(x) \times (x^7 + x^6 + x^3) + x^6 + x^4 + x^3$.
   - $R(x) = x^6 + x^4 + x^3$
   - $T(x) = M(x) \times x^r - R(x) = x^{15} + x^{14} + x^{11} + x^8 + x^6 + x^4 + x^3$ **1.5 pt**
   - $T(x) = 1100100101011000$ **0.5 pt**

   (b) PC2R1 reçoit la chaine de deux octets suivante : "**C9A1**". Que conclut-il ?
   - Chaine binaire = $(C9A1)_{16} = (1100100110100001)_2$
   - $T(x) = 1100100110100001 = x^{15} + x^{14} + x^{11} + x^8 + x^7 + x^5 + 1$.
   - $T(x) = G(x) \times (x^7 + x^6 + x^3) + x^7 + x^6 + x^5 + x^4 + x^3 + 1$.
   - $R(x) = x^7 + x^6 + x^5 + x^4 + x^3 + 1 \neq 0$ **0.5 pt**
   - **Trame erronée** **0.5 pt**

2. Le protocole HDLC vue dans le cours est utilisé pour la couche liaison du réseau R1. PC1R1 veut transmettre la chaine "**C89B**" au poste PC2R1 en une seule trame.
   (a) Donner en format hexadécimal la trame HDLC émise. (*Le champs adresse est supposé égal à 1, et le champs FCS à FF*)
   - Fanion : 7E **0.25 pt**
   - Adresse : 01 **0.25 pt**
   - Info : C89B **0.25 pt**
   - FCS : FF **0.25 pt**
   - Contrôle :
     - Trame I : premier bit = 0
     - N(s) = 000
     - N(r) = 000
     - P/F = 1 (une seule trame)
     - $\Rightarrow$ Champs contrôle = 00001000 = 08
   - Trame HDLC = **7E 01 08 C8 9B FF 7E** **1 pt**

(b) Que conclut PC1R1 en recevant comme réponse la trame : "**7E01B8FF7E**"
- Champs contrôle = B8 = 10111000 **0.25 pt**
- Type de trame = S (commence par 10) **0.25 pt**
- Champ SS = 11 (SREJ) **0.25 pt**
- N(s) = 000 **0.25 pt**
- Le poste demande la retransmission de la trame numéro 000 **0.5 pt**

Exercice 3 Couche réseaux (5.5 pts : 0.5 + 3 + 2)

On dispose de le l'adresse réseau **202.16.148.0** pour l'utiliser pour adresser les différentes interfaces des différents réseaux.

1. Le réseau appartient à la classe **C** **0.5 pt**
2. Proposer pour chacun des sous-réseaux du schéma une adresse réseau, un masque de sous réseaux, une adresse de diffusion, une plage d'adresses IP utilisables.
   - On 4 sous réseaux R1, R2, ADSL1 et ADSL2
   - Le nombre de machines maximum dans les quatre sous-réseau est de 31 machines (30 postes + la passerelle) ⇒ nombre de bits machines = 6 et le nombre de bits réseau = 2
   - Proposition d'adressage **0.75 pt** pour chaque sous-réseau

Réseau	@ réseau	Masque	@ diffusion	plages d'adresses
ADSL1	202.16.148.0	255.255.255.192	202.16.148.63	202.16.148.1 à 202.16.148.62
R1	202.16.148.64	255.255.255.192	202.16.148.127	202.16.148.65 à 202.16.148.126
ADSL2	202.16.148.128	255.255.255.192	202.16.148.191	202.16.148.129 à 202.16.148.190
R2	202.16.148.192	255.255.255.192	202.16.148.255	202.16.148.193 à 202.16.148.254

3. Pour chaque interface indiqué par une flèche sur le schéma, donner la configuration IP suivante :

Interface	@ IP	Masque	@ Passerelle
R (ADSL1)	202.16.148.1	255.255.255.192	202.16.148.1
R (ADSL2)	202.16.148.129	255.255.255.192	202.16.148.129
MR1 (ADSL1)	202.16.148.2	255.255.255.192	202.16.148.1
MR2 (ADSL2)	202.16.148.130	255.255.255.192	202.16.148.129
PC1R1	202.16.148.66	255.255.255.192	202.16.148.65 (MR1 dans R1)
PC30R1	202.16.148.96	255.255.255.192	202.16.148.65 (MR1 dans R1)
PC1R2	202.16.148.194	255.255.255.192	202.16.148.193 (MR2 dans R2)
PC30R2	202.16.148.204	255.255.255.192	202.16.148.193 (MR2 dans R2)

0.25 pt pour chaque deux interfaces

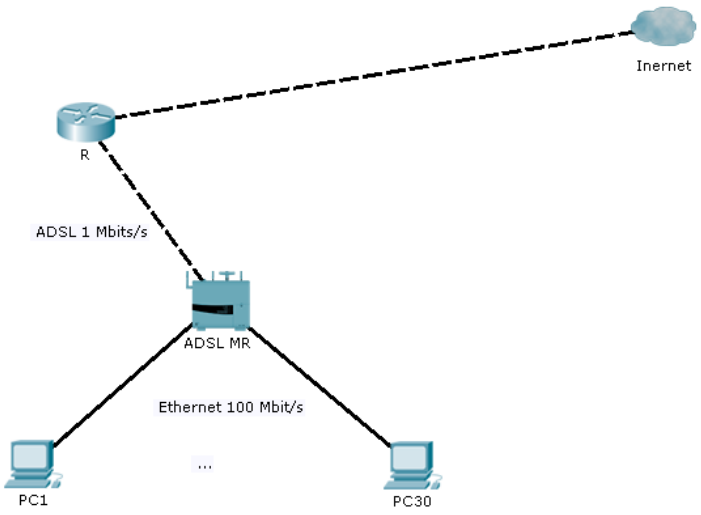
Université Mohamed Khider-Biskra
Faculté des Sciences Exactes et des Sciences de la Nature et de la Vie
Département d'informatique

$2^{ème}$ année LMD
29 Juin 2019

Réseaux de communication
10:00-11:30 A1, A2, A3

Examen

Soit le réseau représenté dans la figure suivante :



Le modem routeur "ADSL MR" relie les 30 postes, de PC1 à PC30, par des câbles RJ45 avec un débit de 100 Mbits/s. Le modem est aussi relié au routeur R de la poste par une liaison téléphonique d'un débit de 1 Mbits/s.

Questions de cours : (4 pts : 1 + 2 + 1)

1. Citer les sept couches du modèles OSI.
2. Donner pour chacun des termes suivants la couche à la quelle il appartient : IP, Parité, ADSL, Switch, RJ45, Trame, Masque, CRC.
3. Quels sont les informations ajoutées par la couche liaison aux données reçues de la couche réseau avant d'être transmises à la couche physique.

Exercice 1 Couche physique (8 pts : 2 + 1 + 1.5 + 1.5 + 2)

1. On veut transmettre dans le réseau local Ethernet la chaine binaire "**11000110**" du poste PC1 au Modem routeur MR. Donner sur un schéma la forme du signal émis dans le cas d'utilisation d'un codage de **Macherster différentiel**.
2. On veut transmettre la chaine binaire "**1100011001100011**" du Modem routeur MR au routeur de la poste en utilisant la liaison téléphonique ADSL.
   Sachant que le modem utilise une modulation combiné de deux phases : $\frac{\pi}{2}$ et $\frac{3\pi}{2}$ et deux amplitudes 3 et 6 volts,
   (a) Calculer la valence du signal.

(b) Calculer la rapidité de modulation de cette liaison.

(c) Calculer le temps nécessaire à la transmission de cette chaine.

(d) Donner sur un schéma la forme du signal émis.

Exercice 2 Couche réseaux (8 pts : 1 + 1.5 + 1.5 + 2 + 2)

La configuration IP du poste PC1 est donnée comme suit :

```
Adresse IP:193.55.42.72
Masque : 255.255.255. ?
Passerelle: 193.55.42.65
Serveur DNS: 193.55.42.65
```

1. Préciser à quelle classe appartient ce réseau.
2. Donner l'adresse du modem-routeur.
3. Combien d'adresses IP faut-il utiliser pour adresser toutes la machine de ce réseau ?
4. Quelle est donc la plus grande valeur qu'on peut attribuer au quatrième octet du masque (marqué par ?) ? Donner alors la valeur complète du masque.
5. En utilisant le masque précédent, donner :
   - L'adresse de sous-réseau,
   - L'adresse de diffusion dans le réseau.
   - L'adresse IP la plus basse.
   - L'adresse IP la plus haute.

Bonne chance

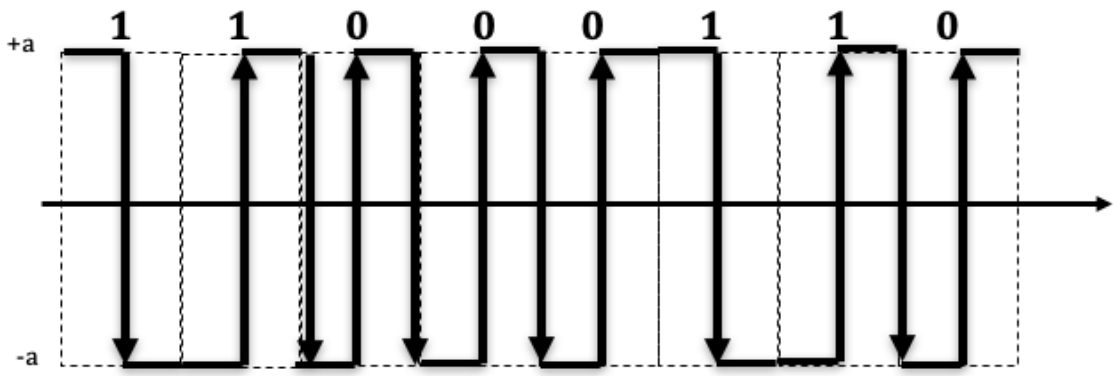
Corrigé type

Questions de cours : (4 pts : 1 + 2 + 1)

1. Citer les sept couches du modèles OSI.
   1.Couche Physique, 2.Couche Liaison, 3.Couche Réseaux, 4.Couche Transport, 5. Couche Session, 6.Couche Présentation, 7.Couche Application **1 pt**
2. Donner pour chacun des termes suivants la couche à la quelle il appartient :
   IP :Couche réseau, Parité :Couche liaison, ADSL :Couche physique, RJ45 :Couche physique, Switch :Couche liaison, Trame :Couche liaison, Masque :Couche réseau, CRC :Couche liaison. **2 pts**
3. Quels sont les information ajoutées par la couche liaison aux données reçues de la couche réseau avant d'être transmises à la couche physique.
   Le fanion, l'adresse, le FCS, le champ contrôle, les bits de bit stuffing **1 pt**

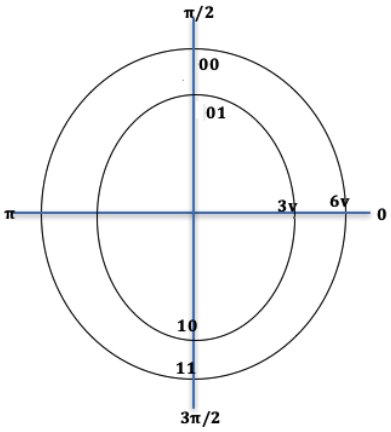
Exercice 1 Couche physique (8 pts : 2 + 1 + 1.5 + 1.5 + 2)

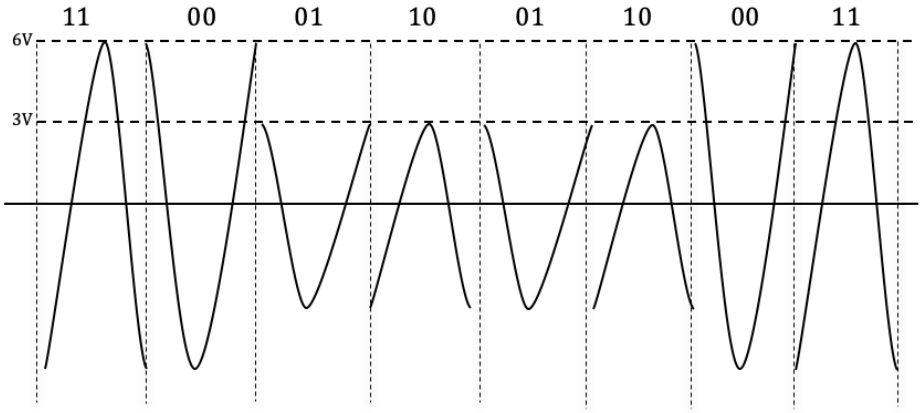
1. Chaine binaire = "**11000110**". **Macherster différentiel**.



2pts

2. Chaine binaire "**1100011001100011**" du Modem routeur MR au routeur de la poste en utilisant la liaison téléphonique. Sachant que le modem utilise une modulation combiné de deux phases :$\frac{\pi}{2}$ et $\frac{3\pi}{2}$ et deux amplitudes 3 et 6 volts.
   (a) Valence du signal
   2 phases * 2 amplitude $\Rightarrow V = 4$ **1 pt**
   (b) Calculer la rapidité de modulation de cette liaison,
   Nombre de bits / bauds = $log_2(V) = 2$
   $Debit = log_2(V) \times R \Rightarrow R = \frac{Debit}{log_2(V)} = \frac{1Mbits/s}{2bits} = 512Kbauds$ **1.5 pt**
   (c) Calculer le temps nécessaire à la transmission de cette chaine.
   Nombre de bits à transmettre = 16 bits
   Débit = 1 Mbits/s = 10^6
   Temps de transmission = $\frac{Nb\ bits}{Debit} = \frac{16}{10^6}s = 16 \times 10^{-3}ms$ **1.5 pt**
   (d) Donner sur un schéma la forme du signal émis.
   2 pts





Exercice 2 Couche réseaux (8 pts : 1 + 1.5 + 1.5 + 2 + 2)

La configuration IP du poste PC1 est donnée comme suit :

```
Adresse IP:193.55.42.72
Masque : 255.255.255. ?
Passerelle: 193.55.42.65
Serveur DNS: 193.55.42.65
```

1. Préciser à quelle classe appartient ce réseau.
   Classe C
2. Donner l'adresse du modem-routeur. **1 pt**
   193.55.42.65 **1.5 pt**
3. Combien d'adresses IP faut-il utiliser pour adresser toutes la machine de ce réseau ?
   Nombre de machine = 30 machines + le modem-routeur = 31 machines ⇒ il faut 31 adresses **1.5 pt**
4. Quelle est donc la plus grande valeur qu'on peut attribuer au quatrième octet du masque (marqué par ?) ? Donner alors la valeur complète du masque.
   Nombre d'adresses = 31 ⇒ Nombre de bits pour les machines = au moins 6bits ⇒ la valeur du dernier octet du masque sera au plus 11000000 = 192 **1 pt**
   La valeur du masque = 255.255.255.192 **0.5 pt**
5. En utilisant le masque précédent, donner :
   – L'adresse de sous-réseau,
   Adresse de sous-réseau = adresse IP **and** masque = 193.55.42

= 193.55.42.72 and 255.255.255.192
= 193.55.42.0100 1000 **and** 255.255.255.1100 0000
= 193.55.42.0100 0000
= **193.55.42.64** **0.75 pt**

– L'adresse de diffusion dans le réseau
Adresse diffusion : 193.55.42.01**11 1111** = **193.55.42.127** **0.75 pt**

– L'adresse IP la plus basse.
Adresse la plus basse = **193.55.42.65** **0.5 pt**

– L'adresse IP la plus haute
Adresse la plus haute = **193.55.42.126** **0.5 pt**

Références

[1] Douglas Comer. Tcp/ip : Architecture, protocoles, applications. troisième édition. intereditions, 1996.

[2] Dominique Dromard, Danièle et Seret. *Architecture des réseaux.* Pearson Education France, 2009.

[3] S. Lohier and D. Présent. *Réseaux et transmissions - 6e ed : Protocoles, infrastructures et services.* InfoSup. Dunod, 2016.

[4] J.L. Montagnier. *Réseaux d'entreprise par la pratique.* Solutions réseaux. Eyrolles, 2004.

[5] Guy Pujolle. *Les réseaux : Edition 2014.* Editions Eyrolles, 2014.

[6] Pierre Rolin. *Réseaux locaux : normes et protocoles.* Hermès, 1993.

[7] A. Tanenbaum. *Réseaux : Architectures, Protocoles et Applications.* InterEditions, 1995.