DOMAINE:

TECHNOLOGIE INFORMATIQUE

RESEAUX INFORMATIQUES

VERSIONS & DATES	*OBJET*	*AUTEUR(S)*
Version 1.0 – septembre 2009	*Création*	*Bernard GIACOMONI - Association A.T.L.A.N.T.I.C*

SOMMAIRE

I INTRODUCTION:

L'objet de ce document est de présenter un panorama des technologies employées pour la conception des réseaux informatiques, qu'il s'agisse de réseaux locaux ou de réseaux étendus. Le rôle des différentes couches de traitement intervenant dans la transmission des informations est décrit, ainsi que les mécanismes et les solutions technologiques disponibles pour les implémenter.

II GENERALITES SUR LES RESEAUX:

II.1 NOTION DE RESEAU INFORMATIQUE:

Dans le domaine de l'informatique, un réseau de communication est un ensemble de moyens matériels et logiciels permettant de faire communiquer entre eux différents systèmes informatiques.

Par extension, la notion de réseau englobe souvent non seulement le réseau, en tant que moyen de communication, mais aussi les systèmes qu'il interconnecte.

REMARQUES:

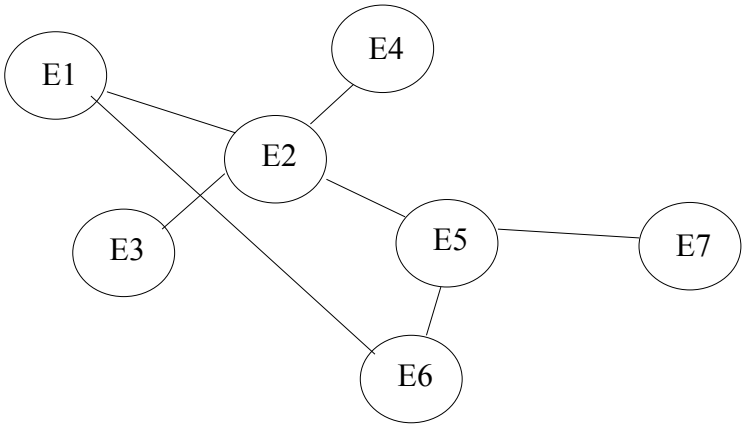
La notion de réseau recouvre trois aspects:

- Un aspect **matériel**, qui concerne les infrastructures d'interconnexion.
- Un aspect **logique**, qui concerne les fonctions de contrôle et de commande des échanges d'informations.
- Un aspect **utilisateur**, qui concerne les services que ces utilisateurs peuvent attendre du réseau.

II.2 CONCEPTS ATTACHES A LA NOTION DE RESEAU:

II.2.1 MODELISATION GRAPHIQUE:

Un réseau informatique peut être représenté graphiquement sous le forme d'un maillage dans lequel les noeuds représentent des équipements informatiques et les liens entre noeuds représentent l'interconnexion entre ces noeuds, c'est à dire la possibilité d'échanger des informations entre ces équipements:



SCHEMA N° I: TOPOLOGIE D'UN RESEAU

La représentation spaciale d'un réseau constitue sa **TOPOLOGIE**.

REMARQUES:

- Dans un réseau, tous les noeuds sont reliés au moins à un autre noeud.
- Un noeud qui n'est relié qu'à un seul noeud est dit «**noeud terminal**» (dans l'exemple, E1, E3, E4 et E7 sont terminaux)
- Un noeud relié à plusieus noeud est appelé «**noeud intermédiaire**». (dans l'exemple, E2, E5 et E6 sont intermédiaires)
- Lorsque deux noeuds sont reliés directement par un lien, ces noeuds sont dits **adjacents** (ici, E1 et E2 sont adjacents, E1 et E3 ne le sont pas, E1 est adjacent à E6).

II.2.2 NAVIGATION DANS UN RESEAU-NOTION DE ROUTAGE:

Pour échanger des informations entre noeuds non adjacents, il suffit de trouver un chemin formé par une série de noeuds adjacents qui relient le noeud de départ au noeud d'arrivée. Pour deux noeuds donnés le chemin n'est pas unique. Par exemple, pour relier E1 à E7, il existe au moins deux **routes** possibles:

- E1->E2->E5->E7
- E1->E6->E5-E7

L'action de déterminer une route entre deux noeuds non adjacents est appelée **ROUTAGE** de l'information.

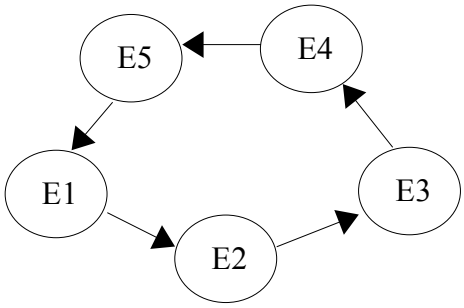
Dans un routage d'information, les noeuds intermédiaires jouent donc le rôle de **COMMUTATEURS** permettant d'aiguiller l'information à travers les mailles du réseau vers sa destination finale.

II.2.3 HOTES D'UN RESEAU INFORMATIQUE:

Dans un réseau informatique, un **HOTE** est un noeud **CLIENT** du réseau. Ceci signifie qu'il est destiné à permettre aux utilisateurs l'accès aux **SERVICES** offerts par le réseau.

REMARQUE:

Il est à noter qu'un hôte n'est pas forcément un noeud terminal. En effet, certaines topologies de réseau impliquent que certains noeuds soient à la fois HÔTES et COMMUTATEURS. C'est le cas, par exemple, dans un réseau «en anneau»:



Dans un réseau en anneau, chaque noeud à un double rôle:
- Supporter un poste CLIENT du réseau (fonction d'hôte)
- Assurer le transit de l'information entre ses deux noeuds adjacents (fonction de commutation)
*Pour ajouter un hôte, il faudra l'**insérer** dans la boucle.*

SCHEMA N° II-RESEAU EN ANNEAU

II.2.4 COMPLEXITE DE LA NOTION DE RESEAU:

Un réseau informatique est donc un équipement complexe et évolutif qui prend à sa charge la résolution des problèmes suivants:

- L'accès physique au média matériel (adaptation du signal, méthode d'accès)
- Le codage de l'information sur ce média.
- La transmission de l'information entre deux noeuds (transmission point à point).
- Le routage de l'information à travers le maillage.
- Le dialogue entre les processus logiciels mis en relation (synchronisation, codage-décodage, etc.).

II.3 RESEAUX INFORMATIQUES ET SYSTEMES D'EXPLOITATION:

II.3.1 INTRODUCTION:

L'études des réseaux informatiques nécessite la connaîssance des principaux concepts liés aux systèmes d'exploitation des ordinateurs (En anglais: Operating Systèmes: O.S.). En effet, nous allons voir que la communication dans un réseau informatique s'effectue toujours entre deux entités logicielles (processus logiciels) s'exécutant sur le même système matériel ou dans des machines différentes. L'exécution de ces logiciels est entièrement supportée et contrôlée par le système d'exploitation.. En particulier, la totalité des fonction de gestion de la communication avec le (ou les) réseau(x) connectés à la machine est prise en compte par lui.

II.3.2 NOTION DE PROCESSUS LOGICIEL:

II.3.2.1 DEFINITION :

*Un **PROCESSUS** logiciel est une **instance en cours d'exécution** d'un programme informatique.*

Il importe de bien préciser ces notions:

- Pour l'utilisateur d'un ordinateur, un programme (une application) informatique se présente sous la forme d'un **fichier**, enregistré sur un support permanent (le disque dur, par exemple). Dans la plupart des cas, ces fichiers portent l'extension **.exe**, qui permet au système d'exploitation de les différencier d'autres types de fichier (fichier image avec extension .jpg, par exemple). Un fichier .exe contient à la fois des **instructions exécutables** et des **données**, l'ensemble constituant un **programme informatique** (on dit aussi application informatique, quand le programme n'appartient pas au système d'exploitation).
- Lorsque l'utilisateur lance l'exécution du programme (par exemple, sous windows, en double-cliquant sur un icône), le système charge en mémoire vive (R.A.M) de l'ordinateur une **copie** (on dit «une instance») du contenu du fichier .exe. C'est cette instance qui constitue un **processus logiciel**.
- Une fois chargé en mémoire, le processus devient **éligible**, mais il n'en est pas pour autant mis à exécution automatiquement. C'est le système d'exploitation qui va décider de l'exécution du processus et la gérer. Nous verrons comment dans le prochain paragraphe.
- Remarquons que rien n'empêche un utilisateur de démarrer plusieurs instances d'un même programme (à moins que le programme lui-même l'interdise): par exemple, sous window, il est possible de démarrer plusieurs instances du programme «calculatrice» (c*liquer programmes->accessoires->calculatrice*). Chaque instance constituera un processus, qui se matérialisera sur l'écran par une fenêtre.

REMARQUES:

- *Très souvent, dans le domaine des systèmes d'exploitation, la notion de **processus** est confondue avec la notion de **tâche.** Bien qu'il existe certaines différences entre ces deux notions, nous pouvons les confondre dans la présente étude.*
- *Il ne faut pas confondre la notion de **processus** avec celle de **processeur** (très souvent désignés tous deux sous la forme contractée «process»): un **processeur** est un **exécutant matériel** (en fait, un circuit intégré extrèmement complexe) capable d'exécuter des **processus informatiques.***

II.3.2.2 GESTION DES PROCESSUS:

Nous avons vu que c'est le système d'exploitation qui gère l'exécution d'un processus éligible. La plupart des systèmes d'exploitation courants (windows, linux, etc) sont multi-tâches. Ceci veut dire qu'ils sont capables de gérer l'exécution **simultanée** de **plusieurs processus**. Cette simultanéïté n'est, en général, qu'apparente. En effet, les machines courantes ne possèdent qu'un seul **processeur** matériel, qui ne peut exécuter qu'une **tâche** à la fois (même dans le cas des processeurs «multi-coeurs»). En fait, les systèmes d'exploitation partagent le temps d'utilisation du processeur entre les différents processus éligibles. Il existe pour cela deux mécanismes:

- Le premier est basé sur le fait que la plupart des processus sont obligés d'interrompre très souvent leur exécution pour attendre un événement donné. C'est, par exemple, le cas d'un navigateur web qui passe le plus clair de son temps à attendre

soit une commande de l'utilisateur (clavier ou souris), soit une page web du site auquel il est connecté. Le système d'exploitation réalloue ces temps d'attente à d'autres processus.

- Le deuxième consiste à découper le temps d'utilisation du processeur en petits intervalles (de l'ordre de 100 à 500 ms), et à les allouer successivement aux processus éligibles et non en attente d'événements. Ce mécanisme est appelé «temps partagé» (ou «time-shearing» en anglais).
- Aux deux mécanismes précédents peuvent se surajouter des notions de priorités d'exécution attachées aux processus qui permettent de favoriser les tâches présentant des contraintes particulières (notamment dans les systèmes d'exploitation dits «en temps réel»)

La simultanéïté n'est donc réelle que dans les machines équipées de plusieurs processeurs indépendants et d'un O.S. qui gère cette exécution simultanée. Sinon, il s'agit de simultanéïté «apparente». Bien évidemment, si l'O.S. est **monotâche** (MS-DOS, par exemple), ou si aucun autre processus n'est éligible lors de son chargement, un processus passera immédiatement en exécution après son chargement en mémoire.

NOTA:

Dans un ordinateur, toute activité, qu'elle soit liée au système d'exploitation ou à un utilisateur passe par l'exécution d'un processus logiciel. Un ordinateur dans lequel aucun processus logiciel (pas même un processus du système d'exploitation) n'est en exécution ou au moins en attente d'événement est soit arrêté, soit en panne.

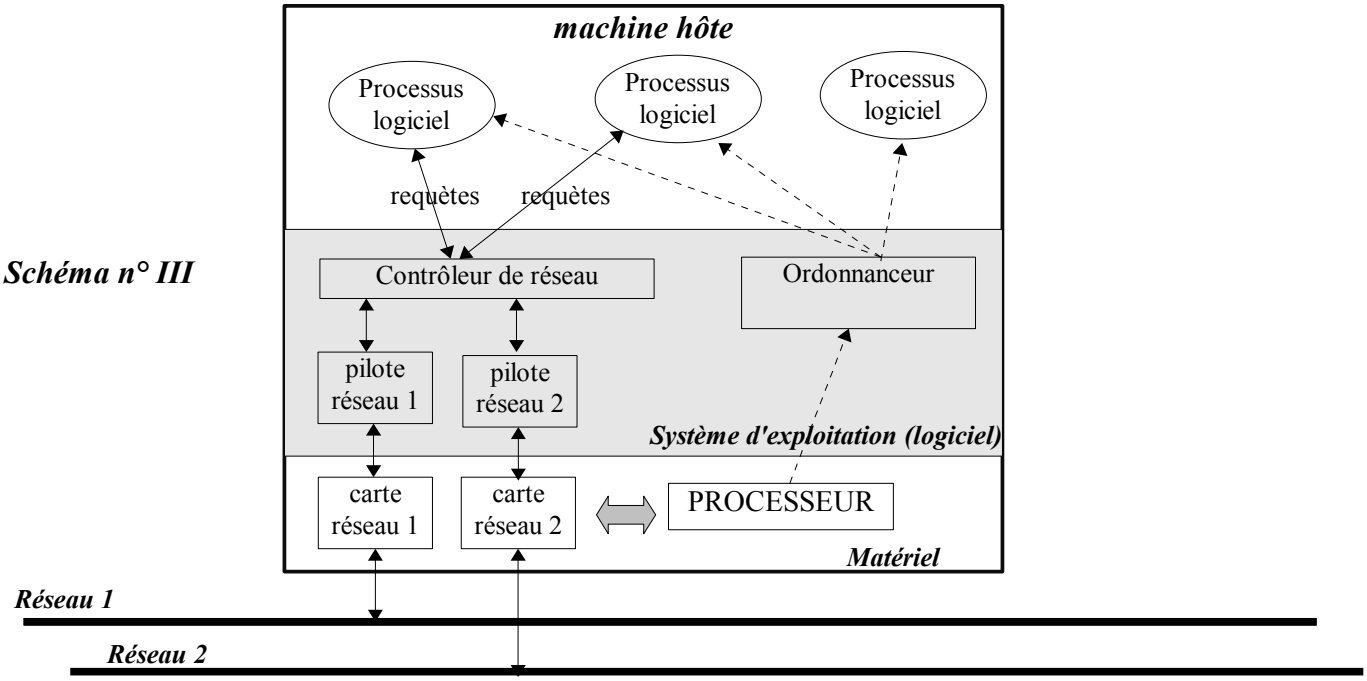
II.3.2.3 RÔLE DU SYSTEME D'EXPLOITATION DANS LA COMMUNICATION RESEAU:

Le système d'exploitation lui-même n'est rien d'autre qu'un **logiciel** particulier qui se lance au démarrage de la machine (boot). Il s'exécute sous la forme de plusieurs processus logiciels dont les deux principales missions sont:

- L'ordonnancement de l'exécution des processus (de ses propres processus et de ceux des utilisateurs).
- La gestion de la communication entre les processus (logiciels) et le matériel.

Le composant du système d'exploitation qui gère l'ordonnancement des tâches s'appelle «ORDONNANCEUR» en français, ou encore «SCHEDULER» en anglais. Les composants du systèmes qui gèrent la communication entre les processus logiciels utilisateurs et les organes d'entrée-sortie s'appellent «contrôleurs» quand ils gèrent un certain type d'entrée-sortie ou «pilotes de périphériques» («drivers» en anglais), quand ils sont chargés de gérer un périphérique particulier. Le schéma suivant illustre les rapports entre le système d'exploitation et les processus utilisateurs d'une part et avec la périphérie matérielle d'autre part.

Schéma n° III



COMMENTAIRES:

- L'ordonnanceur, que nous voyons figurer dans le système d'exploitation est chargé de gérer l'allocation du processeur matériel à l'exécution des différents processus utilisateurs.
- Pour communiquer avec un réseau, les processus adressent au système d'exploitation des requètes (ici, requètes d'entrée-sortie). Ces requètes vont activer le logiciel contrôleur de réseau, qui va se charger d'aiguiller l'exécution vers le pilote de périphérique correspondant au réseau désiré. Ce pilote de périphérique va se charger de piloter l'équipement matériel, de façon à assurer l'opération d'entrée-sortie désirée.

REMARQUE: *Ce mécanisme n'est pas spécifique à a communication réseau: il pourrait s'appliquer à n'importe quel type d'opération d'entrée-sortie.*

II.4 DIFFERENTS TYPES DE RESEAUX:

On distingue communément 2 types de réseaux, en fonction de leur taille et de leur destination: les réseaux locaux et les réseaux étendus.

II.4.1 LES RESEAUX LOCAUX:

On désigne souvent les réseaux locaux sous l'acronyme L.A.N. (Local Area Network). Un réseau est dit local lorsqu'il réalise l'interconnection des systèmes informatiques d'une organisation (entreprise, association, administration, etc) regroupée dans une même implantation géographique, à l'intérieur d'un seul bâtiment ou d'un groupe de bâtiments situés sur une même implantation géographique.

II.4.2 LES RESEAUX ETENDUS:

Ils sont communément désignés par l'acronyme W.A.N. (Wide Area Networks). Contrairement aux L.A.N, ils peuvent interconnecter des systèmes informatiques ou des réseaux locaux dispersés sur plusieurs implantations: ainsi, un WAN peut interconnecter les réseaux locaux de différentes agences d'une même entreprise.

II.4.3 DIFFERENCES ENTRE RESEAUX LOCAUX ET RESEAUX ETENDUS:

Les interconnexions à l'intérieur d'un réseau local n'excèdent pas, en général, quelques centaines de mètres. Ces faibles distances autorisent l'utilisation de médias et de technologies de transmission simples, même pour des volumes d'informations élevés. D'autre part (et, c'est peut-être la condition la plus dimensionnante), la totalité des équipements d'un réseau local est installée sur le domaine de l'organisation qui le possède et l'utilise. Celle-ci maîtrise donc totalement le choix des matériels et des technologies utilisées, des modes et conditions d'utilisation et des accès au réseau. En particulier, l'ensemble du système peut être fourni par un seul constructeur, ce qui garantit la compatibilité des différents composants. Les L.A.N. sont des réseaux **fermés**, c'est à dire dédiés uniquement à un certain type d'utilisateurs et n'hébergeant que certains services, en fonction des choix du propriétaire.

En revanche, dans le cas d'un réseau étendu, il sera parfois impossible que l'organisation assure certaines liaisons avec ses propres matériels (par exemple, la liaison entre deux agences situés dans des implantations éloignées), pour des raisons de coût, et parce que ces liaisons nécessiteraient l'occupation ou la traversée du domaine public ou de domaines privés de particuliers ou d'autres organisations. De ce fait, il sera nécessaire pour assurer ces liaisons, d'utiliser des infrastructures publiques (réseau de télécommunication NUMERIS, par exemple). De ce fait:

- Contrairement à un réseau local, un réseau étendu interconnectera la plupart du temps des systèmes hétérogènes du point de vue des types de matériels et des technologies. Il devra donc intégrer des mécanismes de passerelles résolvant les incompatibilités entre les différents éléments.
- D'autre part, la transmission d'informations sur de longue distances impose des technologies adaptées, en général plus élaborées et plus coûteuses que celles qui suffisent pour un L.A.N.

Dans la catégorie des réseaux étendus on trouvera:

- Les Réseaux «d'entreprises», qui permettent l'interconnexion de sites éloignés d'une même organisation. Ils sont en général composés de réseaux locaux interconnectés par des équipements passerelles (routeurs d'agences) qui utilisent les services d'infrastructures publiques. Ce type de réseau reste un réseau **fermé**, dédié uniquement aux besoins de l'entreprise.
- Les Réseaux grand public (métropolitains, nationaux, mondiaux) du type d'internet. Il s'agit de réseaux **ouverts**, dont la vocation est d'intégrer (dans la mesure du possible) tous les types d'utilisateurs et tous les types de services.

II.5 SYSTEMES REPARTIS:

II.5.1 DEFINITION:

Un système informatique est dit «**réparti**» lorsqu'il est composé de sous-systèmes:

1. Indépendants et autonomes du point de vue de leur technologie, de leur structure et de leur fonctionnement.
2. Distants géographiquement.
3. Coopérant entre eux sans notion de hiérarchie.

II.5.2 CONSEQUENCES:

- Le premier point implique la faculté de gérer la communication entre des sous-systèmes hétérogénes du point de vue des matériels et des systèmes d'exploitation. Ceci implique de disposer de mécanismes (matériels, logiciels, protocoles d'échange) de haut niveau pour assurer l'adaptation des échanges entre systèmes différents.
- D'autre part, une conséquence de l'exigence d'autonomie est la nécessité de disposer de **mécanismes de synchronisation** entre les processus supportés par les différents composants.
- Le deuxième point implique un système d'interconnexion physique adapté au transport d'informations sur des distances importantes. En effet, les contraintes (parasitage, perte en ligne, etc..) ne sont pas du tout les mêmes qu'à l'intérieur d'un système localisé.
- Enfin, du fait de l'absence de hiérarchie entre les sous-systèmes, les fonctions de surveillance du fonctionnement, de détection des erreurs, de synchronisation et d'ordonnancement des traitements sont forcément réparties: ceci implique une **coopération** entre sous-systèmes basée sur une **suspicion** mutuelle, chacun d'entre eux accomplissant une partie des fonctions de surveillance.

II.5.3 COOPERATION ENTRE PROCESSUS:

Dans un système réparti, chaque sous-système matériel supporte un certain nombre de processus logiciels en cours d'exécution. Ces processus doivent coopérer afin d'accomplir les missions assignées au système réparti. Cette coopération se traduit par un certain nombre d'activités. Par exemple:

- Transmission de données et de commandes entre processus et contrôle des échanges.
- Déclenchement ou arrêt d'un processus par un autre.
- Synchronisation des traitements de processus différents.
- Contrôle des accès aux ressources communes.

Actuellement, il n'existe pas de système d'exploitation supportant ces types de traitements à l'échelle d'un système réparti: chaque sous-système possède son propre système d'exploitation qui n'assure ces tâches que localement. En revanche, il existe des **PROTOCOLES** de communication qui permettent à des processus répartis sur des systèmes matériels différents d'échanger des données et des commandes, de mettre en commun certaines ressources et de synchroniser leurs traitements. Ces protocoles utilisent en général des réseaux informatiques.

II.5.4 CONCLUSION:

De ce qui précède, il découle que le principal composant d'un système réparti est une interconnexion de **réseaux informatiques**. De fait, la plupart des technologies de réseau existantes prennent en charge une bonne part de la problématique des systèmes répartis, non seulement en ce qui concerne la transmission de l'information à l'intérieur du système, mais aussi en ce qui concerne la coopération entre les processus logiciels répartis.

III RESEAUX ET NORMALISATION I.S.O:

III.1 INTRODUCTION:

Le développement des systèmes informatiques en réseau débute dès la fin des années 1960. A cette époque, la multiplication des applications de l'informatique dans le domaine professionnel fait apparaître l'intérêt d'interconnecter les différents systèmes de traitement d'un même organisme (entreprise, administration, etc.). Il s'agit donc surtout de réseaux d'entreprises, car à cette époque, il n'existe pas d'informatique «grand public», les matériels étant bien trop onéreux et encombrants, leur utilisation trop peu «conviviale» et les applications bien trop «professionnelles» pour s'adresser aux particuliers.

Pour satisfaire ces besoins, les entreprises se tournaient vers les systèmes fournis par les grandes entreprises du moment: SNA pour IBM, DNA pour DEC, AppleTalk pour Apple, etc. Cependant, ces architectures conçues à partir de technologies spécifiques à chaque fournisseur montrèrent vite leurs limites face à l'évolution rapide des besoins:

- Impossibilité (en général) d'y intégrer des composants en provenance d'un autre constructeur.
- Grandes difficultés pour interconnecter des réseaux de constructeurs différents.

Ces inconvénients constituaient des freins à l'évolution de l'informatisation des société et des menaces pour la pérennité des systèmes (en cas d'arrêt de production d'un type de matériel, par exemple).

Dès 1969, la Defense Advanced Research Project Agency (D.A.R.P.A), du Département de la Défense des U.S.A mis en service le réseau étendu ARPA-Net interconnectant certains centres de recherche et universités des U.S.A.

En 1974, le protocole de transmission TCP-IP fut introduit sur ARPA-Net, constituant un premier standard de communication (non lié à un constructeur).

En 1976, le CCITT (Comité Consultatif International Télégraphique et Téléphonique) définit le protocole de communication X25. Ce protocole, issu de la collaboration de cinq états (Etats unis, France, Canada, Belgique, royaume Uni), allait, en particulier, être utilisé par France Télecom pour son réseau TRANSPAC (minitel), entré en service en 1979. TRANSPAC a été le premier réseau «grand public» disponible au niveau d'un état.

Dès 1978, l'I.S.O (International Standards Organisation, dépendant de l'O.N.U.) décida de mettre de l'ordre dans les architectures réseau en créant des normes. Le but recherché était de faciliter l'INTERCONNEXION de systèmes OUVERTS (c'est à dire accueillant des hôtes de nature hétérogènes). Le Modèle O.S.I (Open Systèms Interconnection), résultat de ses travaux avait pour objectifs:

- De permettre l'interconnexion de systèmes hétérogènes.
- D'éviter la mainmise d'un fournisseur particulier sur la clientèle (possibilité de construire des architectures hétérogènes pourvu que les composants respectent certaines recommandations concernant leurs interfaces et les protocoles de communication).
- De permettre l'adaptation des infrastructures à l'augmentation des besoins en termes de flux d'informations sans remettre en cause les investissements antérieurs.

Le modèle O.S.I. n'a pas rendu obsolète les standard TCP-IP ou X25. Le fait que ces architectures s'insèrent assez facilement dans le modèle OSI laisse même à penser que l'ISO s'est largement inspiré d'elles dans ses travaux. En fait, même si les solutions réseau proposées actuellement couvrent rarement toutes les recommandations du modèle OSI, celui-ci est un excellent outil pour l'analyse et la compréhension de la problématique des réseaux.

III.2 LE MODELE O.S.I:

III.2.1 OBJECTIFS:

Le modèle O.S.I. se donne pour objectif de définir un ensemble de règles architecturales permettant de concevoir et de réaliser des systèmes d'interconnexion ouverts (Open Systems Interconnexion), c'est à dire pouvant être bâtis à partir de composants **hétérogénes** (issus de fournisseurs différents et de technologies différentes) et **évolutifs** (adaptables à l'évolution des besoins et des technologies).

D'autre part, le modèle doit englober tous les cas, depuis le cas simple de la communication point à point entre deux machines de même type et de même système d'exploitation jusqu'au cas complexe où deux processeurs situés dans des hôtes de types différents, munis de systèmes d'exploitation différents et hébergés par des sous-réseaux de technologies différentes, distants l'un de l'autre, dialoguent par l'intermédiaire d'un réseau étendu.

III.2.2 PRINCIPES GENERAUX DE LA DECOMPOSITION EN COUCHES:

III.2.2.1 PROBLEMATIQUE GLOBALE:

La problématique globale traitée par le modèle O.S.I. est la **communication entre deux applications informatiques** hébergées par **deux hôtes distants** d'un même **réseau étendu**. Une application informatique s'exécutant sous forme de processus logiciels, la communication sera donc, en fait, **établie entre deux processu**s.

Le schéma n° IV (voir plus loin) donne une représentation graphique de la situation: nous pouvons prendre pour exemple, pour fixer les esprits, le processus A1.1 de l'hôte A1 du L.A.N. A communicant avec l'hôte B1.3 de l'hôte B1 du L.A.N. B.

Au niveau d'une application informatique, un message est représenté par une structure de données plus ou moins complexe renfermant les informations à communiquer. C'est cette structure de données qu'il va falloir faire parvenir au processus destinataire, sous une forme exploitable par celui-ci. L'acheminement du message depuis l'émetteur vers le destinataire va poser deux sortes de problèmes:

- Le problème de l'adaptation du mode de représentation de l'information aux différents supports.
- Le problème de l'acheminement des informations à travers le réseau.

III.2.2.2 ADAPTATION DE L'INFORMATION AUX SUPPORTS:

Durant son «voyage», de l'émetteur au récepteur, l'information va utiliser différents supports: les mémoire vives des hôtes communicants et des commutateurs, les médias de transport (paire torsadée, fibre optique, ondes électromagnétiques, etc.). A chacun de ces supports correspond un mode de représentation particulier de cette information. Par exemple:

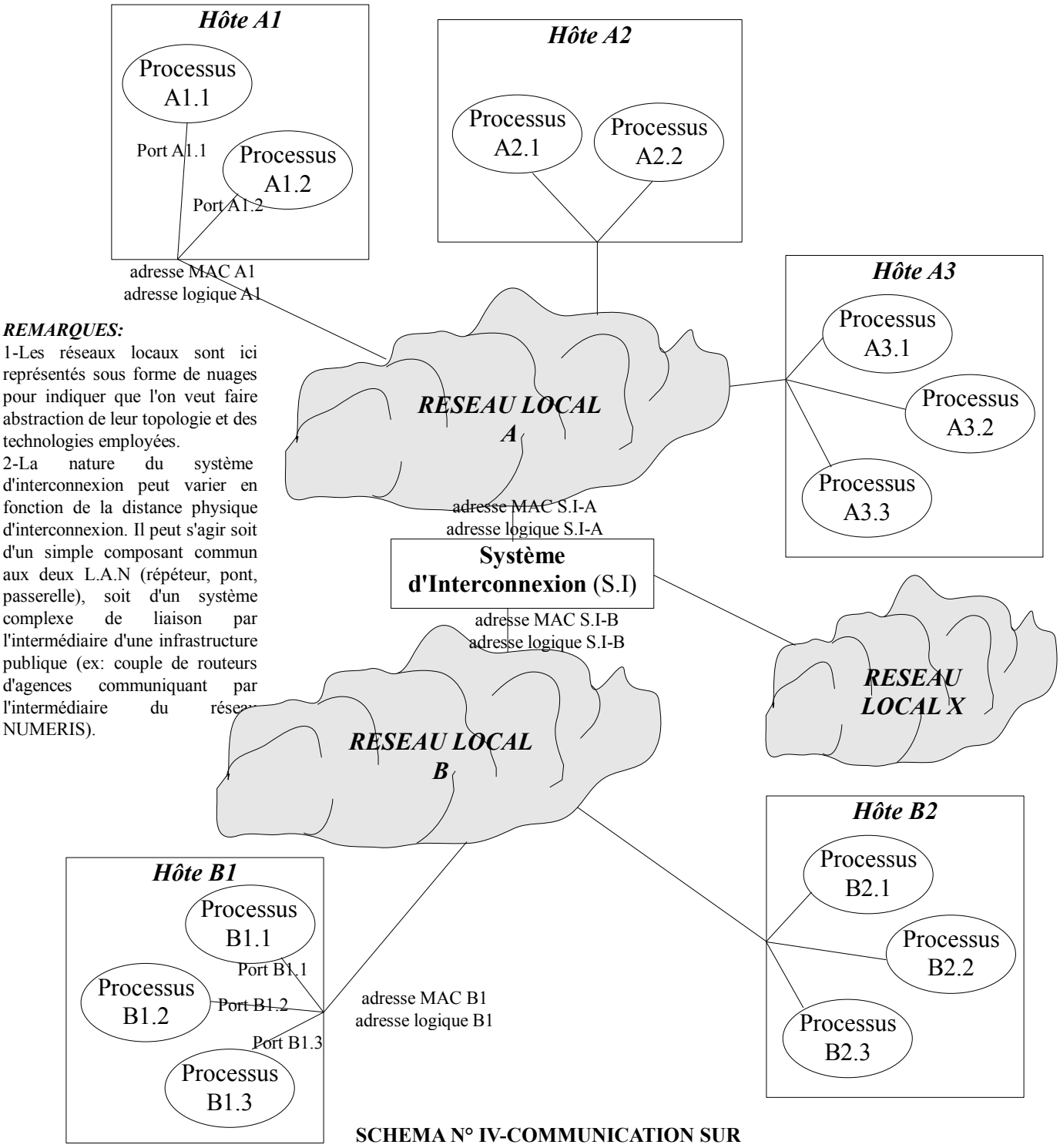
- Au niveau des applications, la représentation des données n'est pas forcément identique dans les deux hôtes: un entier n'est pas représenté de la même manière dans un système UNIX et dans un système WINDOWS. Cette particularité induira la nécessité de faire des conversions de formats de représentation des données avant de présenter le message au destinataire.
- Au niveau des médias de transport, l'information n'est plus représentée par des configurations binaires statiques, mais par des trains d'impulsions (électriques, optiques, etc..) circulant sur ces médias. Il faudra donc effectuer une conversion lors de l'injection sur le média et la conversion inverse lors de l'acquisition des signaux par le système matériel destinataire.
- La plupart des médias imposent une limite à la durée d'un train d'impulsions, qui oblige à des opérations de segmentation-réassemblage des messages.
- Etc.

La communication exigera donc une succession de conversions de formats de représentation (en général suivies de la conversion inverse).

III.2.2.3 ACHEMINEMENT DES INFORMATIONS A TRAVERS LE RESEAU:

L'acheminement des informations à travers le réseau pose le problème de l'adressage. Ce problème ne peut être résolu par un seul système d'adressage reliant les différents processus tournant sur les hôtes du réseau. En effet:

- D'une part, un processus logiciel étant une entité éphémère, il est impossible de lui attribuer une adresse fixe.
- D'autre part, le modèle devant rester ouvert, la communication doit pouvoir s'adapter, à chaque niveau de traitement, au système d'adressage associé à la technologie de transmission utilisée pour ce niveau.



REMARQUES:

1-Les réseaux locaux sont ici représentés sous forme de nuages pour indiquer que l'on veut faire abstraction de leur topologie et des technologies employées.

2-La nature du système d'interconnexion peut varier en fonction de la distance physique d'interconnexion. Il peut s'agir soit d'un simple composant commun aux deux L.A.N (répéteur, pont, passerelle), soit d'un système complexe de liaison par l'intermédiaire d'une infrastructure publique (ex: couple de routeurs d'agences communiquant par l'intermédiaire du réseau NUMERIS).

SCHEMA N° IV-COMMUNICATION SUR UN RESEAU ETENDU

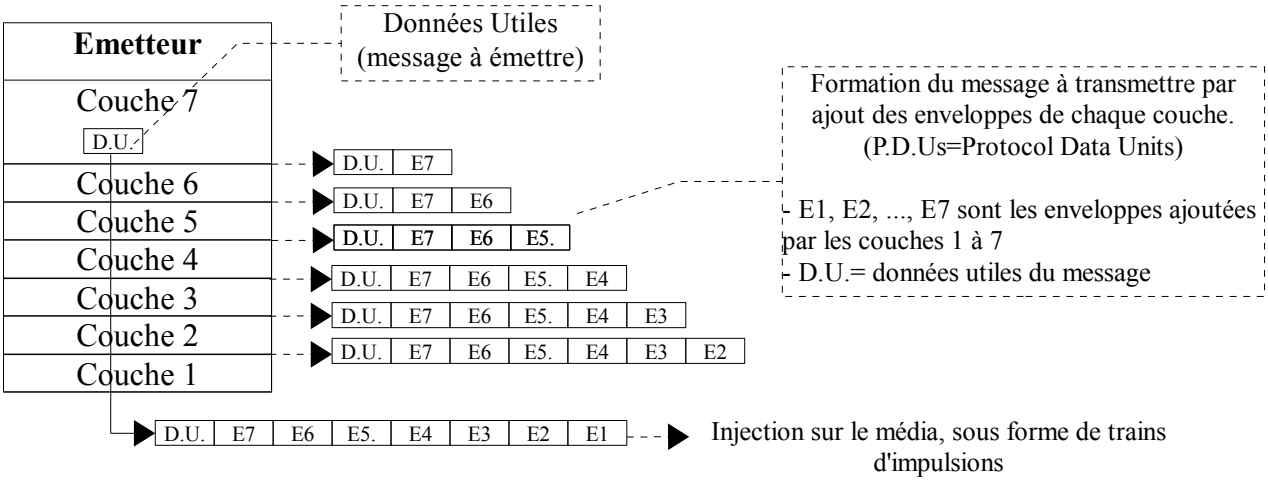
III.2.3 DESCRIPTION GLOBALE:

Le modèle OSI structure la communication entre processus logiciels en sept «couches» de traitements (logiciels et matériels):

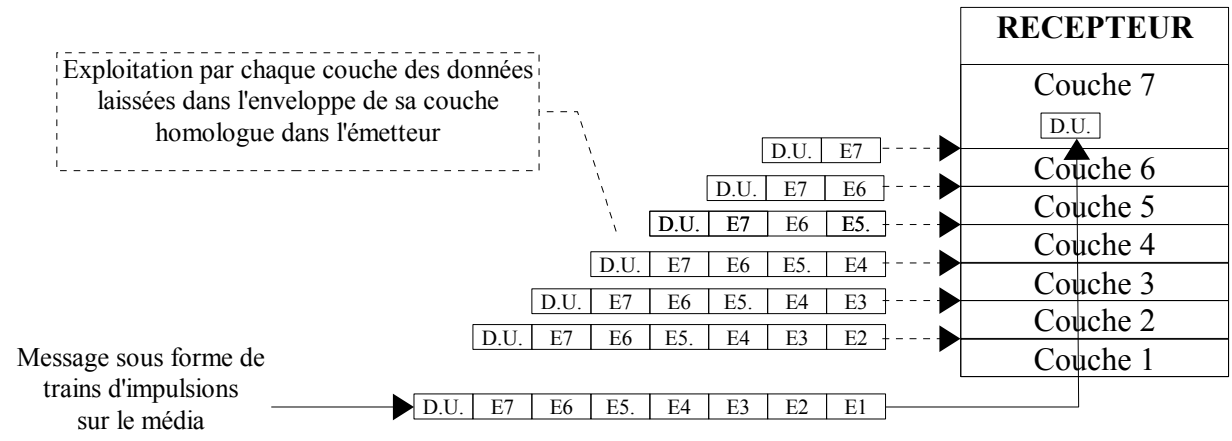
- Dans l'émetteur, un message est traité successivement par les couches de 7 à 1, de façon à passer de la représentation du message sous forme de structure de données à sa représentation sous forme de trains d'impulsions à injecter sur le média, contenant toutes les informations d'adressage nécessaires à son acheminement.
- Dans le récepteur, le message est traité successivement par les couches de 1 à 7, de façon à passer de la représentation du message sous forme de trains d'impulsions extraites du média à sa représentation sous forme de structure de données en mémoire, débarrassée des informations d'adressage et converties au format de représentation de l'hôte récepteur.

Chaque couche encapsule donc une étape de la communication dans l'émetteur et l'étape inverse (ou symétrique) dans le récepteur. Elle permet aux couches supérieures de **faire abstraction des détails d'implémentation** des couches inférieures (matériels, logiciels, protocoles utilisés par ces couches). Pour ce faire:

Dans l'émetteur, chaque couche opère les changements de représentation et les segmentations utiles, puis ajoute au message une «enveloppe» contenant les données utiles à l'acheminement du message, à son réassemblage, au contrôle de l'intégrité des données, puis passe le message à la couche inférieure:



Dans le récepteur, chaque couche exploite l'enveloppe ajoutée par son homologue dans l'émetteur, puis passe le message à la couche supérieure:



REMARQUE:

La couche n° 1 correspond au matériel de connexion (cartes réseau). Les autres couches sont des couches logicielles.

UNITE DE DONNEES DE PROTOCOLES (P.D.Us):

Pour une couche donnée, on appelle Protocol Data Unit (P.D.U.) le bloc composé des données utiles et des enveloppes ajoutées par cette couche et par les couches supérieures du modèle OSI (Par exemple, les P.D.U. de la couche 4 sont composés des données utiles et des enveloppes E7, E6, E5 et E4). On note souvent (N)-PDU l'unité de donnée de protocole de la couche N.

Rappelons que certaines couches encapsulent des mécanismes de segmentation (émission) – réassemblage (réception). A un P.D.U de la couche N peuvent donc correspondre plusieurs P.D.U.s de la couche N-1.

LES POINTS D'ACCES AUX SERVICES:

Chaque couche offre au niveau supérieur un certain nombre de points d'activation appelés **Service Acces Points** (S.A.P). Il s'agit en fait de primitives logicielles permettant d'activer les mécanismes encapsulés dans cette couche. Les arguments échangés par ces primitives sont appelés Service Data Units (S.D.U), qui correspondent aux données utiles encapsulées par les enveloppes correspondant aux couches supérieures (Donc, le S.D.U. d'un S.A.P. de la couche N est un (N+1)-PDU).

LES INFORMATIONS DE CONTRÔLE DE PROTOCOLE(P.C.I.):

Les informations contenues dans les enveloppes de protocole sont appelées Protocol Control Informations (P.C.I). Un P.D.U donné est donc formé du P.D.U. transmis par la couche supérieure et des P.C.I. ajoutées par la couche:

(N)-PDU = (N+1)-PDU+(N)-PCI

Les enveloppes des différentes couches pourront comprendre les informations suivantes:

- La longueur du segment de données encapsulé dans le P.D.U.
- Les informations permettant l'adressage de l'entité réceptrice et, le cas échéant, le retour de compte-rendus vers l'entité émettrice (suivant la couche, ces entités pourront être des machines ou des processus dans des machines)
- L'identificateur du protocole utilisé dans la couche émettrice. Cette information permettra à la couche homologue réceptrice de déterminer le traitement à appliquer à l'enveloppe du P.D.U.
- Des informations de contrôle de la transmission (checksum, CRC, etc). Celles-ci permettront à la couche homologue réceptrice de vérifier l'intégrité des données transmises.
- En cas de segmentation-réassemblage des messages, numéro de séquence du segment de données correspondant au P.D.U. Ces informations permettront de réassembler le message dans le bon ordre ou de détecter la perte éventuelle d'un segment (détection de time-out).
- Et toute information liée aux mécanismes implémentés dans la couche émettrice.

REMARQUE:

Les organes d'interconnexion des réseaux utilisent également les informations contenues dans les différentes couches pour effectuer le routage des messages.

III.2.4 MECANISMES DES COUCHES O.S.I:

III.2.4.1 LA COUCHE N° 1 (COUCHE PHYSIQUE):

SERVICES OFFERTS PAR LA COUCHE:

Cette couche assure et contrôle la transmissions d'impulsions (électriques, optiques, etc.) sur le canal de communication (média physique). Les P.D.Us de cette couche («trames physiques») sont des trains d'impulsions codant les configurations binaires représentant les données à transmettre, auxquelles sont additionnées des impulsions de synchronisation permettant de reconnaître les débuts et fins de trames. La dénomination «couche physique» vient du fait que ces traitements sont supportés par les composants matériels de liaison (cartes réseau et médias).

La couche physique permet de faire abstraction des détails d'implémentation suivants:

- Caractéristiques de la technologie de transmission des médias (paires torsadées, coaxiaux, fibre optique, transmission wifi, etc.)
- Caractéristiques mécaniques (connecteurs, topologie, etc.)
- Mécanismes de transmission des trames physiques (codage électrique ou optique, synchronisation émetteur-récepteur, procédures d'établissement, de maintien et de libération du circuit de données).

TRAITEMENTS EN EMISSION:

Pour émettre des données sur le réseau A, l'hôte A1 va devoir les transformer en une trame physique adaptée au média du réseau A, puis injecter ces impulsions sur ce média. Pour ce faire:

- Les données à émettre (configurations binaires en mémoire vive) vont d'abord être transformées en impulsions électriques en fonction du type de codage choisi. Des impulsions de synchronisation vont être ajoutées pour permette au récepteur de détecter les débuts et fin de trame.
- Ces impulsions seront ensuite soit injectées telles-quelles sur le média (transmission en bande de base), soit utilisées pour moduler une onde porteuse qui sera injectée sur ce média (transmission en modulation).
- Si le média n'est pas un conducteur électrique, les signaux devront subir une dernière transformation avant injection sur le média: transformation en signaux luminaux (fibre optique) ou en ondes hertziennes (transmission sans fil)

TRAITEMENTS EN RECEPTION:

La couche physique du destinataire devra acquérir les signaux sur le média, puis effectuer les transformations inverses:

- Conversion en signaux électriques (si le média n'est pas un conducteur électrique)
- Détection de la porteuse et démodulation (si la transmission n'est pas en bande de base)
- Suppression des bits de synchronisation.
- Transformation des signaux électriques en configurations binaires en mémoire.

ENVELOPPE DE LA COUCHE PHYSIQUE:

Elle est constituée par les bits de synchronisation.

III.2.4.2 LA COUCHE N° 2 (COUCHE LIAISON):

SERVICES OFFERTS PAR LA COUCHE:

La couche liaison permet d'établir des liaisons de données entre des hôtes connectés **au même média physique**. Cette couche permet donc de définir un réseau local entre machines.

La couche liaison offre des traitement de segmentation-réassemblage du flot de données permettant d'adapter la longueur des trames physiques aux contraintes du média.

D'autre part, la couche assure le contrôle de la transmission qui permet de s'assurer du bon acheminement des trames.

Enfin, pour effectuer un échange de données, la couche physique n'est suffisante que dans le cas d'une liaison «point à point» c'est à dire concernant uniquement un couple de machines. Or, un réseau est, par définition, destiné à accueillir plus de deux hôtes. De ce fait, la couche liaison encapsule:

- Un système d'adressage des messages permettant à la machine émettrice de **spécifier** la machine destinataire du message, et à la machine destinataire de **reconnaître** les messages qui lui sont destinés.
- Des mécanismes contrôlant l'accès des machines au média, et en particulier, de régler le problème des accès simultanés en émission.

REMARQUES:

- Les traitements correspondant à l'adressage physique et à l'accès de l'émetteur au média font partie de la sous-couche **M.A.C. (Média Acces Control)**
- Les traitements de segmentation-réassemblage et de contrôle de la transmission qui permettent de s'assurer du bon acheminement des messages constituent la sous-couche L.L.C.(**Logical Link Contrôl)**.

ADRESSAGE PHYSIQUE

Les composants de connexion réseau («cartes réseau») intègrent un identificateur appelé «adresse physique». Pour un composant donné d'une technologie donnée, cette adresse (configuration binaire) est unique et codée «en dur» dans le matériel (par exemple, toutes les cartes de connexion de technologie ethernet possèdent une adresse physique codée sur 6 octets). Cette adresse, qui peut être lue par la machine hébergeant le composant, peut donc servir à adresser des machines interconnectées au moyen du même type de matériel réseau, ce qui est le cas dans un L.A.N.

REMARQUES:

- L'adresse physique est le plus souvent appelée: **adresse M.A.**C (adresse Média Accès Contrôl),
- L'adresse MAC identifie la connexion d'un hôte à un réseau (en fait, son matériel de connexion). Un hôte possède donc autant d'adresses MAC que de connexions réseau.
- L'adresse MAC **broadcast** est une adresse particulière qui permet d'acheminer un message vers tous les hôtes d'un L.A.N.

ACCES AU MEDIA:

Sauf emploi de technologies très particulières que l'on trouve rarement sur un réseau local (multiplexage en fréquences), le transport **simultané** de plusieurs messages sur le même média est impossible. Les mécanismes d'accès au média ont donc pour but de s'assurer que lorsqu'un hôte émet, il est le seul à le faire pendant toute la durée de l'émission. Il existe deux catégories de méthodes d'accès:

- L'accès aléatoire, (appelé encore «par contention») dans lequel le candidat émetteur «écoute» ce qui se passe sur le média et émet dès que celui-ci est libre.
- L'accès partagé dans le temps qui accorde successivement à chaque hôte du réseau un droit d'émission. Ce droit est appelé «jeton» (en anglais: token).

TRAITEMENTS EN EMISSION:

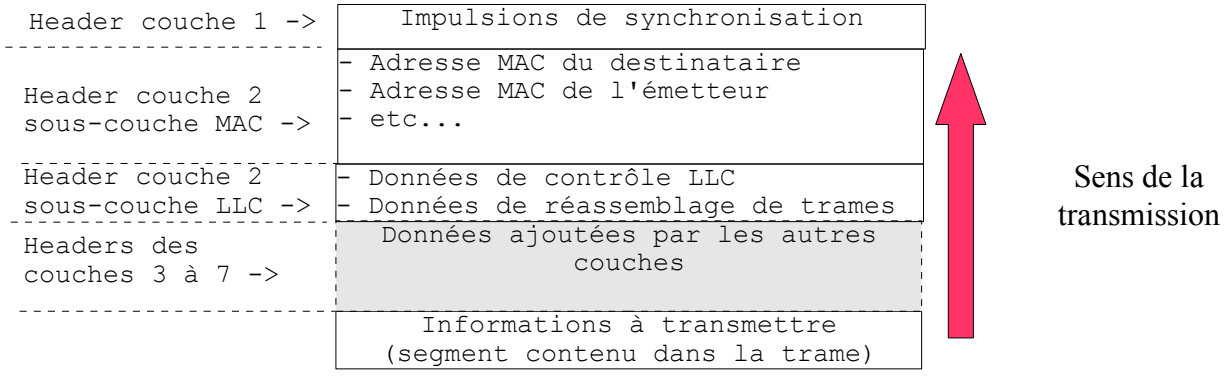
- En fonction de la taille des S.D.Us transmis par la couche 3, la sous-couche LLC segmente le flot de données en **trames** de longueur inférieure ou égale à la dimension maximale supportée par la technologie du média (Maximum Transfer Unit: M.T.U). Pour internet, la M.T.U. est 1500 octets.
- Puis, la sous-couche LLC encapsule chaque trame dans une enveloppe contenant des paramètres de réassemblage des trames et de contrôle de la liaison (check-sums, CRC, etc). Ces paramètres forment l'enveloppe LLC
- La couche MAC ajoute au message les adresses MAC de l'émetteur et du destinataire, qui font donc partie de l'enveloppe MAC
- Puis, la couche MAC tente d'accéder au média en utilisant la méthode d'acces implémentée.

TRAITEMENTS EN RECEPTION:

- Lorsque la couche physique lui transmet un message, la sous-couche MAC d'un hôte compare l'adresse MAC du destinataire, contenue dans l'enveloppe MAC du message à l'adresse MAC du récepteur. S'il y a concordance, le message est transmis à la sous-couche LLC
- La sous-couche LLC récupére les paramètres de contrôle du message contenues dans la sous-couche LLC et les compare aux mêmes données calculées à partir du message reçu pour déterminer si la transmission a été bonne. En cas d'erreur, un message d'alarme est renvoyé à l'émetteur.
- Puis, la sous-couche LLC réassemble les trames reçues avant de transmettre les informations aux couches supérieures.

ENVELOPPE TOTALE DE LA COUCHE LIAISON:

Cette enveloppe va comprendre les headers correspondant aux deux sous-couches (MAC et LLC):



III.2.4.3 LA COUCHE 3 (COUCHE RESEAU):

SERVICES OFFERTS PAR LA COUCHE:

La couche réseau permet d'assurer la communication entre deux (ou plusieurs) **hôtes** à travers un **réseau étendu** (c'est à dire à travers une interconnexion de réseaux locaux). Cette opération, appelée **routage**, concerne des entités appelées **paquets** d'informations (ces paquets étant eux-mêmes des segments de messages). Les hôtes communicants sont identifiés par un système d'adressage indépendant du matériel appelé **adressage logiques**. La couche gère également les problèmes de congestion des réseaux locaux.

REMARQUE:
Le P.D.U de la couche réseau est appelé «paquet», car il peut s'agir soit d'un message complet échangé entre deux applications réseau, soit d'une portion d'un message segmenté par la couche 4 de l'émetteur. Chaque paquet d'un message est routé individuellement.

NOTION D'ADRESSE LOGIQUE:

Dans le cas d'une communication entre hôtes situés sur des réseaux différents, le mécanisme d'adressage MAC ne permet pas forcément de spécifier l'adresse de la machine destinataire. En effet:

- D'une part, les réseaux interconnectés ne sont pas forcément de même technologie: de ce fait, les systèmes d'adressage peuvent être complètement différents. Il est donc impossible de se contenter de propager simplement les trames avec leurs «enveloppes» des niveaux 1 et 2 sur des réseaux interconnectés.
- D'autre part, dans le cas ou un réseau est connecté à plusieurs autres réseaux, propager un message systématiquement sur tous les réseaux interconnectés aboutirait à une augmentation inutile et surtout incontrôlable du trafic.

De ce fait, la couche 3 de l'OSI implémente son propre mécanisme d'adressage: l'**adressage logique**. Comme les adresses MAC, les adresses «logiques» sont des identificateurs (configurations binaires) attribués à tous les hôtes d'un réseau étendu. Cependant, alors que l'adresse MAC est codée «en dur» dans chaque composant de connexion et ne peut être modifiée, l'adresse logique est indépendante du matériel: c'est l'architecte réseau qui détermine le plan d'adressage logique des différents hôtes.

L'adresse logique d'un hôte sur un réseau local donné peut être décomposée en deux partie: l'adresse du réseau local et l'adresse de l'hôte dans ce réseau local. L'adresse logique a donc l'avantage de permettre de déterminer le réseau destinataire du message. Elle permet donc le **routage inter-reseaux** des messages.

NOTA: *rien n'empêche d'attribuer plusieurs adresses logiques à la même connexion réseau. Cette possibilité permet de créer plusieurs réseaux «logiques» sur le même média.*

RESOLUTION DES ADRESSE LOGIQUES:

La couche 3 permet de masquer l'adresse MAC pour l'utilisateur. Cependant, comme celle-ci est nécessaire pour le fonctionnement de la couche 2, la couche 3 encapsule un mécanisme de résolution des adresses logiques en adresses MAC (Address Resolution Protocol-A.R.P dans l'architecture TCP-IP). Ce mécanisme permet d'entretenir dans chaque hôte une table de correspondance adresse logique --> adresse MAC (cache ARP).

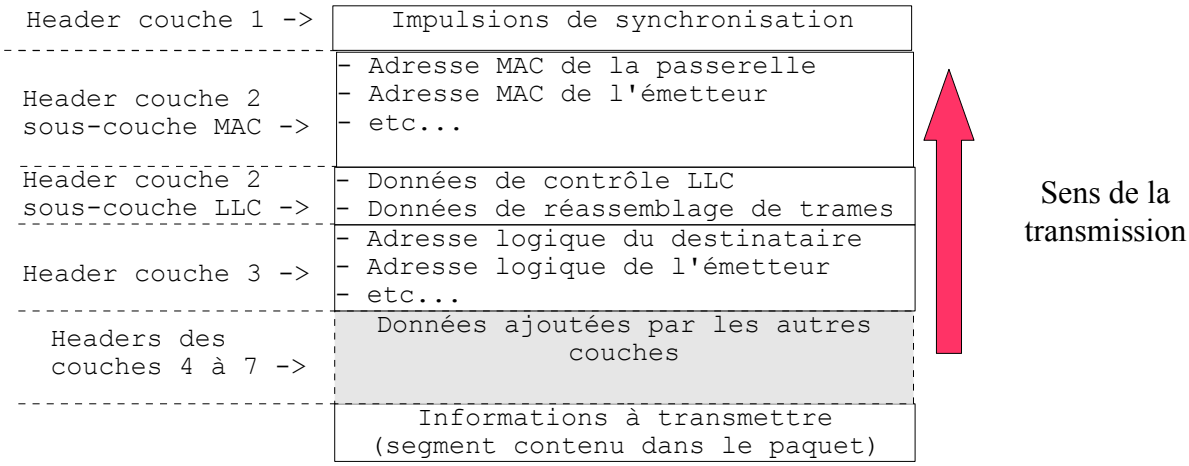
TRAITEMENTS EN EMISSION:

- Lorsque la couche 3 est activée pour une émission vers une adresse logique, elle ajoute au message une enveloppe contenant les adresses logiques de l'émetteur et du destinataire.
- Puis, le mécanisme d'ARP recherche dans le cache ARP l'adresse MAC correspondant à l'adresse logique du destinataire. Si elle existe, la couche 2 est activée pour émission vers cette adresse MAC. Sinon, un message d'interrogation contenant l'adresse logique à résoudre est envoyé vers tous les hôtes du réseau avec une adresse MAC «broadcast». Si l'un des hôtes reconnaît cette adresse logique, il répond par son adresse MAC. La couche 3 active alors la couche 2 avec cette adresse.

TRAITEMENTS EN RECEPTION:

- Lorsque la couche liaison lui transmet un message, la couche réseau compare l'adresse logique du destinataire, contenue dans l'enveloppe MAC du message à l'adresse logique du récepteur. S'il y a concordance, la couche traite les données de l'enveloppe, puis transmet le message à la couche supérieure.

ENVELOPPE DE LA COUCHE RESEAU:



MECANISME DU ROUTAGE INTER-RESEAUX:

Lors de la transmission d'un message entre deux hôtes situés sur deux réseaux différents, l'émetteur adressera physiquement son message non au destinataire (dont il ne peut atteindre l'adresse MAC), mais à l'équipement d'interconnexion. Celui-ci (Il s'agit dans ce cas d'un PONT ROUTEUR) effectuera l'acquisition du message sur la connexion qui le relie au L.A.N de l'émetteur. Puis, il recherchera sur le réseau destinataire l'adresse MAC de la machine destinataire. Il utilisera pour cela un système de tables de routage. Une table de routage renferme, pour chaque réseau connecté au routeur, la correspondance entre les adresses MAC et les adresses physiques des hôtes de ce réseau. Le routeur prélèvera donc dans le message reçu l'adresse logique du destinataire et cherchera dans les tables de routage l'adresse MAC qui lui correspond. Puis il réémettra le message sur le réseau destinataire après avoir placé cette adresse MAC dans le champ «adresse MAC destinataire»:

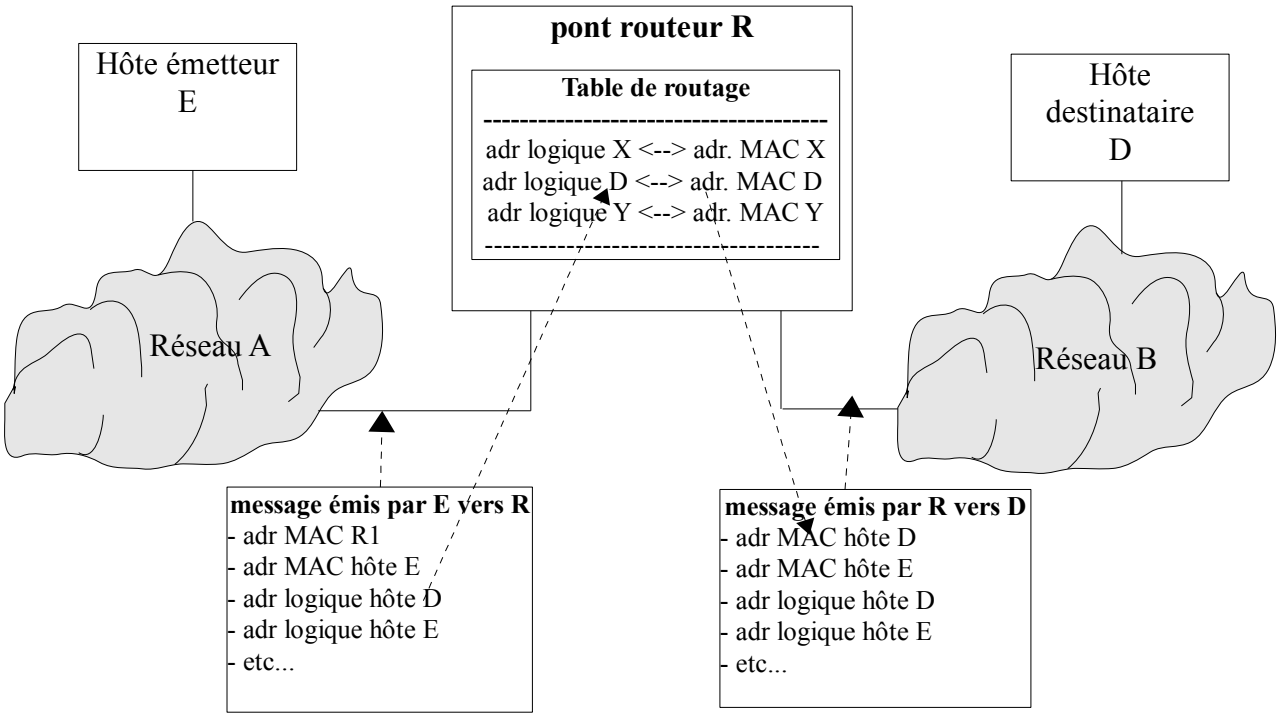


Schéma n° V-Mécanisme de routage

REMARQUES:

- Les **ponts routeurs** sont des composants dans lesquels les couches 1, 2 et 3 de l'OSI sont implémentées. Ils peuvent en général être connectés à plusieurs réseaux de technologies différentes, ce qui leur permet de jouer un rôle de passerelle inter-réseaux.
- Un routeur peut interconnecter directement deux L.A.N ou bien passer par un réseau public. Dans ce cas, l'interconnexion nécessite deux routeurs, chacun effectuant la connexion entre l'un des L.A.N. Et l'infrastructure d'interconnexion.
- Les ponts routeurs qui permettent de se connecter à des infrastructures publiques (de type réseau téléphonique ou internet direct) sont dits «routeurs d'agence» (Les XX-box de connexion internet sont des exemples de routeurs).

L'ensemble de ces mécanismes sont encapsulés dans la couche N° 3 de l'ISO (couche «Réseau»).

III.2.4.4 LA COUCHE 4 (COUCHE TRANSPORT):

SERVICES OFFERTS PAR LA COUCHE:

Cette couche permet d'assurer la communication entre des **processus logiciels** hébergés par des hôtes d'un réseau. Elle assure l'acheminement de bout en bout d'un **message complet** émis par une application réseau, vers un ou des processus destinataires, désignés par leur **numéro de port** (associés à l'**adresse logique** de l'hôte qui les héberge). Les P.D.Us de la couche 4 sont donc des **messages**.

La couche gère l'établissement de circuits logiques (connexions et déconnexions) et contrôle les échanges. C'est elle qui prend en compte la segmentation-réassemblage d'un message en paquets de données.

SELECTION DU PROCESSUS DESTINATAIRE-NOTION DE PORT:

Pour pouvoir recevoir un message réseau, un processus logiciel doit adresser à la couche transport une requète d'ouverture d'un **port** de communication. Ce port, qui est identifié par un simple nombre entier, constitue pour le processus un canal de communication par lequel il peut recevoir des informations sur le réseau. L'identificateur d'un port est unique pour tous les processus d'une machine. Un processus peut ouvrir plusieurs ports.

TRANSMISSION PAR PAQUETS:

Pour assurer une bonne gestion des temps de parole des différents hôtes, il n'est pas souhaîtable qu'un hôte donné émette de manière continue de trop gros flux d'information, bloquant ainsi la communication des autres hôtes. De ce fait, les messages sont souvent transmis par «paquets», de longueur relativement courte (jusqu'à 65536 octets). La transmission par paquets implique des mécanisme de découpage-réassemblage des messages.

De ce fait, les P.D.Us manipulés par la couche 4 contiennent des **messages** alors que les S.D.Us transmis à la couche 3 contiennent des **paquets**.

TRAITEMENTS SUPPORTES EN EMISSION:

Lorsque les couches supérieures activent la couche 4 pour émission, elles lui communiquent, en même temps que le S.D.U correspondant au message à émettre, les identificateurs des ports des processus émetteur et destinataire.

Si un mode de transmission par paquets a été choisi, le message est segmenté. Chaque paquet va être transmis indépendamment à la couche 3 pour émission sur le réseau. L'enveloppe couche 4 de chaque paquet contiendra les données permettant le réassemblage correct du message (numero de sequence du paquet).

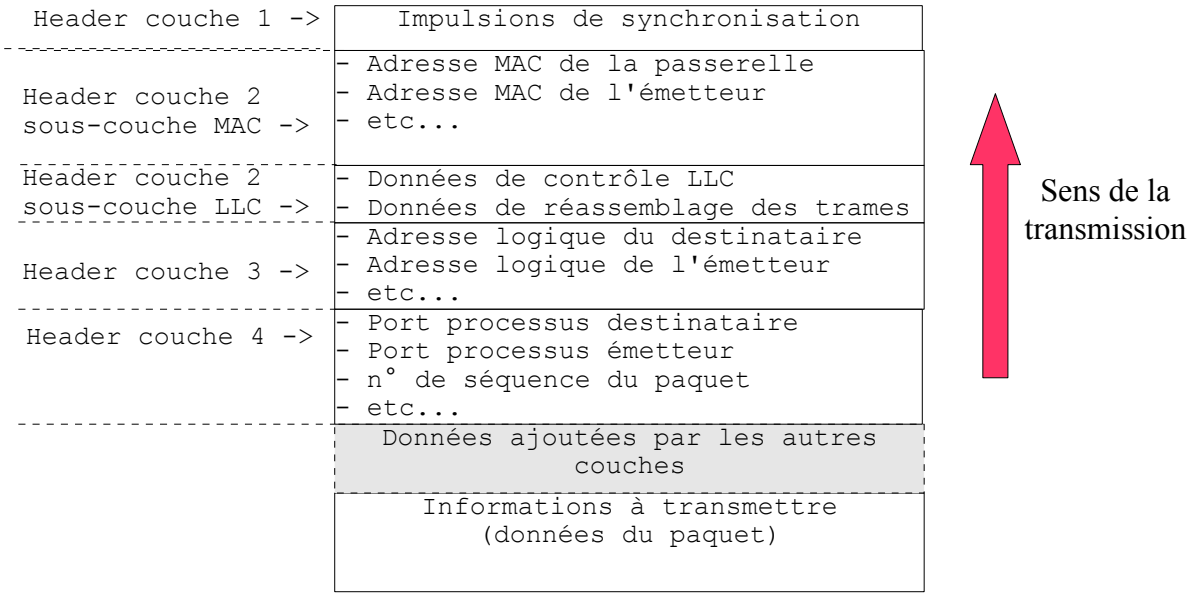
La couche 4 activera la couche 3 pour émission autant de fois qu'il y a de paquets à émettre.

Lorsque la transmission se fait en mode connecté, la couche 4 reçoit, pour chaque paquet émis, un compte-rendu de réception de la part de la couche 4 du récepteur. En cas d'échec, une procédure de réémission est lancée.

TRAITEMENTS SUPPORTES EN RECEPTION:

- Lorsque la couche 3 transmet un message reçu à la couche 4, cette couche procède au réassemblage du message, si nécessaire, en s'aidant des numéros de séquence.
- Si le mode de transmission est un mode «connecté», un compte-rendu de réception est transmis à l'émetteur à la réception de chaque paquet.
- Puis, la couche transport transmet le message aux couches supérieures.

ENVELOPPE DE LA COUCHE TRANSPORT:



III.2.4.5 LA COUCHE 5 (COUCHE SESSION):

SERVICES OFFERTS PAR LA COUCHE:

La couche 5 renferme des mécanismes permettant de gérer les sessions de communication entre applications distantes.

En informatique, une «session d'utilisation» d'un logiciel caractérise une phase d'utilisation de ce logiciel par un utilisateur donné. Une session possède donc un début (ouverture de session, connexion), une phase d'activité et une fin (clôture de session). Certains logiciels pouvant être utilisés simultanément par plusieurs utilisateurs (par exemple, un site web), plusieurs sessions d'utilisation d'un même logiciel peuvent être ouvertes simultanément, par des utilisateurs différents. A une session donnée peuvent être associées un certain nombre d'informations (identification de l'utilisateur, mot de passe, etc.).

La notion de «session des communication» généralise la notion de session au cas où plusieurs utilisateurs communiquent entre eux à l'aide d'applications réseau. La couche session assure la synchronisation entre processus communiquants: elle gère l'établissement et la clôture de la communication et ordonnance les échanges en administrant les «droits de parole».

La couche session permet également de sécuriser les échanges au moyen de «points de reprise» insérés dans le flot de données échangées. Ceux-ci permettent, en cas de dysfonctionnement de la transmission pendant un échange, de reprendre la transmission à partir du dernier point de reprise valide.

ENVELOPPE COUCHE 5:

L'enveloppe de la couche session contiendra des données en rapport avec les services encapsulés (matérialisation de points de reprise, données de session, etc.).

III.2.4.6 LA COUCHE N° 6 (COUCHE PRESENTATION):

SERVICES OFFERTS PAR LA COUCHE:

La couche 6 est, dédiée à la «PRESENTATION des données». Son objectif est de résoudre les différences de représentation des données échangées par les applications communicantes. Les principales causes de différences sont:

- Une différence de représentation de certaines données dans des systèmes d'exploitation différents (par exemple, un système sous window ne représente pas les entiers en mémoire de la même façon qu'un système unix).
- Une différence dans l'alignement des données (Par exemple, pour optimiser l'accès aux données, certains systèmes autorisent l'alignement des adresses des membres d'une structure sur des multiples de 4 octets, introduisant ainsi des «blancs» dans ces structures).
- Le cryptage des informations.
- l'utilisation de procédés de compression des données afin de minimiser le trafic.
- Etc.

Cette couche n'encapsule pas de système d'adressage particulier.

TRAITEMENTS SUPPORTES EN EMISSION:

Suivant les services activés, les S.D.Us transmis par la couche application peuvent être soumis à:

- La conversion des données dans un système dit de «syntaxe abstraite», indépendant des systèmes d'exploitation.
- L'encryptage
- La compression.
- Etc.

L'enveloppe couche 6, ajoutée au P.D.U, devra contenir les informations permettant d'effectuer dans le récepteur les opérations de présentation compatibles avec celui-ci.

TRAITEMENTS SUPPORTES EN RECEPTION:

Ce sont les traitements symétriques de ceux effectués en émission: en fonction des informations contenues dans l'enveloppe de la couche 6, les P.D.Us transmis par la couche 5 seront soumis aux transformations nécessaires pour rendre leur présentation compatible avec les rêgles de présentation locales (décompression , décryptage, conversion de syntaxe abstraite à syntaxe locale). Ensuite, les P.D.Us, débarrassés de leur enveloppe couche 6, seront transmis à la couche application.

III.2.4.7 REMARQUE SUR LES COUCHES 5 A 7:

Dans les architectures réseau (et notamment dans TCP-IP), les couches 5 et 6 sont souvent confondues avec la couche 7. En effet, la plupart des applications réseau proposées prennent place directement sur la couche 4. Ceci revient à dire que ces applications reprennent plus ou moins à leur compte les services des couches session et présentation.

III.2.4.8 LA COUCHE N° 7 (COUCHE APPLICATION):

SERVICES OFFERTS PAR LA COUCHE 7:

La couche 7 héberge les applications qui offrent aux utilisateurs les services de base attachés au réseau (transfer de fichiers, messagerie électronique, accès au web, etc...). De là vient sa dénomination: «couche APPLICATION».

Les applications réseau communicantes ont rarement un rôle symétrique. En général, la communication s'effectue suivant le modèle **client-serveur**: l'application cliente envoie à l'application serveuse des **requètes**, qui sont des demandes de fourniture de services. Le serveur répond par la fourniture du **service** demandé.

EXEMPLES:

- *Un navigateur internet (client HTTP) expédie vers le serveur HTTP d'un site internet une requète de chargement d'une page WEB. Le serveur répond par l'envoi du contenu de cette page.*
- *Un «Client FTP» envoie vers un «serveur FTP» une requète de téléchargement d'un fichier. Le serveur répond par l'envoi du contenu du fichier.*

ADRESSAGE COUCHE 7:

Les applications de la couche 7 doivent, pour accéder aux ressources offertes par les différents hôtes de réseau étendu, disposer de systèmes d'adressage de ces ressources (fichiers, applications, etc.). Pour respecter le caractère ouvert du modèle, ces systèmes doivent indépendants de toute technologie et de tout système d'exploitation. D'autre part, ils nécessitent l'adjonction de mécanismes de **résolution** permettant d'établir la correspondance des adresses couche 7 avec les adresses utilisées par les couches inférieures du modèle

Le système le plus répandu, car employé par les applications web est celui des U.R.L (Uniform Ressource Locator), associé au mécanisme de résolution d'adresses D.N.S. (Domain Name Service).

ENVELOPPE COUCHE 7:

On trouvera dans cette enveloppe:

- Les information permettant d'identifier le type de l'application émettrice du message.
- L'adresse couche 7 de la ressource destinataire.
- Etc.

III.2.5 MODELE O.S.I. ET PROTOCOLES DE COMMUNICATION:

III.2.5.1 DEFINITION:

Dans le domaine informatique, un protocole de communication définit un langage permettant d'établir et d'entretenir la communication entre deux entités matérielles ou logicielles. Un protocole est composé:

- D'un ensemble de règles permettant d'organiser les informations élémentaires en messages cohérents et reconnaissables par le destinataire.
- De procédures assurant la synchronisation entre expéditeur et destinataire.
- De procédures assurant la sécurité et l'intégrité de la transmission de l'information.

De plus, un protocole prend souvent en charge la gestion des anomalies et dysfonctionnements (pannes de materiel, perte d'information, etc...).

III.2.5.2 DIFFERENTS TYPES DE PROTOCOLES:

Il existe 2 grandes familles de protocoles de communication:

Les protocoles ouverts ou publics: Ce sont les protocoles qui correspondent aux normes internationales (OSI, INTERNET, X25,etc..). Ces protocoles s'appliquent à des architectures composites, et permettent la communication entre systèmes de type différent.

Les protocoles fermés ou privés: Ils correspondent à des réseaux destinés à relier les matériels d'un même constructeur, dans le cadre d'une architecture "propriétaire": SNA(IBM), DEC net (Digital), Appletalk (Apple), etc....

III.2.5.3 COUCHES DE L'OSI ET PROTOCOLES DE COMMUNICATION:

Dans le modèle O.S.I. chaque couche décrit et normalise le dialogue entre elle-même et la couche homologue de l'hôte avec lequel elle veut communiquer. On peut donc dire que chaque couche spécifie une catégorie de protocole de communication à son niveau. On aura ainsi:

- Au niveau de la couche 1: des protocoles de codage électriques (codage Manchester, NRZ, etc)
- Au niveau de la sous-couche MAC: des protocoles d'accès au média (CSMA-CD, etc.)
- Au niveau de la sous-couche LLC: des protocoles de liaison de données (HDLC, BSC, etc.)
- Etc...
- Au niveau de la couche 7, des protocoles de dialogue entre processus applicatifs (HTTP, FTP, SNMP, etc.)

Les unités de communication des protocoles de niveau élevé se trouvent en quelque sorte «emboîtées» dans celles des protocoles de plus bas niveau. Il y a donc «emboîtement» de protocoles, comme il y a empilement de couches.

III.2.6 RESUME:

Le tableau de la page suivante résume les fonctionnalités des sept couches du modèle O.S.I:

MODELE O.S.I. = Open Systems Interconnexion	
COUCHE	**ACTIVITE**
7-APPLICATION	**Point d'accès au réseau pour les processus utilisateurs:** Apporte à l'utilisateur les services de base offerts par le réseau: • Accès au web • Transfert de fichiers • Messagerie • etc.
6-PRESENTATION	**Traite l'information de manière à la rendre compatible entre tâches communicantes:** • Conversion, reformatage, cryptage-décriptage, compression-décompression. • Assure l'indépendance entre l'utilisateur et le transport de l'information.
5-SESSION	**Organise et synchronise les échanges entre tâches distantes:** • Etablit liaison entre programmes d'application distants, commande leur dialogue (qui doit parler, qui parle...) • Insére des points de reprise dans le flot de données de manière à pouvoir reprendre le dialogue après une panne.
4.TRANSPORT	**Assure le bon acheminement des messages complets au destinataire.** • Etablit et gère une communication de **PORT ÉMETTEUR** à **PORT RÉCEPTEUR**. • Gère les **connexions et déconnexions** (T.C.P) • Contrôle le flux**.** • Découpage en paquets (émission - TCT) • Réasseblage dans le bon ordre (réception - TCP)
3.RESEAU	**Assure le routage des paquets sur le sous-réseau local et vers les réseaux interconnectés.** • Etablit et gère une communication de l'**ADRESSE IP** de l'émetteur vers l'**ADRESSE IP** du récepteur. • Encapsule le mécanisme de routage et de calcul des tables de routage (tables statiques ou dynamiques...). • Contrôle également les problèmes d'engorgement du sous-réseau.
2.LIAISON	**Etablit des liaisons de données entre la machine locale et les autres machines connectées au médium physique.** **Sous-couche: Logical Link Contrôl (LLC):** ***<u>En Réception:</u>*** • Découpe le flux de bits en **TRAME** (par détection des bits d'en-tête et de fin de trame). • Détecte les erreurs de transmission et gère l'envoi d'un C.R. de réception à l'émetteur ***<u>En émission:</u>*** • Transforme les messages de la couche réseau en «trames» pouvant être émises sur le média • Elabore des données de contrôle et les inclue dans les trames. • Traite les C.R. Du récepteur et réémet les trames que le récepteur a signalé en erreur. **Sous-couche: Medium accès Contrôl (MAC):** • Etablit et gère une communication entre deux ADRESSES PHYSIQUES (Adresses MAC). • Prend en charge la **méthode d'accès** au média.
1.PHYSIQUE	***Transmet des signaux (électriques, optiques) codant des configurations binaires, de façon brute sur un canal de communication. Contrôle la transmission des données sur le média. Elle normalise:*** • Les caractéristiques électriques. • Les caractéristiques mécaniques (connecteurs, topologie...) • Les mécanismes de transmission et procédures d'établissement, de maintien et de libération du circuit de données.

IV TECHNOLOGIE DES RESEAUX:

IV.1 GENERALITES:

IV.1.1 DIFFERENTS TYPES DE RESEAUX:

Le problème de la communication sur un réseau est d'abord lié à la nécessite d'établir et de maintenir la **connexion** entre les 2 hôtes dialoguants, pendant la durée de l'échange. Ceci peut être réalisé de 3 manières différentes:

IV.1.1.1 RESEAUX A COMMUTATION DE CIRCUITS:

***Exemple**: Réseau téléphonique classique*

Lorsque deux hôtes communiquent sur un réseau à commutation de circuit, un **Circuit Physique** est établi entre les 2 hôtes, pendant toute la durée de la communication. La connexion est dite **dédiée**: le circuit physique ne peut être utilisé par personne d'autre, jusqu'à la déconnexion. Ce type de connexion se caractérise par trois phases de fonctionnement: la **Connexion**, le **Transfer** (d'informations) et la **Déconnexion**.

IV.1.1.2 RESEAUX A COMMUTATION DE MESSAGES:

***Exemples**: Courrier, télégrammes.*

Dans ce type de réseau, l'équipement physique de communication est partagée temporellement entre les différents utilisateur. L'information est découpée en messages indépendants, chacun de ceux-ci possédant toutes les informations de routage nécessaires à leur acheminement.

La commutation de l'information se fait donc au niveau du message et non du circuit. Aucune connexion entre émetteur et récepteur n'est nécéssaire. Contrairement aux réseaux à commutation de circuits, la connexion physique entre hôtes est toujours établie.

Les messages des différents utilisateurs circulent en série sur le média (**multiplexage temporel)**.

REMARQUE:

Pour que le multiplexage ait un bon rendement il est nécessaire que les messages soient **relativement courts.**

IV.1.1.3 RESEAUX A COMMUTATION DE PAQUETS:

***Exemples**: Transpac, X25, TCP*

Pour transmettre des messages longs tout en conservant les avantages de la commutation de messages, une solution consiste à fragmenter les messages en **Paquets** dont la longueur peut être optimisée en fonction des exigences du réseau. Chaque paquet est commuté indépendamment par le réseau. Il doit donc contenir toutes les informations relatives à son routage et au ré-assemblage des fragments.

Notons que la taille d'un paquet peut atteindre 65536 octets. Le transfer d'une telle quantité d'information occupe un média courant (débit voisin de 100 Mbits) pendant 6 à 8 ms, ce qui est loin d'être négligeable.

Commutation de paquets avec établissement de circuits virtuels:

Dans ce cas, une "connexion logique" est établie avant l'envoi des paquets. Ceci signifie que tous les paquets suivent le même circuit virtuel, et arrivent dans le bon ordre. Le réassemblage du message total est donc garanti. Cette connexion logique implique un mécanisme d'acquittement (**ACK**) de la part du récepteur, de façon à contrôler l'envoi des paquets.

Commutation de paquets sans établissement de circuits virtuels (Datagram):

Dans ce cas, le réseau traite chaque paquet indépendamment. De ce fait, l'ordre d'arrivée n'est plus garanti, le trajet (routage) pouvant différer pour chaque paquet. Le réassemblage du message total est donc à la charge de l'application utilisatrice.

IV.1.1.4 RESEAUX A COMMUTATION DE CELLULES:

***Exemples**: A.T.M.*

La commutation de cellules (appelée aussi «commutation de labels») consiste à fragmenter les messages en **cellules** qui, à la différence des paquets, sont de longueur fixe et de faible taille (53 octets dans la solution A.T.M). Dans ce type de solution, une connexion logique est établie avec établissement de circuits virtuels. Toutes les cellules d'un même message suivent le même circuit virtuel. Les équipements physiques de communication sont multiplexés temporellement entre les différents utilisateur.

L'avantage de la commutation de cellules par rapport à la commutation de paquets est qu'associée à une architecture de réseau basée sur des «étoiles actives» munies de commutateurs évolués (voir plus loin ces notions), elle permet d'assurer un certain déterminisme temporel en ce qui concerne la durée d'acheminement des informations.

IV.1.2 TOPOLOGIE DES RESEAUX:

IV.1.2.1 TOPOLOGIE EN BUS:

Dans une topologie «en bus», chaque station est branchée en dérivation par rapport au média commun. Les informations émises par une station sont diffusées à toutes les autres. La station destinataire doit acquérir au passage les messages qui la concernent. Cette topologie la plus utilisée, essentiellement car elle est à la base de la solution ETHERNET:

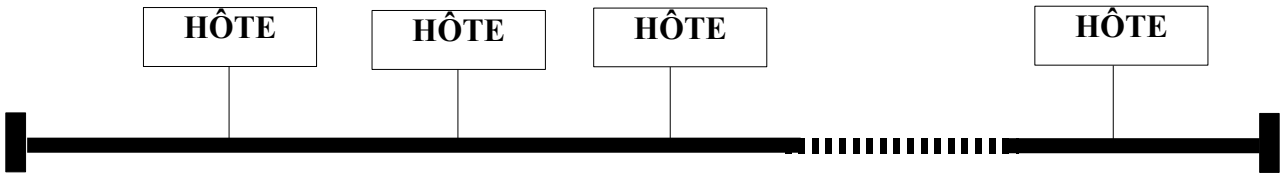


Schéma n° VI : topologie en BUS

Le média peut être constitué d'une paire torsadée ou d'un câble coaxial. La gestion du réseau n'est pas centralisée (toutes les stations jouent le même rôle).

AVANTAGES:

Le BUS peut être entièrement passif: pour les petites configurations (pour ETHERNET, 100 stations au maximum sur 500 m), aucun composant electronique actif n'est nécessaire. Pour les installations plus importantes, les tronçons (<= 500 m) doivent être reliés par des répéteurs actifs qui régénèrent les signaux.

INCONVENIENTS:

En cas de rupture du média, il est pratiquement impossible de reconfigurer dynamiquement le réseau. Il y a donc interruption totale du service jusqu'à réparation du matériel.

IV.1.2.2 TOPOLOGIE EN ANNEAU:

Dans une topologie en anneau, chaque station est branchée en série sur le média commun:

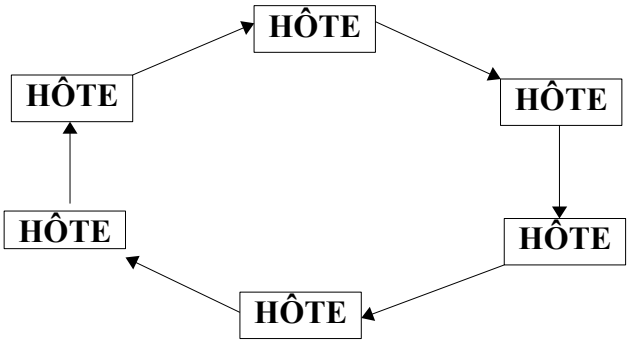


Schéma n° VII-Topologie en anneau

Dans un anneau, la circulation de l'information est unidirectionnelle. Comme dans le cas du BUS, le contrôle du réseau est décentralisé: il n'y a pas de station spécialement dédiée à la gestion du l'anneau.

AVANTAGES:

Cette topologie présente l'intérêt de permettre l'utilisation de n'importe quel type de support entre deux hôtes (paire torsadée, câble coaxial, fibre optique), chaque couple d'hôtes pouvant avoir une solution différente.

INCONVENIENTS:

La défaillance d'une station (au moins pour les organes de répétition du message) entraîne la défaillance totale du réseau. Pour sécuriser le réseau, on place au niveau de chaque connexion un court-circuit pour pallier le cas d'une station défaillante. Dans certaines solutions (FDDI), l'anneau est doublé, ce qui permet de pallier la défaillance d'un tronçon de communication.

IV.1.2.3 RESEAUX EN BOUCLES:

Leur topologie est identique à celle des réseaux en anneau. La différence réside dans la présence d'une station SUPERVISEUR qui contrôle le bon fonctionnement de la méthode d'accès au réseau.

IV.1.2.4 TOPOLOGIE EN ETOILE:

Dans cette topologie, les stations sont toutes reliées à commutateur qui assure la communication entre stations.

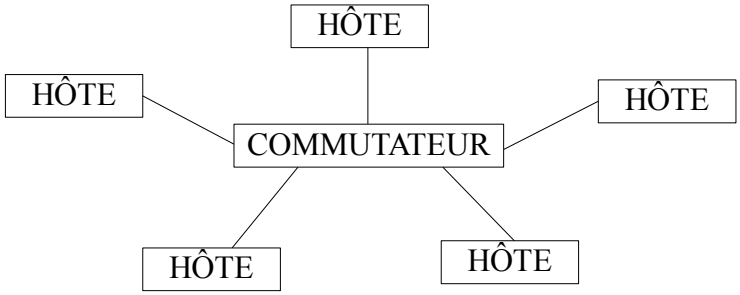


Schéma n° VIII-Topologie en étoile

RESEAU EN ETOILE ACTIVE:

Le commutateur est un composant actif et complexe qui assure la gestion centralisée du réseau.

Exemple: les Private Automatic Band eXchange (PABX). Un PABX est un réseau privé destiné à relier les postes téléphoniques d'une implantation locale entre eux (lignes internes) et avec le réseau téléphonique public (lignes externes).

RESEAU EN ETOILE PASSIVE:

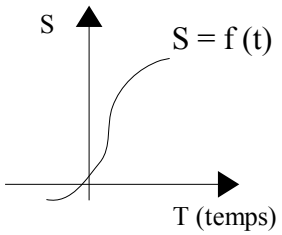
Dans ce cas, le commutateur est un simple répéteur qui transmet les message reçus sur l'ensemble des autres lignes.

IV.1.3 TRANSMISSION DU SIGNAL:

IV.1.3.1 NOTION DE SIGNAL:

DEFINITION:

On appelle SIGNAL la variation dans le temps d'une grandeur physique quand cette variation est **porteuse d'une information** (ou encore **représentative** d'une information). On peut donc représenter un signal comme une fonction du temps: S = f(t) où S représente l'amplitude du signal:

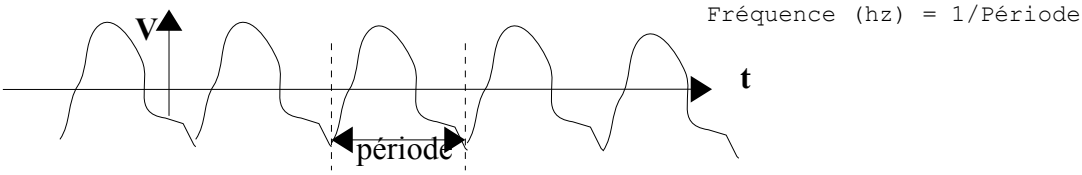


Dans le domaine de l'informatique et des télécommunications, les signaux sont essentiellement de 3 sortes:

- Les signaux électriques: variation de tension en fonction du temps dans un conducteur.
- Les signaux optiques: variation d'intensité lumineuse en fonction du temps dans une fibre optiques.
- Les signaux hertziens: propagation d'une onde électromagnétique dans l'espace (ex: faisceau hertzien, wifi)

SIGNAL PERIODIQUE-FREQUENCE ET PERIODE:

Signal périodique: C'est un signal qui se répète régulièrement dans le temps:



Exemple: *courant alternatif à 50 hz => 50 hertz correspondent à une période de 1/50 s = 20 ms)*

BANDE PASSANTE:

Pour un circuit donné, les fréquences transmissibles sont comprises entre une limite minimale et une limite maximale. La plage des valeurs des fréquences transmissibles ainsi délimitée est la **BANDE PASSANTE** du circuit. Elle dépend de la technologie et de la structure de ce circuit.

La **LARGEUR DE BANDE** est la différence (en hertz) entre fréquence basse et fréquence haute.

EXEMPLE:

Le réseau téléphonique est prévu pour transmettre les fréquences de 300 hz à 3400 hz. Sa **BANDE PASSANTE** est donc de : 3400 – 300 = 3100 hz.

IV.1.3.2 SIGNAUX NUMERIQUES ET ANALOGIQUES:

La représentation d'une grandeur physique par un signal est dite **ANALOGIQUE** quand l'amplitude du signal à un instant donné est proportionnelle à la valeur courante de la grandeur physique représentée.

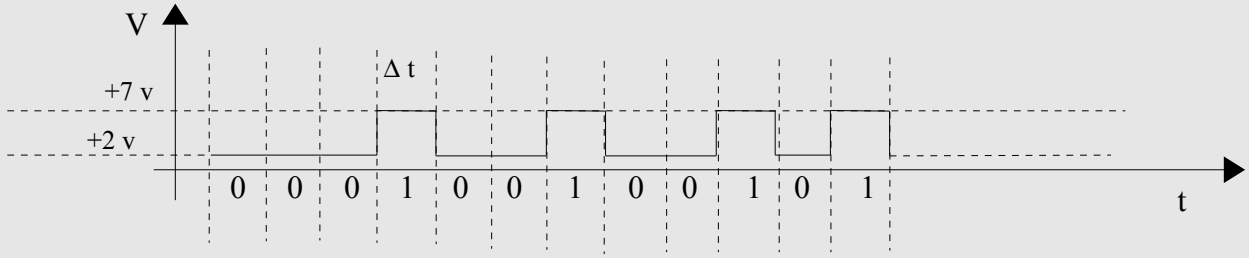
EXEMPLE:

*La température mesurée par un capteur est transmise à un système de traitement sous la forme d'un signal électrique dont l'amplitude est égale à 0,01 volt par degrés Kelvin (ainsi, pour une mesure de 293 degrès Kelvin, le signal aura une amplitude de 293*0,01 = 2,93 volts. Cette représentation est dite ANALOGIQUE.*

La représentation d'une grandeur physique par un signal est dit **NUMERIQUE** quand les variations d'amplitude du signal sont codées sous forme de nombres représentatifs des valeurs successives de cette grandeur physique, échantillonnées à des instants donnés. En pratique, ces valeurs numériques sont codées sous forme de train d'impulsions représentatives de la configuration binaire du nombre. Chaque impulsion binaire occupe un intervalle de temps fixe et code un bit de la valeur binaire:

EXEMPLE:

Les valeurs successives d'une température mesurée par un capteur sont transmises toutes les secondes à un système de traitement sous la forme d'impulsions électriques représentant les valeurs binaires successives de cette température, avec un quantum de 1 degrès Kelvin. Ainsi, la valeur 293 degrès Kelvin, mesurée à l'instant T sera transmise sous la forme d'une trame codant sur 12 bits le nombre binaire 0001 0010 0101 (soit 293 en base 2). Cette représentation est dite NUMERIQUE (BINAIRE). Une représentation possible du signal est la suivante:



Schema n° IX-Signal numérique codé en binaire

REMARQUE:

L'exemple représente un type de codage pour lequel le temps est découpé en intervalles de durée Δt. Un bit à 0 est représenté par une tension à 2 volts, maintenue pendant un intervalle de temps Δt, un bit à 1 par une tension à 7 volts maintenue pendant le même espace de temps.

IV.1.3.3 CARACTERISTIQUES DES SIGNAUX NUMERIQUES BINAIRES:

CADENCE DE TRANSMISSION:

La bande passante d'un circuit pour un signal numérique est le nombre maximum de **transitions** du signal par seconde qu'il lui est possible de transmettre. Elle s'exprime en BAUDS (d'après le nom d'Emile BAUDOT, inventeur du code Baudot, utilisé pour la télégraphie). Remarquons que, suivant le codage binaire adopté, le nombre de bauds peut être différent du nombre de bits par secondes: ainsi, dans le schéma ci-dessus, la valeur de 12 bits est codée avec 8 transitions du signal.

DEBIT:

C'est le nombre maximum de bits pouvant être transmis en une secondes (exprimé en bits/seconde). Comme l'illustre le schéma n° IX, la durée Δt de transmission de la valeur d'un bit détermine le débit:

Debit = 1 /Δt bits par secondes

EXEMPLE:

pour obtenir un débit de 5 mégabits par seconde, il faut que $5*10^6 = 1/\Delta t$. La durée de transmission d'un bit sera donc de:

$$\Delta t = 1/(5*10^6) = 0,2* 10^{-6} \text{ secondes}$$
soit: 0,2 microsecondes

RELATION ENTRE DEBIT ET CADENCE DE MODULATION:

THEOREME DE SHANNON:

La cadence de transmission maximale d'une ligne est toujours inférieure ou égale au double de sa largeur de bande.

REMARQUE:

Formule mathématique exacte: $D <= 2 * B* \text{Log}_2 (n)$

Avec:

- D = Débit (bits/seconde)
- B = Largeur de bande passante
- n = Valence du signal (nombre d'états possibles du signal)

Pour un signal binaire, n = 2, et comme $\text{Log}_2(2) = 1$, on a: $D <= 2 * B$

Ceci revient à dire que le débit maximum d'une ligne transmettant un signal binaire est égal à sa cadence de transmission et inférieur au double de sa largeur de bande.

IV.2 TECHNOLOGIES DE LA COUCHE PHYSIQUE:

IV.2.1 INTRODUCTION:

Nous avons vu précédemment que la couche physique assure la transmission des signaux (électriques, optiques, électromagnétiques) sur le média. De ce fait, les normes attachées à cette couche concernent:

- D'une part la technologie des médias
- D'autre part, les protocoles de transmission des signaux sur le média

IV.2.2 LES MEDIAS PHYSIQUES:

IV.2.2.1 DIFFERENTS TYPES DE MEDIAS PHYSIQUES:

Actuellement, les médias physiques couramment utilises pour la construction des réseaux sont de 4 types:

- Le câble coaxial.
- La paire torsadée.
- La fibre optique
- Les liaisons sans fils (ondes électromagnétiques ou infra-rouges)

IV.2.2.2 CABLES COAXIAUX:

MEDIA:

Les câbles coaxiaux sont constitués d'une âme conductrice, entourée d'un isolant, lui-meme entouré d'un treillis métallique (blindage). Le tout est entouré d'une enveloppe en matière plastique:

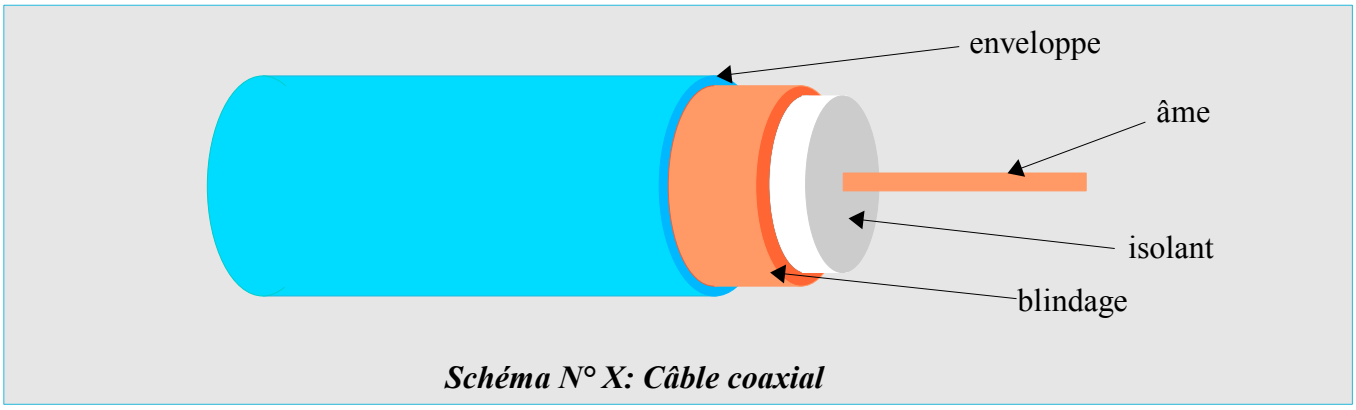


Schéma N° X: Câble coaxial

Les câbles coaxiaux utilisés pour la connectique réseau ont une impédence de 50 ohms. Ils existent en deux modèles:

- 10Base2 (ou ***thinnet***): D'une épaisseur de 6 mm, ils permettent de transporter sans affaiblissement notable un signal en bande de base sur 185 m au maximum.
- 10Base5 (ou ***thicknet***): D'une épaisseur de 12 mm, ils permettent de transporter sans affaiblissement notable un signal en bande de base sur 500 m au maximum.

CONNECTIQUE:

Les liaisons par câbles coaxiaux utilisent des connecteurs B.N.C (connecteurs ronds, mâles et femelles), vissables sur 1/4 de tour. Le schéma suivant décrit les différents connecteurs existants.

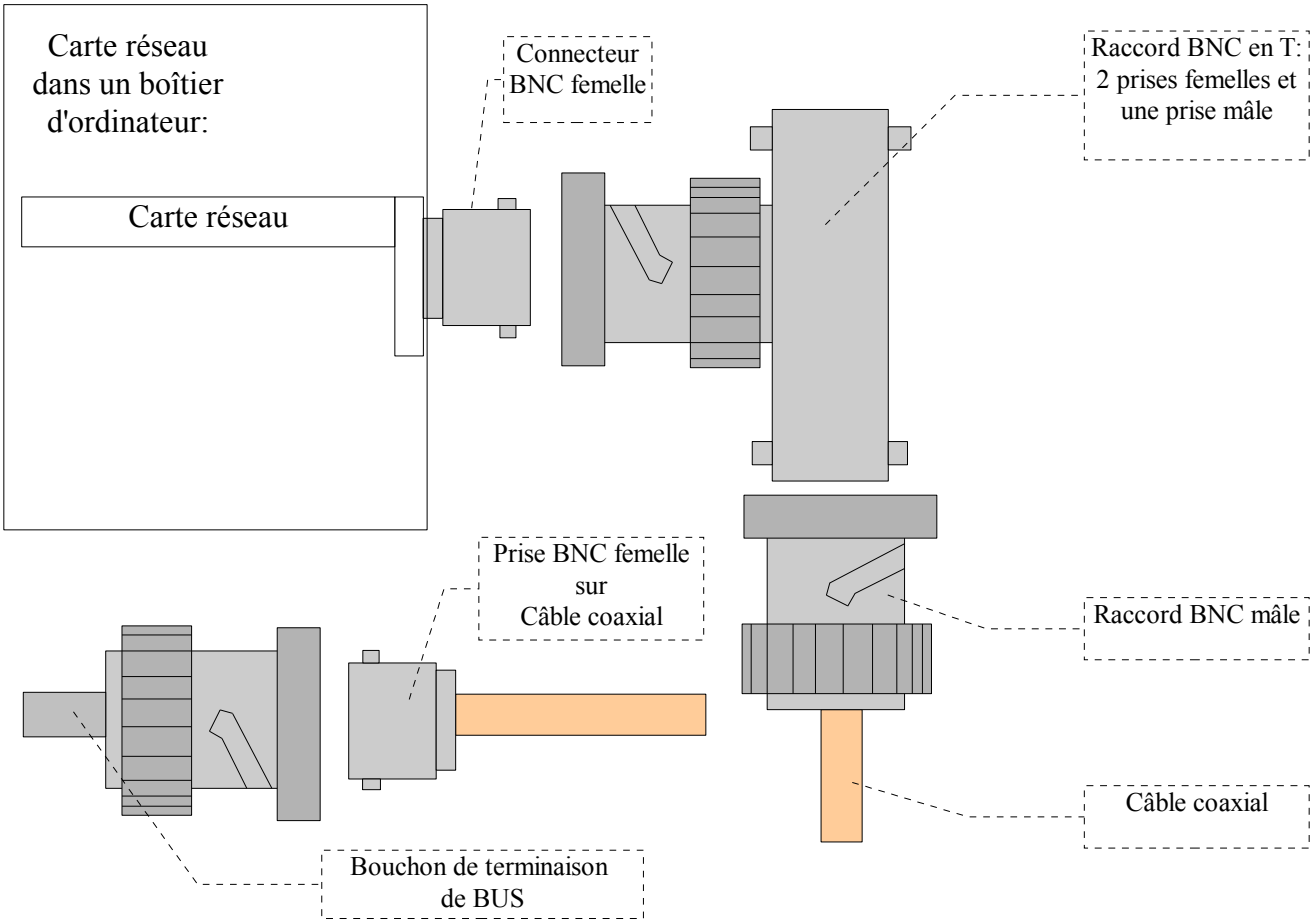


Schéma N° XI: Composants B.N.C d'interconnexion

PERFORMANCES ET UTILISATION:

Le câble coaxial, du fait de son blindage lui assurant une bonne protection contre le rayonnement et les pertes en ligne, permet la transmission de débits élevés sur des distances importantes. Il est, d'autre part, facile à installer: il permet de créer rapidement des topologies en BUS, sans aucun composant d'interconnexion, grâce à ses raccords en T qui se connectent directement sur les cartes réseau (c'est même la seule solution qui permet de réaliser physiquement cette topologie). Cependant, le coût élevé des composants de base contribue actuellement à le cantonner à des installations très simples, à débit inférieur à 10 Mbits et à faible nombre d'hôtes:

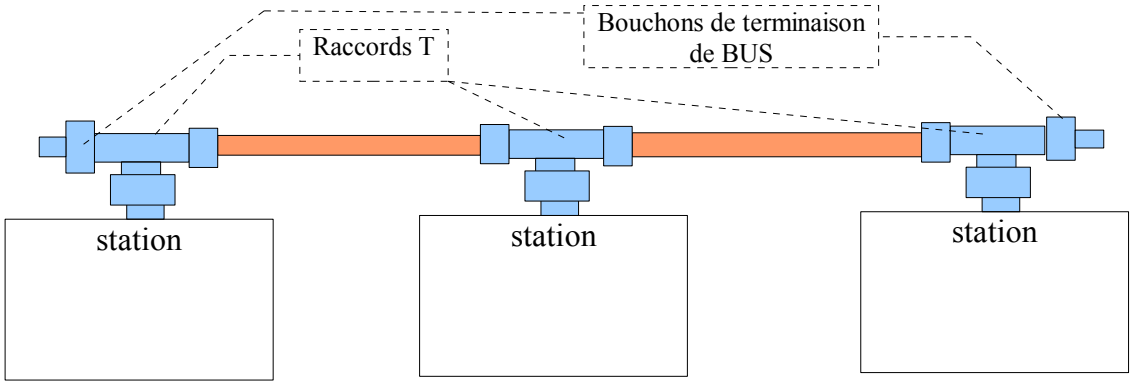


Schéma n° XII: Topologie en B.U.S avec liaison par coaxiaux et connecteurs BNC

IV.2.2.3 PAIRE TORSADEE:

MEDIA:

Une paire torsadée est constituée de deux conducteurs isolés enroulés l'un sur l'autre. En général, les câbles de cette technologie contiennent quatre paires. La technique du torsadage a deux avantages:

- D'une part, ell permet de diminuer le phénomène de **diaphonie**. En effet, les deux brins de la paire transportent le même signal. En un point donné de la torsade, les deux conducteurs forment des spires de sens différent. De ce fait, les champs magnétiques créés par les deux courants dans l'espace environnant, étant d'intensité égale mais de sens différent ont tendance à s'annuler.
- D'autre part, elle tend à maintenir une distance constante entre les conducteurs d'une même paire, ce qui permet de garantir l'impédence caractéristique de cette paire (autour de 100 ohms).

Actuellement, les câbles à paires torsadées utilisés dans le domaine des réseaux sont tous équipés de blindages plus ou moins sophistiqués (simple écran en feuille d'aluminium commun à toutes les paires, blindage de chaque paire, combinaison des deux...). Ces solutions ont permis de se rapprocher des performances du câble coaxial dans les domaines de la perte en ligne et de la résistance au parasitage.

CONNECTIQUE:

Les paires torsadées sont associées en général aux connecteurs de type RJ45. Ceux-ci sont de loin les plus courants dans l'informatique grand public. Ce type de connectique ne permet pas de constituer des topologies en BUS. Les réseaux à paires torsadées sont donc en général des étoiles (passives ou actives). Il est également possible de relier deux machines entre elles par un câble RJ45 croisé, de façon à mettre uniquement deux postes en réseau.

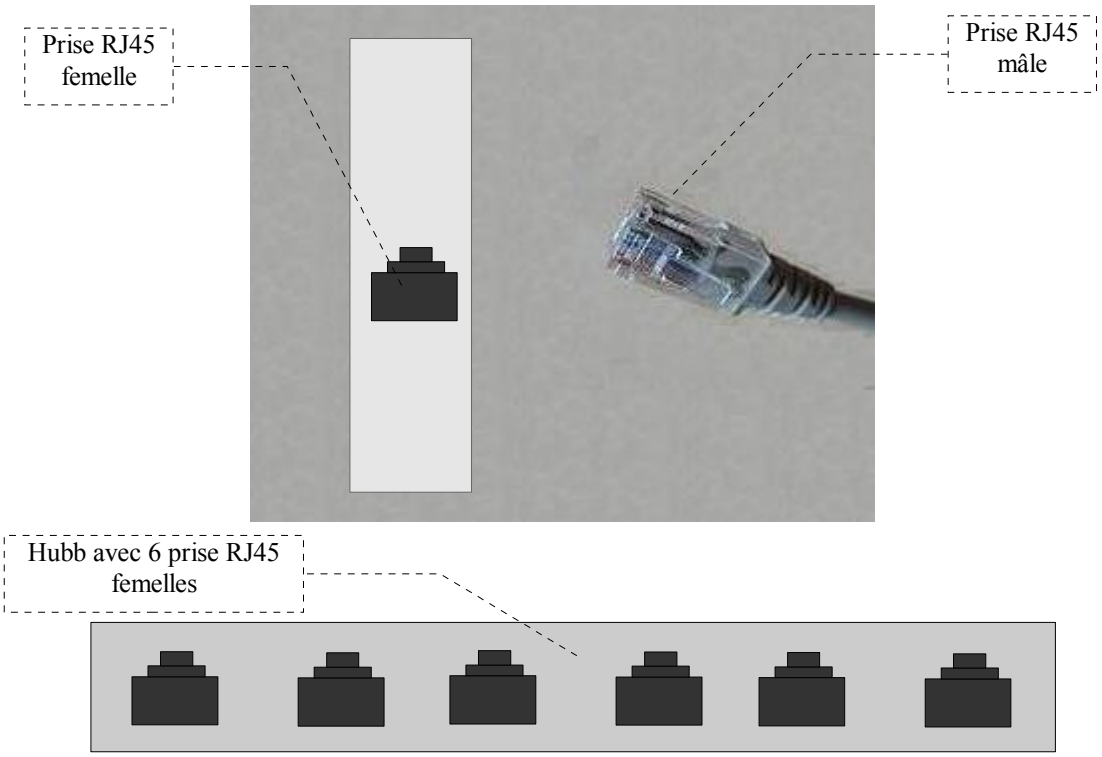


Schéma n° XII: Prises RJ45 et Hubb pour réseau en étoile

PERFORMANCES ET UTILISATION:

La paire torsadée permet actuellement des débits de l'ordre de 100 Mbits dans les solutions standart (fast-ethernet), et de l'ordre du gigabit dans des solutions plus sophistiquées (ethernet gigabits). Les performances de ce type de média, alliées à un coût peu élevé et à un câblage aisé et «propre» en font la solution de loin la plus répandue pour les L.A.N.

IV.2.2.4 FIBRE OPTIQUE:

MEDIA:

La fibre optique est un dispositif permettant de guider des ondes lumineuses (sous la forme de faisceaux lumineux très fins) à l'intérieur d'un brin de verre ou de silicium. Une fibre optique est constitué d'une âme recouverte d'une gaine. Les deux couches sont constituées de verre ou de silicium très pur. L'indice de réfraction de l'âme est choisi légèrement plus élevé que celui de la gaine:

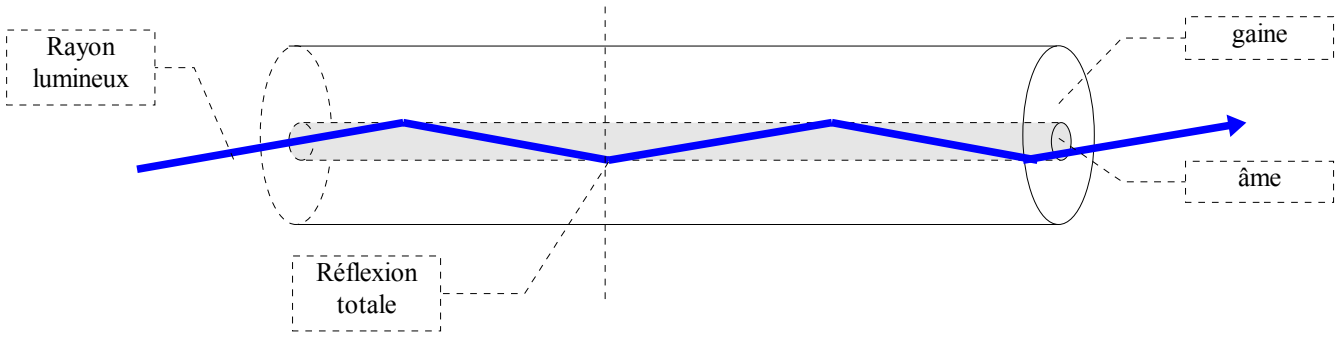


Schéma N° XIII: Fibre optique

Les rayons lumineux, injectés dans l'âme avec une incidence très faible par rapport à son axe, arrivent au contact de la séparation âme-graine avec une incidence également très faible. Du fait de la différence d'indice entre les deux milieux et de la faible incidence, le rayon ne peut pénètrer dans la gaine: il subit au contraire le phénomène de **réflexion totale** qui renvoie le rayon dans l'âme avec un angle de réflexion égal à son angle d'incidence. Le rayon se propage ainsi de réflexion en réflexion dans l'âme de la fibre, avec des pertes très faibles.

Il existe deux types de fibres: les fibres **multimode** et les fibres **monomode**. On appelle **mode** un trajet lumineux donné à l'intérieur de l'âme:

- Les fibres multimode ont une âme relativement épaisse (50 à 100 microns de diamètre). De ce fait, la lumière peut suivre plusieurs trajets (modes) à l'intérieur de la fibre.
- En revanche, les fibres monomodes ont un diamètre de 10 microns, proche de la longueur d'onde de la lumière. De ce fait, le rayon ne peut suivre qu'un seul trajet, pratiquement sans aucune réfraction.

Dans la catégorie des fibres multimode, certaines sont dites «à saut d'indice», car la variation de l'indice entre âme et gaine est brutale. Dans d'autres fibres, l'indice de réfraction entre âme et gaine varie progressivement (fibres à gradiant d'indice). Dans une fibre à gradiant d'indice, le nombre de modes est plus faible que dans une fibre à saut d'indice.

CONNECTIQUE:

- En entrée de la fibre, la transformation du signal électrique en signal optique est assurée par un équipement appelé **transceiver**.
- Dans le cas d'une fibre multimode, le transceiver utilise une **diode électro-luminescente** (En anglais: L.E.D-Light Emitting Diode). Une LED est un composant qui émet une lumière dont l'intensité est fonction du courant qui le traverse.
- Les fibres monomode exigent quant à elles l'utilisation d'une **diode à injection laser** (En anglais I.L.D-Injection Laser Diode), analogue à celles qui sont utilisées dans les lecteurs optiques (CD, DVD).
- En sortie de la fibre, la lumière est re-transformée en signal électrique et adaptée au récepteur par un équipement appelé **détecteur**. La transformation de la lumière en signal électrique est assurée par un composant appelé diode photo-sensible,

encore appelée **photo-diode** (Il existe également des photo-diode avalanche qui fournissent un courant de détection plus élevé).

PERFORMANCES ET UTILISATION:

La fibre optique a pour avantages d'être insensible au rayonnement électromagnétique, d'avoir une durée de vie très élevée (de l'ordre de 20 ans), de permettre des débits très importants avec des pertes très faibles (surtout en monomode). De plus, du fait de l'inexistance du phénomène de diaphonie, un câble optique peut contenir un nombre de fibres beaucoup plus important qu'un câble électrique.

La fibre optique a pour inconvénient son coût relativement élevé. Elle est également plus difficile à installer que la paire torsadée ou le coaxial.

Fibre multimode à saut d'indice:

- Débit: 50 Mégabits.
- Distances: quelques centaines de mètres
- Coût: assez élevé, par rapport à la paire torsadée
- Utilisation: réseaux locaux.

Fibre multimode à gradiant d'indice:

- Débit: 1 Gigabit.
- Distances: quelques kilomètres
- Coût: un peu plus élevé que la fibre à saut d'indice.
- Utilisation: réseaux locaux, réseaux de télécom.

Fibre monomode:

- Débit: 1O Gigabits en standard (mais des essais ont été réussis avec des débits beaucoup plus élevés).
- Distances: Des centaines de kilomètres
- Coût: élevé.
- Utilisation: grands réseaux de télécom, «backbones», câbles sous-marins trans-continentaux, etc...

NOTA:

Quand la fibre décrit une courbe, l'angle d'incidence du rayon par rapport à la surface de l'âme peut se trouver augmenté. Si la courbure est suffisante, cet angle d'incidence ne permet plus la réflexion totale. Il y a alors **réfraction** d'une partie du faisceau dans la gaine, ce qui occasionne la perte du signal. Les fibres optiques sont donc soumises à des contraintes de courbure maximale qui les rendent moins faciles à installer que les paires torsadées.

IV.2.2.5 LIAISON SANS FIL:

MEDIA:

Les média des liaisons sans fil (liaisons WiFi) sont les ondes hertziennes de fréquence 2,4 Giga-hertz (fréquences proches de celles qui sont utilisées par les fours micro-ondes).

CONNECTIQUE:

Les ordinateurs portables intègrent en général un émetteur-récepteur WiFi. En ce qui concerne les ordinateurs de bureau (rarement équipés en natif), l'équipement de connexion est le plus souvent un composant (émetteur-récepteur) connectable sur un port USB (on l'appelle souvent de ce fait «clef WiFi»). Certains ponts routeurs (par exemple, les **-Box des différents fournisseurs d'accès internet) intègrent une liaison WiFi qui leur permet de se connecter par ce moyen à des postes locaux.

PERFORMANCES ET UTILISATION:

En principe, la fréquence utilisée pénètre peu les matériaux. D'autre part, les émissions WiFi sont calibrées à des puissances beaucoup plus faibles que celles des téléphones portables. Les liaisons WiFi se font donc surtout par réflexions successives et ne permettre par de liaisons à grande distance. Elles conviennent donc surtout pour des usages locaux.

IV.2.3 LES METHODES DE SYNCHRONISATION:

IV.2.3.1 GENERALITES:

Sur la totalité des médias utilisés pour les réseaux, la transmission des informations s'effectue **en série**. Les impulsions codant chaque bit d'information sont donc transmises **l'une après l'autre**. D'autre part, ces informations sont groupées par **trains de 8 bits** (octets).

Les impulsions codant chaque bit d'un octet sont toujours de même durée. Cette durée est fixée par **l'horloge de l'émetteur**. La fréquence de cette horloge détermine le débit maximal de l'émetteur en bits par seconde. Le récepteur doit disposer également d'impulsions d'horloge lui permettant de «découper» temporellement le signal afin d'y repérer les valeurs des bits transmis.

Les lignes de transmission de données ne peuvent prendre que deux états: l'état 1 ou l'état 0, qui correspondront chacun à deux valeurs électriques (par exemple: 0 = 0 volts, 1 = +5 volts): une ligne au repos prendra donc forcément un de ces deux états. De ce fait, sans moyen supplémentaire, il serait impossible de détecter une information binaire arrivant après un état repos si cette information correspond au même état de ligne que le repos.

D'autre part, lorsque deux valeurs binaires successives ne provoquent, du fait du codage, aucune transition de la ligne, la deuxième serait également indétectable.

Exemple:

Supposons que l'état repos d'une ligne soit 0 volt et que les valeurs binaires soient codés 0 = 0 volts, 1= +5 volts. Cette ligne, après une période de repos, reçoit l'octet 01101010 «forts poids en tête». Ceci veut dire que la première impulsion reçue sera celle qui code le bit le plus à gauche, c'est à dire 0. Cette valeur 0 étant codée par une tension nulle la distinguer de l'état de repos de la ligne. Le premier bit détectable sera le deuxième, qui provoquera le passage à +5 volts de la ligne. En l'absence d'un mécanisme de synchronisation, le premier bit serait donc perdu.

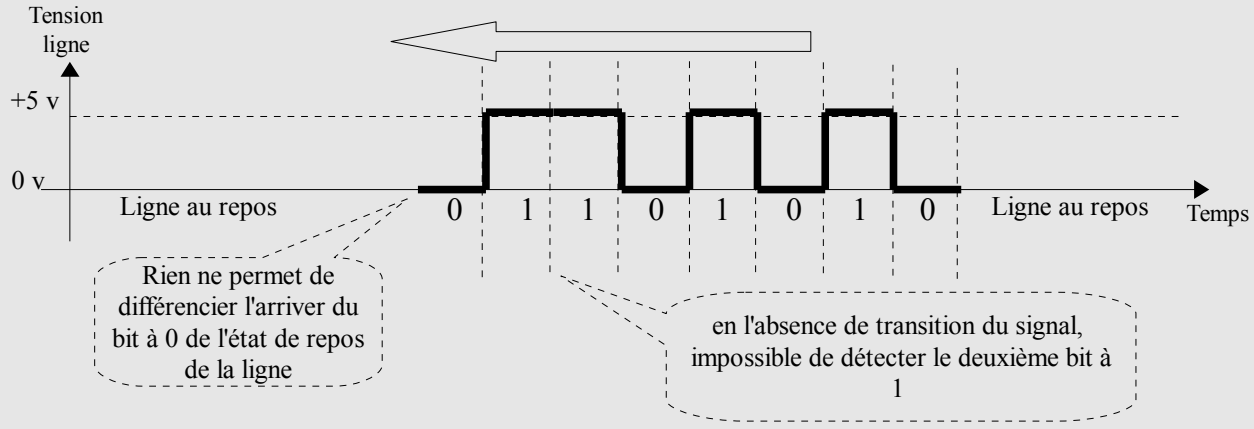


Schéma n° XIV: Impulsions binaires en série

Il est donc nécessaire de disposer de mécanismes permettant:

- D'une part de **synchroniser le début d'acquisition des états de la ligne par le récepteur avec l'arrivée des signaux**.
- D'autre part, de **repérer dans le train d'impulsions toutes les valeurs binaires**, même quand elles ne provoquent pas de transition de l'état de la ligne.

On distingue 2 méthodes de synchronisation:

- La transmission asynchrone
- La transmission synchrone.

IV.2.3.2 TRANSMISSION ASYNCHRONE:

La transmission asynchrone repose sur deux principes:

1. Le récepteur se synchronise sur chaque octet reçu (les octets composant un message peuvent de ce fait arriver d'une manière irrégulière dans le temps, d'où l'adjectif «asynchrone».
2. L'horloges du récepteur, permettant le découpage des octets en bits est indépendante de celle de l'émetteur (mais elle doit avoir la même fréquence).

Chaque octet est précédé d'un "bit start", à une valeur telle qu'il déclenche une transition du signal par rapport au niveau de repos. Ce bit permet au récepteur de détecter le début de chaque octet et de synchroniser le démarrage de son horloge de découpage. De même, chaque caractère doit être suivi d'un "signal stop", d'une largeur minimale égale à un à 2 bits. Ce signal stop ramène le niveau au repos, en vue de la détection du prochain "bit start". Les caractères transmis le sont donc d'une manière totalement asynchrone:

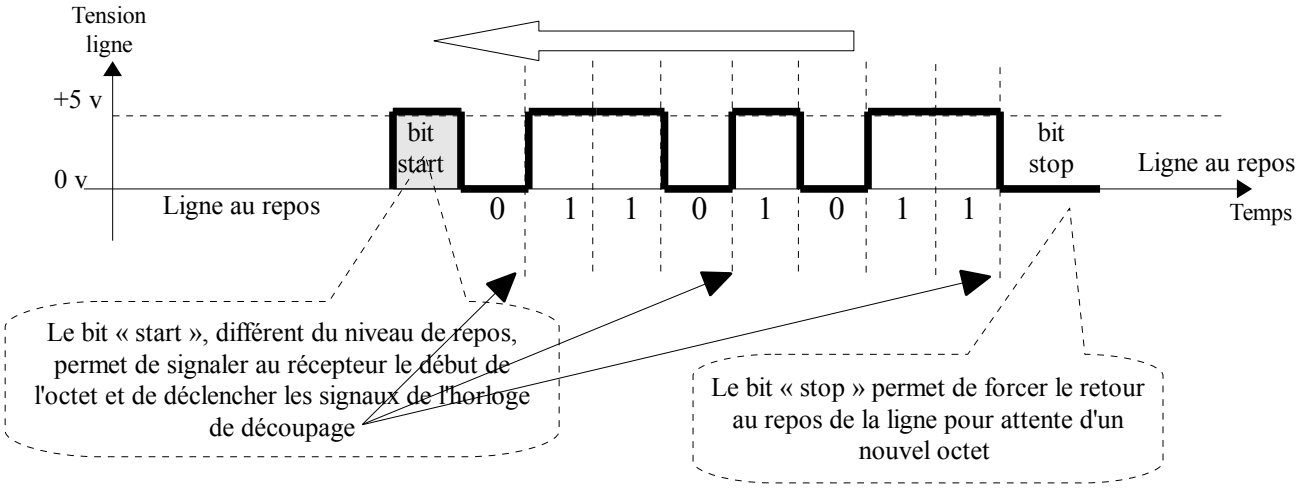


Schéma N° XV: Transmission asynchrone de l'octet 01101011

Une transmission asynchrone ne nécessite qu'une boucle de transmission, soit une paire de conducteurs.

IV.2.3.3 TRANSMISSION SYNCHRONE:

Le principe est que l'émetteur envoie au récepteur non seulement le train de bits correspondant au signal, mais aussi les impulsions d'horloge correspondantes. Ces impulsions vont permettre au récepteur de «découper» le train de bits reçu. De ce fait, des bits start et stop ne sont pas nécessaires.

Les octets d'un message sont transmis les uns à la suite des autres, sans interruption, en synchronisme avec l'horloge transmise, d'où l'appellation «synchrone».

Cette transmission va nécessiter un conducteur de plus que pour une transmission asynchrone, pour transmettre les impulsions d'horloge. Une transmission synchrone nécessite donc 3 fils.

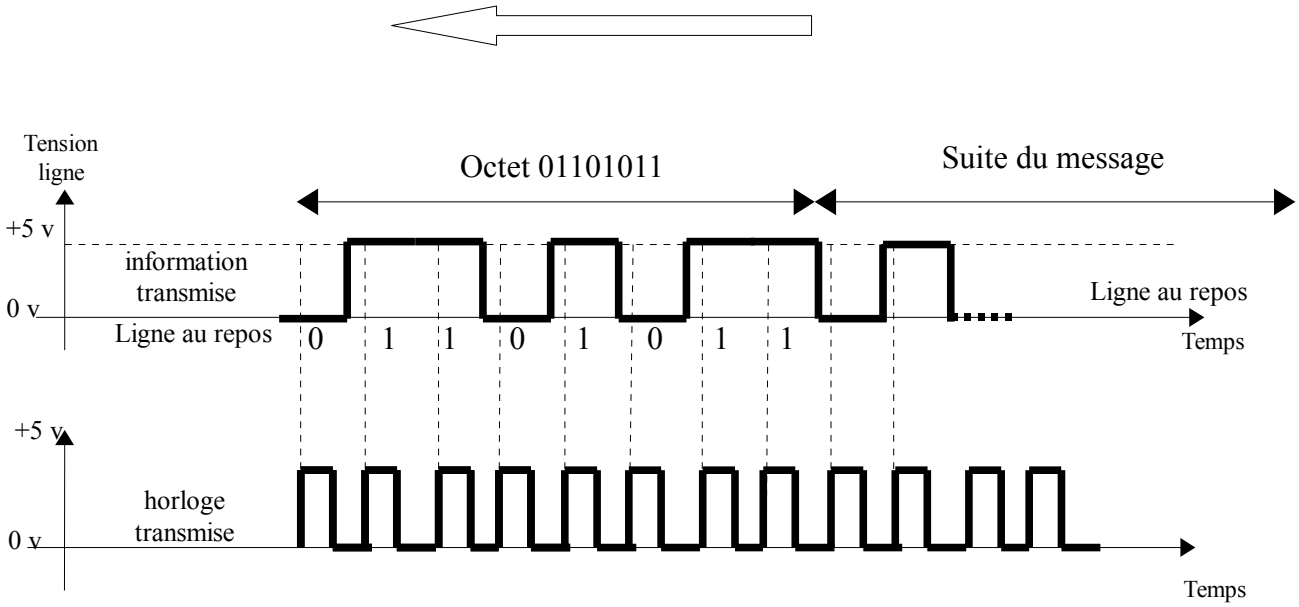


Schéma N° XVI: Transmission synchrone de l'octet 01101011

I
V.2.3.4 REMARQUE:

A débit égal, la transmission en mode synchrone est plus performante qu'en mode asynchrone. En effet, l'ajout des bits start et stop dégrade le débit réel d'une transmission asynchrone d'environ 25 %. En revanche, la transmission synchrone nécessite un conducteur de plus.

IV.2.4 LES METHODES DE CODAGE EN BANDE DE BASE :

IV.2.4.1 GENERALITES:

On dit qu'une information binaire est codée «en bande de base» lorsque la ligne ne transmet que des signaux carrés représentant directement la valeur des bits transmis. Une méthode «basique» de codage en bande de base est celle que nous avons représentée dans les schémas 14 à 16: chaque bit est représenté par le maintien du potentiel de la ligne à un niveau donné, pendant un intervalle de temps défini (par exemple, la valeur 1 est représentée par le maintien de la ligne à +5 volts pendant 100 micro-secondes, la valeur 0 est représentée par le maintien de la ligne à 0 volts pendant la même durée). Cependant, cette méthode n'est pratiquement jamais utilisée en transmission, car elle possède des inconvénients techniques. En fait, les 3 principales méthodes de codage sont:

- le codage NRZ
- Le codage MANCHESTER
- Le codage NRZI.

IV.2.4.2 CODAGE NRZ:

Le codage NRZ (no Return to Zero) consiste à utiliser 3 états de la ligne:

- La tension 0 représente l'absence de signal
- La tension +V représente la valeur 1
- La tension -V représente la valeur 0

Cette représentation est donc très proche d'un codage binaire basique:

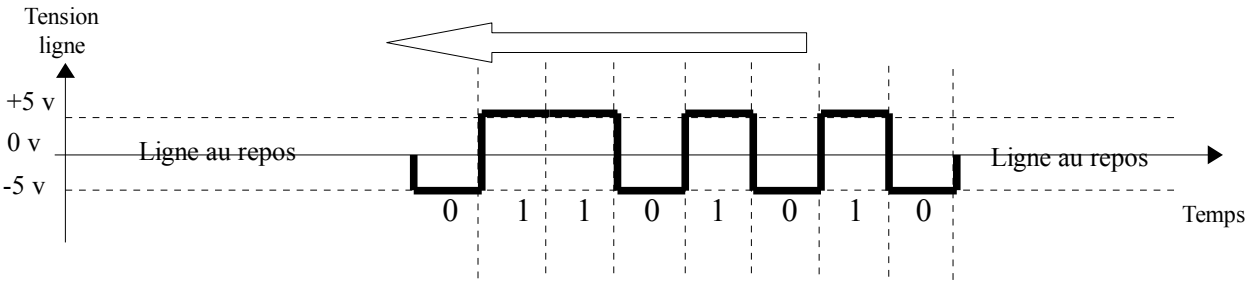


Schéma n° XVII: Codage NRZ

IV.2.4.3 METHODE DE CODAGE MANCHESTER:

Les principes en sont les suivants:

- Les bits à 1 sont représentés par une transition ascendante située au milieu de l'intervalle temporel alloué au codage du bit.
- Les bits à 0 sont représentés par une transition descendante située également au milieu de l'intervalle temporel allouée au codage du bit.
- Si la valeur du bit à coder est la même que celle du bit précédent, une transition du signal est également effectuée au début de l'intervalle temporel allouée au codage du bit.

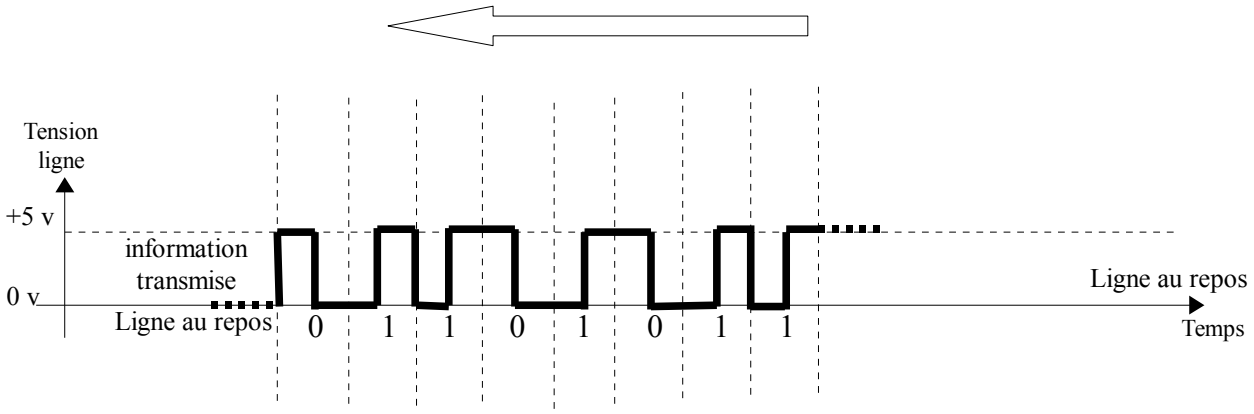


Schéma N° XVIII: Codage de l'octet 01101011 en Manchester

Le codage Manchester a l'avantage d'éviter qu'il se produise de trop longues périodes sans transition du signal: dans le cas d'une transmission synchrone, ces configurations peuvent provoquer la désynchronisation de l'horloge du récepteur.

L'inconvénient est que ce système produit jusqu'à deux transitions du signal par bit transmis. A débit égal, il consomme donc plus de bande passante qu'un codage NRZ. De ce fait, on le trouve surtout sur du câble coaxial.

IV.2.4.4 CODAGE NRZI:

NRZI est l'acronyme de: No Return To Zero Inverted. En effet, il consiste à coder les valeurs zéro par une transition et les valeurs 1 par une absence de transition.

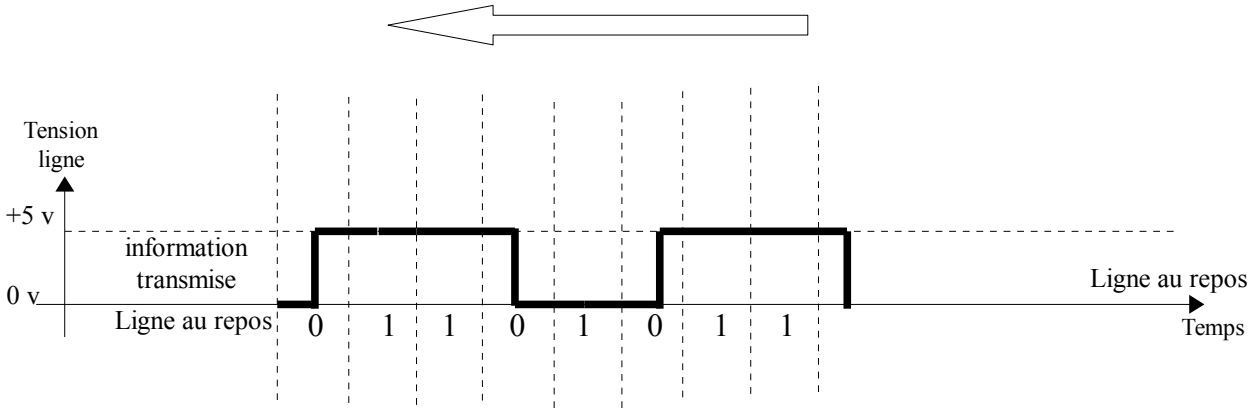


Schéma N° XIX: Codage de l'octet 01101011 en NRZI

Cette méthode minimise le nombre de transitions du signal. Elle consomme donc peu de bande passante. L'inconvénient est qu'une longue suite de valeurs à 1 se traduit par une longue période sans transition du signal.

IV.2.5 LES METHODES DE CODAGE EN LARGE BANDE (MODULATION):

IV.2.5.1 DEFINITION DE LA MODULATION:

La modulation consiste à représenter l'information binaire à transmettre par des variations du signal électrique d'une "onde porteuse". Une porteuse est une onde électrique sinusoïdale de fréquence élevée (nettement plus élevée que le débit nécessaire pour la transmission du signal représentant l'information). Ces variations (appelées «modulations») peuvent porter sur l'**amplitude**, la **fréquence** ou la **phase** de l'onde.

IV.2.5.2 AVANTAGES DE LA MODULATION:

- La modulation permet d'**augmenter la portée des transmissions**. En effet, sur la plupart des médias, les signaux à haute fréquence s'atténues moins vite que les signaux a basse fréquence.
- Seuls, les signaux de fréquence élevée peuvent donner naissance à des ondes électromagnétiques perceptibles: la modulation est donc la seule technique possible pour la **transmission sans fil** (wifi).
- La modulation permet de "**Multiplexer en Fréquences**" un média. Le multiplexage en fréquence consiste à transmettre sur le même média plusieurs signaux modulés par des porteuses appartenant à des bandes de fréquence suffisamment éloignées les unes des autres. En réception, le signal correspondant à une porteuse donnée peut être séparé des autres signaux par un filtre en fréquence:

IV.2.5.3 LES MODEM:

MODEM est l'acronyme de Modulateur-Démodulateur. Un modem est un composant qui permet:

- En émission, de **moduler** une onde porteuse avec un signal binaire, puis de l'injecter sur un média donné.
- En réception, de **démoduler** une onde porteuse reçue sur un média donné afin d'en extraire le signal binaire de modulation.

Les MODEM sont à la base de la plupart des transmissions dès qu'elles dépassent le cadre local. Une transmission par modem nécessite deux de ces composants, un par hôte communicant:

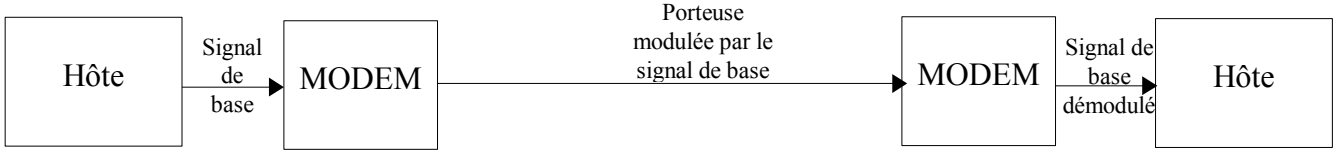


Schéma n° XX: modulation et démodulation

IV.2.5.4 LES TECHNIQUES DE MODULATION:

Il existe 3 procédés de modulation:

- **La Modulation d'Amplitude:** L'amplitude de la porteuse est fonction de l'amplitude du signal de base (par exemple, un bit à 1 sera représenté par un intervalle de temps ou l'amplitude est importante, un bit à 0 par un intervalle de temps ou l'amplitude est faible).
- **La Modulation de fréquence:** La fréquence de la porteuse varie en fonction de l'amplitude du signal de base. Ceci revient à dire que dans chaque bande, on utilise 2 fréquences de porteuse: une fréquence représente la valeur 0, l'autre la valeur 1.
- **La Modulation de phase:** Chaque transition du signal de base est représentée par une inversion de la phase du signal sinusoïdal de l'onde porteuse.

Le schéma de la page suivante représente les différentes techniques de modulation:

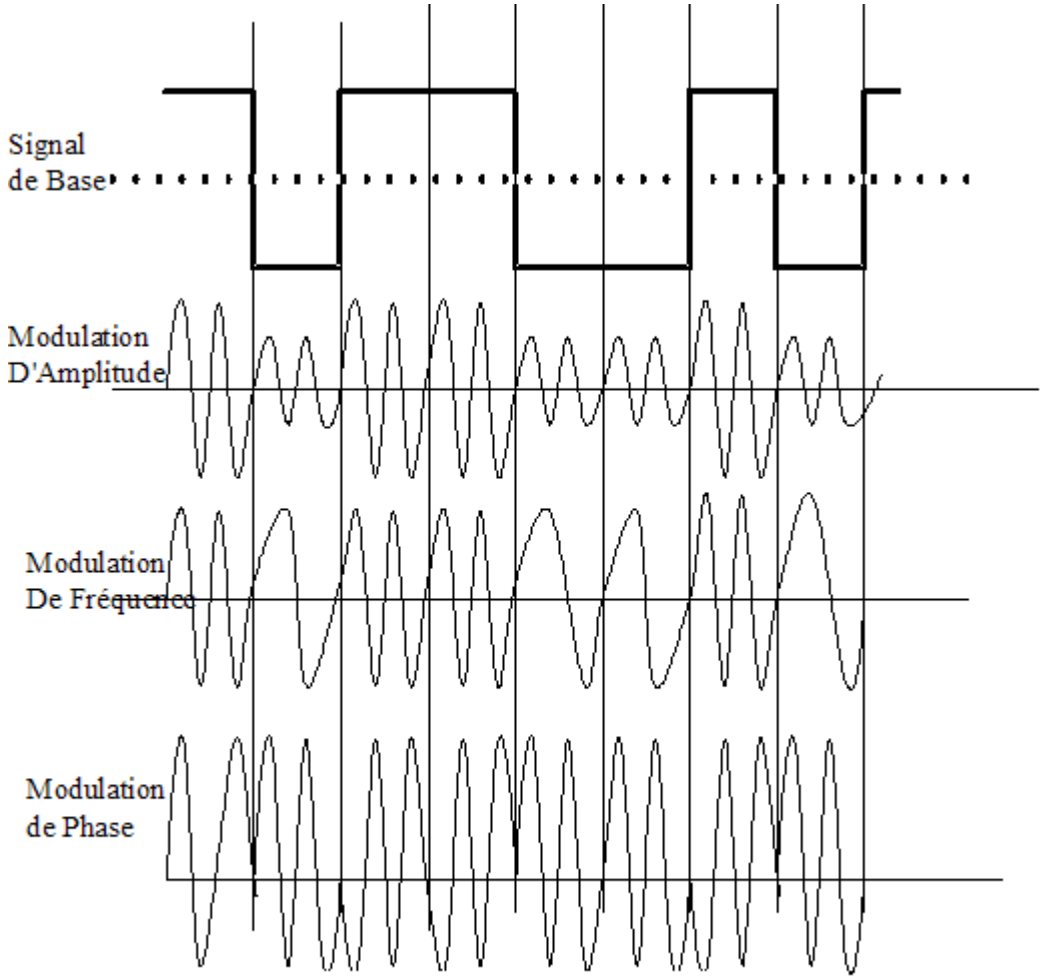


Schéma n° XXI: Techniques de modulation

REMARQUE:

Quel que soit le type de la modulation, celle-ci a pour effet de faire varier légèrement la fréquence instantanée du signal global par rapport à la fréquence porteuse. Chaque signal modulé occupe donc une bande de fréquence centrée sur la fréquence porteuse. De ce fait, sur un média multiplexé en fréquence, les fréquences des différentes porteuses doivent être suffisamment différentes les unes des autres pour éviter tout chevauchement des bandes. Le nombre de canaux de fréquences pour un média donné est donc forcément limité par le pouvoir discriminant des filtres démodulateurs et par la bande passante du média.

IV.2.5.5 LES MODEMS TELEPHONIQUES:

Nous avons vu qu'un réseau local se caractérise par la concentration des hôtes dans un périmètre donné à l'intérieur duquel on gère librement l'installation des équipements, et par des distances d'interconnexion assez faibles. De ce fait, sur un L.A.N. les liaisons internes se feront en bande de base. En revanche, dès qu'il s'agit d'établir une communication entre hôtes distants, situés sur des sites différents, il est difficile et très onéreux de mettre en place des liaisons spécifiques. Il faut alors utiliser des infrastructures de communication publiques. La plus accessible est le réseau téléphonique.

Le réseau téléphonique classique est un réseau dit «à commutation de circuits». Ceci veut dire que, pour la durée de chaque communication, un circuit physique est établi entre les deux hôtes. Les informations audio des communications téléphoniques sont en représentation analogique. Elles utilisent les fréquences comprises entre 300 et 3400 hz, soit une bande passante de 3100 hz.

LES MODEM TELEPHONIQUES CLASSIQUES:

Pour communiquer entre deux hôtes, ces modem utilisent l'infrastructure du réseau téléphonique à commutation de circuit selon les mêmes modalités qu'un poste téléphonique classique. Ceci implique que ces modem gèrent l'établissement, le maintien et la clôture du circuit de communication: composition du numéro, établissement du circuit physique par les commutateurs, décrochage de la ligne par le modem du correspondant appelé, communication, raccrochage et libération du circuit.

Ce type de liaison a l'avantage d'être peu coûteux en infrastructures et disponible pratiquement partout. C'est pour cette raison qu'il a été utilisé en priorité pour le raccordement des particuliers aux fournisseurs d'accès internet. Cependant, le débit est limité à 56 Kbits/s en voie montante et 33 Kbits/s en voie descendante. D'autre part, bien que communicant en signal modulé, ces modem exploitent la même bande que la téléphonie classique: les postes téléphoniques connectés aux mêmes raccordements sont donc indisponibles pendant toute la communication modem.

LES MODEM A.D.S.L:

Le terme A.D.S.L. (Asymétric Digital Suscribed Line) désigne un procédé de transmission de signaux numériques entre deux postes à partir des liaisons téléphoniques locales de ces deux postes («boucle de cuivre» locale, reliant l'abonné au central téléphonique).

REMARQUE:

Dans les pays francophones, on utilise parfois les termes: R.N.A (Raccordement Numérique Asymétrique) ou encore LNPA (Ligne Numérique à Paires Asymétriques).

Contrairement aux modems classiques, les liaisons A.D.S.L. n'utilisent que la boucle de téléphonie locale: à partir du central téléphonique, le flux A.D.S.L. est séparé de celui de la téléphonie classique, comme le montre le scéma ci-dessous:

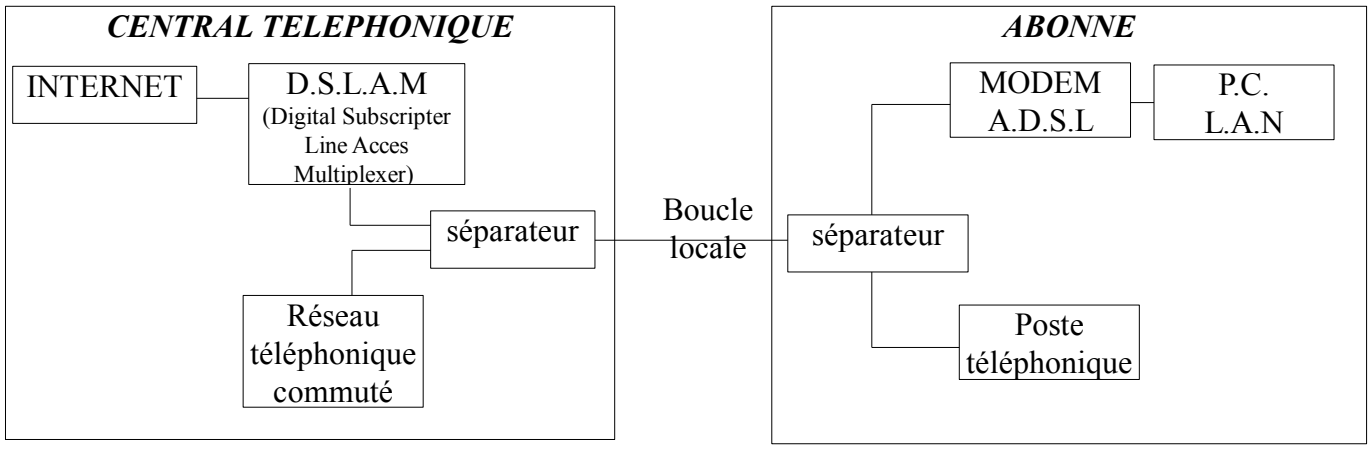


Schéma n° XXII: liaison A.D.S.L

COMMENTAIRES:

- Pour séparer les flux téléphoniques et A.D.S.L, une liaison A.D.S.L. utilise un multiplexage en fréquence. La technique de modulation D.T.M. (Discret Multi Tone) consiste à diviser la bande de fréquences de 0 à 1,104 Mhz en 256 canaux de 4,3125 Khz. Les 6 premiers canaux sont réservés à la téléphonie analogique, les 27 suivants à la voie A.D.S.L. montante et le reste à la voie descendante. A chacun des canaux ADSN correspond une sous-porteuse. L'ensemble du dispositif permet d'atteindre des débits très élevés (en France, le réseau permet actuellement jusqu'à 10 mbits en voie descendante et 0,8 Mbits en voie montante, mais les débits pourraient être nettement améliorés).
- En voie montante, le modem A.D.S.L. de l'abonné émet le signal numérique modulé suivant la technique D.T.M. Au niveau du séparateur de l'abonné, ce signal est ajouté aux signaux émis par le poste de téléphonie local sur la bande analogique. Le

signal résultant est envoyé sur la boucle téléphonique locale vers le central de l'abonné. Au niveau du central, le trafic A.D.S.L. est séparé du trafic téléphonique par le séparateur et envoyé vers le D.S.L.A.M. qui le démultiplexe et l'adapte avant de l'injecter sur le réseau internet. Le trafic téléphonique est, lui, envoyé vers le réseau commuté classique.

- En voie descendante, au niveau du central, le trafic internet est multiplexé par le D.S.L.A.M., puis ajouté au trafic téléphonique avant d'être injecté sur la boucle locale de l'abonné. Chez celui-ci, le séparateur (filtre A.D.S.L) sépare le trafic A.D.S.L. de signaux de téléphonie classiques. Ces derniers sont dirigés vers le poste téléphonique. Le trafic A.D.S.L. est acheminé vers le modem qui le démultiplexe et le démodule avant de l'envoyer vers le PC ou de le distribuer vers un réseau local grâce à un pont routeur (les **-box des fournisseurs d'accès).
- La séparation du trafic A.D.S.L. du trafic de la téléphonie analogique permet d'utiliser les postes téléphoniques en même temps que la liaison A.D.S.L.
- Ce type de liaison est dit «asymétrique» car le débit montant (de l'usager vers le standard) est nettement plus faible que le débit descendant (du standard vers l'usager). Il est donc bien adapté à une liaison du type client-serveur comme celle qui relie un utilisateur d'internet à son fournisseur d'accès.

IV.3 TECHNOLOGIES DE LA COUCHE LIAISON:

IV.3.1 METHODES D'ACCES AU MEDIA (COUCHE MAC: MEDIUM ACCES CONTROL)

Une méthode d'accès permet:

- D'assurer le partage du «temps de parole» entre les hôtes du réseau.
- D'éviter l'accès simultané de plusieurs hôtes au média si celui-ci ne le permet pas (collisions entre messages).
- D'assurer un bon rendement du réseau en favorisant l'utilisation optimale de la bande passante.

Deux méthodes d'accès sont les plus utilisées:

- L'accès «aléatoire», encore appelé «accès par contention».
- L'accès partagé dans le temps, encore appelé «accès par partage de jetons».

IV.3.1.1 ACCES PAR PARTAGE DE JETON:

PRINCIPE:

Le droit d'émettre est alloué successivement à tous les hôtes du réseau suivant un ordre déterminé. Ce droit d'émettre est matérialisé par un petit message appelé TOKEN (jeton en français): lorsqu'un hôte «possède» le jeton (ce qui revient à dire que le message vient de lui être tranmis), il peut émettre un message destiné à un ou plusieurs autres hôtes. Cependant, ce message est toujours transmis vers la station suivante dans l'ordre d'attribution établi. Le message est ainsi relayé d'hôte en hôte vers son ou ses destinataires. La durée de transmission d'un message dépend donc du nombre d'hôtes relais entre émetteur et destinataire.

Par la suite, le possesseur du jeton transmet celui-ci à l'hôte suivant dans l'ordre d'attribution. Lorsque le dernier poste de la liste a utilisé son jeton, il le transmet au premier, et ainsi de suite.

Seul, le possesseur du jeton a le droit d'émettre ses messages personnels. Les autres hôtes se contentent de relayer les messages reçus de leurs prédécesseurs dans la liste vers leurs successeurs, en faisant une copie de ceux qui leurs sont destinés.

En général, c'est l'émetteur d'un message qui le retire de la circulation: lorsqu'il détecte ce message sur le réseau, il lui suffit de ne pas le relayer.

REMARQUE:

Nous pouvons voir que ce principe structure les postes en «anneau logique», puisque le jeton parcours toujours la liste des hôtes dans le même ordre, en rebouclant à la fin. Ceci ne veut pas dire qu'il implique une ***topologie en anneau****: un tel mécanisme peut fonctionner sur n'importe quelle topologie physique pourvu qu'un ordre de transmission du jeton ait été défini dans l'ensemble des hôtes: cet ordre définit un anneau «logique».*

VARIANTES DE FONCTIONNEMENT:

On distinge deux types de fonctionnement:

1. **Passage immédiat du jeton:** Après avoir émis une trame, la station détentrice du jeton réinjecte immédiatement le jeton sur le réseau, derrière la trame émise. De ce fait, la station suivante reçoit trame et jeton en même temps. Elle a donc le droit d'émettre elle aussi une trame derrière la trame reçue. Plusieurs trames peuvent donc circuler sur le réseau à un instant donné. Le temps d'attente du jeton pour une station est très variable, car il dépend du nombre et de la taille des trames en circulation. En revanche, la bande passante est bien utilisée.
2. **Jeton et trame unique:** Dans ce cas, la station détentrice du jeton attend le retour de la trame émise avant de libérer le jeton. Comme c'est elle qui la retire de la circulation, une seule trame circule sur le réseau à un instant donné. De ce fait, l'émetteur n'a pas besoin, pour retirer son message, de vérifier son adresse. Cette solution a l'inconvénient de mal utiliser la bande passante. En revanche, le temps d'attente du jeton dans une station devient pratiquement constant.

ANNEAU A JETON (TOKEN RING):

Il s'agit d'une topologie en anneau associé à un accès par circulation de jeton. Cette topologie a la particularité d'établir un ordre physique entre les hôtes: une station donnée ne peut émettre directement que vers la station suivante. De ce fait, le jeton peut être réduit au minimum car il n'a pas besoin de contenir une adresse de station.

BUS A JETON (TOCKEN BUS):

Dans ce cas, la topologie du réseau étant un B.U.S., il n'existe pas d'ordre physique des stations car chacune a la possibilité de communiquer directement avec toutes les autres. Il faut donc créer et maintenir un «anneau logique» représenté par une liste ordonnée des stations du réseau. Cette technique correspond à la norme ISO 8802.7.

REMARQUES:

Cette méthode d'accès ne peut être entièrement décentralisée: en effet, il est nécessaire d'avoir une station qui se charge des tâches suivantes:

- La génération du jeton au démarrage.
- La détection de la perte du jeton et sa régénération.
- La détection de la duplication du jeton et la suppression des doublons.
- La détection et la suppression des trames erronées.

Dans le cas d'un anneau à jeton, l'ajout ou le retrait d'un poste demande une intervention assez lourde, car pourl'introduire dans l'anneau, il faut modifier les connexions physiques de deux autres postes.

De ce fait, la gestion d'un réseau a jeton est assez complexe.

IV.3.1.2 ACCES PAR CONTENTION-CSMA-CD:

PRINCIPE:

Cette technique est aussi appelée «accès aléatoire», car il n'y a pas d'attribution du droit d'émettre. Elle est illustrée par le protocole d'accès désigné par l'acronyme C.S.M.A-CD (Carrier Sense Multiple Acces-Collision Detection), caractéristique d'éthernet, mais des techniques semblables sont utilisées pour d'autres réseaux, notamment les réseaux locaux WiFi.

Le principe du CSMA-CD est le suivant:

- Une station désirant émettre commence par écouter le trafic sur le canal de transmission afin de détecter s'il est occupé par une émission en cours. La technique de détection du trafic consiste à tenter d'extraire du signal une «pseudo-porteuse» (Carrier Sense = détection de porteuse). Cette phase est appelée L.B.T (Listen Before Talking).
- Si le canal est occupé, la transmission est différée d'une durée aléatoire (choisie grâce à un algorithme appelé Back-Off) puis on revient en phase LBT.
- Sinon, on commence à émettre le message tout en continuant d'écouter le trafic. Cette phase est appelée L.W.T. (Listen While Talking).
- Si, dans cette phase, on détecte une autre émission, susceptible de perturber le message envoyé, on arrête l'émission en cours et on émet un signal de brouillage (Jamming signal) pour forcer l'arrêt des autres émissions. Puis, après une durée aléatoire (algorithme de back-off), on réessaie d'émettre (retour en phase L.B.T).
- Sinon, l'émission se termine et on libère le canal.

En effet, si la phase L.B.T. réduit considérablement le risque de collision, il ne l'empêche pas totalement, car il existe toujours la possibilité que deux station se mettent à émettre en même temps, ou dans un intervalle de temps inférieur à la propagation du signal de l'une vers l'autre. De ce fait, la phase L.W.T. avec sa détection des collisions est indispensable.

Le choix d'un délais de réémission aléatoire permet de rendre infime la probabilité que deux stations entrées en collision réémettent au même moment, provoquant ainsi des collisions en chaîne.

REMARQUES:

- L'accès par contention a l'avantage d'être entièrement décentralisé, ce qui facilite la gestion du réseau (l'ajout ou le retrait d'une station n'a aucun impact sur les autres hôtes, le nombre de station n'augmente pas la durée de transmission).
- Le rendement d'un réseau géré en CSMA/CD est d'autant meilleur que la charge du réseau en nombre d'équipements et en volume de données est faible. Dans ce cas, le réseau peut être utilisé jusqu'à 90% de ses capacités avec des délais d'attente en LBT assez faibles, et une probabilité de collision inférieure à 1%. Lorsque le nombre de postes ou le volume de données émises augmente, les délais d'attente et la probabilité de collision augmentent très rapidement.
- Le principal inconvénient de l'accès par contention est de ne pas permettre de garantir les dates d'émission. De ce fait, ce mode d'accès convient mal aux applications à contraintes temps réel fortes, sauf si l'utilisation du réseau reste faible par rapport aux capacités de transmission et si l'on n'exige pas un déterminisme absolu.

IV.3.1.3 ANNEAU A TRAME CIRCULANTE (SLOTTEN RING):

Cette méthode est peu utilisée. Elle a été mise au point par l'université de CAMBRIDGE au début des années 1980 (Cambridge Ring - Anneau de Cambridge).

Dans ce type d'architecture, les stations sont reliées point à point par des interfaces actives. Des trames de longueur fixe circulent sur l'anneau. L'en-tête de chaque trame indique si cette trame est vide ou occupée. Lorsqu'une station reçoit une trame vide, elle peut la remplir et l'utiliser pour transmettre un message à une autre station. Les trames sont recopiées par le destinataire et vidées par l'émetteur, après un tour de l'anneau.

Ce type d'architecture nécessite qu'un des noeuds soit dédié aux fonctions de gestion des exceptions. L'avantage principal est que les durées de propagation sont déterministes. Les inconvénients sont la fixité de la longueur des trames et le mauvais rendement à faible charge.

IV.3.1.4 ACCES GERE PAR COMMUTATEUR (TOPOLOGIE EN ETOILE ACTIVE):

Dans ce type de solution, tous les hôtes sont reliés directement à un équipement d'interconnexion actif, c'est à dire ne se contentant pas de répéter les messages entrants sur les ports en sortie (commutateurs, switches en anglais). Chaque liaison hôte-commutateur possède une voie montante distincte de la voie descendante (liaison full-duplex).

Dans une topologie de ce type, l'accès d'un hôte au réseau est toujours possible puisqu'il est le seul à accéder en émission à son média. Les mécanismes d'accès par contention peuvent (et doivent) donc être désactivés. Le commutateur assure le routage entre ses ports et l'injection sur les voies descendantes. En général, ce type de commutateur utilise en interne des algorithmes analogues à ceux de la technologie A.T.M (commutation de cellules, multiplexage temporel des flux injectés sur les voies descendantes par gestion de files d'attentes).

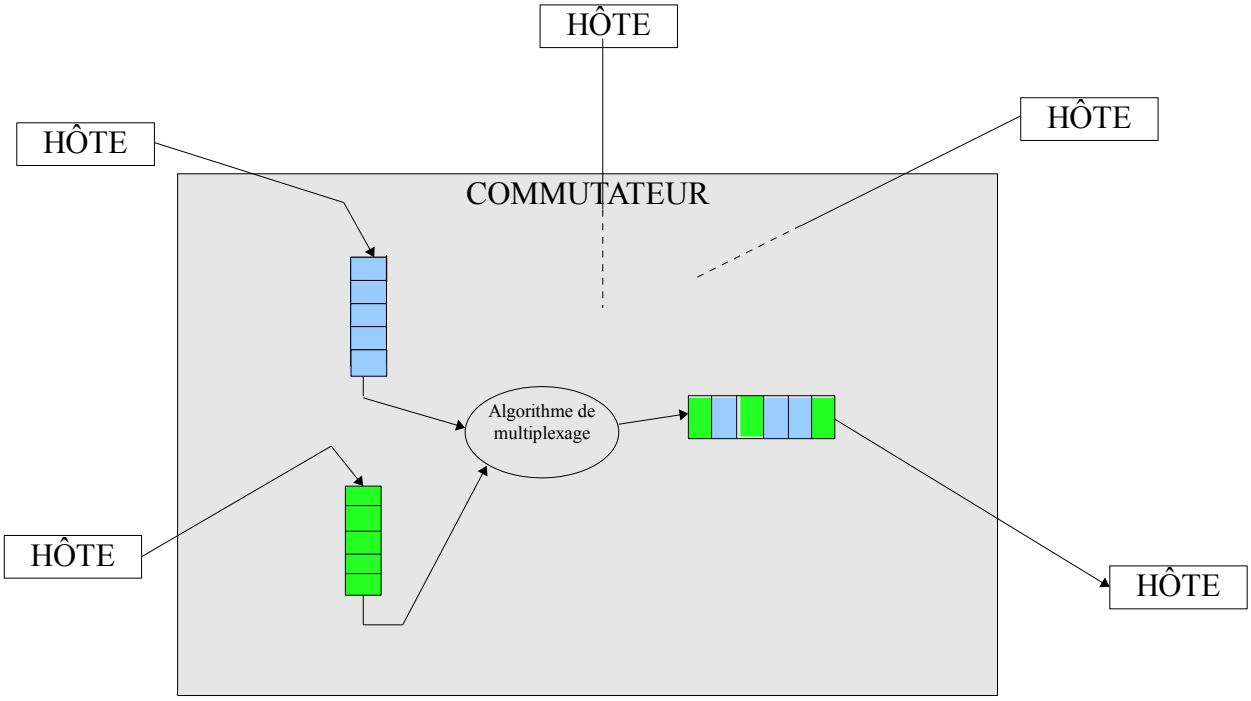


Schéma n° XXIII: Topologie en étoile active

REMARQUES:

- *Ce type de commutateur peut également offrir des fonctionnalités de filtrage programmable du trafic très évoluées.*
- *Rien n'oblige à ce que les connexions des hôtes au commutateurs soient toutes de même technologie: un même commutateur peut offrir des liaisons éthernet sur paire torsadée, des liaisons wifi, etc..*

Ce type de solution présente, évidemment, beaucoup d'avantages:

- Il règle le problème de l'accès au réseau: celui-ci est permanent. De ce fait, il garantie le déterminisme des dates d'acheminement.
- Il garantit (dans une certaine mesure) les temps de trajet des informations.
- Un dysfonctionnement d'un des hôtes ne peut remettre en cause le fonctionnement global.

Cependant, il s'agit d'une solution coûteuse. En effet, le fonctionnement du commutateur doit être très sécurisé, ce qui exige des architectures matérielles complexes, avec de nombreuses redondances, notamment au niveau de l'alimentation électrique.

Cette solution est à la base des réseaux A.T.M.

IV.3.2 L'ADRESSAGE PHYSIQUE (ADRESSE M.A.C):

Le format des adresses M.A.C. est normalisé par l'I.E.E.E (Institute of Electrical and Electronics Engineers). Deux types d'adresses MAC sont définies. L'un d'eux concerne les réseaux non interconnectés, l'autre les réseaux interconnectés:

IV.3.2.1 ADRESSE MAC POUR RESEAUX NON INTERCONNECTES:

Ces adresses sont libellées sur 16 bits (2 octets). Leur format est le suivant:

CHAMP	SIGNIFICATION	COMMENTAIRES
Bit 0	I/G (Individuelle/Groupe)	- Si I/G = 0, l'adresse est l'adresse d'un hôte - Si I/G = 1, l'adresse est celle d'un groupe d'hôtes (adresse multicast)
Bits 1 à 23	Adresse	- Si I/G = 0, adresse de l'hôte (fixée localement par l'utilisateur) - Si I/G = 1, identificateur du groupe d'hôtes

IV.3.2.2 ADRESSE MAC POUR RESEAUX INTERCONNECTES:

Ces adresses sont libellées sur 48 bits (6 octets). Leur format est le suivant:

CHAMP	SIGNIFICATION	COMMENTAIRES
Bit 0	I/G (Individuelle/Groupe)	- Si I/G = 0, l'adresse est l'adresse d'un hôte - Si I/G = 1, l'adresse est celle d'un groupe d'hôtes (adresse multicast)
Bit 1	U/L (Universelle/Locale)	- Si U/L = 0, il s'agit d'une adresse universelle, dont la valeur du champ «Constructeur» est fournie par l'IEEE (groupe de travail 802.2) - Si U/L = 1, il s'agit d'une adresse locale. La valeur des autres champs peut alors être fixée par l'utilisateur
Bits 2 à 23	Constructeur	L'IEEE fixe une valeur pour chaque constructeur. Exemple: pour 3COM -> 02:60:8C
Bits 24 à 47	Identificateur de l'équipement	Le constructeur identifie chaque équipement d'une manière unique à l'aide de ce champ.

REMARQUES:

- L'adresse MAC d'un équipement est codée «en dur» dans cet équipement (elle peut être lue, mais non modifiée).
- Les bits 0 et 1 d'une adresse lue sur un équipement respectant les norme IEEE sont fixés à la valeur 0 (il s'agit d'adresses indiviuelles et universelles)
- En revanche, la valeur d'une adresse MAC circulant sur le réseau ne correspondra à l'adresse MAC fournie par l'équipement que dans le cas d'un échange en unicast.

- L'adresse MAC d'un équipement est lue au lancement du système d'exploitation et sauvegardée dans un fichier de configuration. En général, les systèmes d'exploitation permettent de modifier cette adresse pendant la durée de la session d'utilisation, mais la valeur «en dur» sera rétablie au prochain lancement.

IV.3.2.3 ADRESSAGE ETHERNET:

L'adressage des matériels utilisant la technologie ethernet est pratiquement conforme aux recommandantions IEEE, sauf en ce qui concerne le mode multicast. En effet, une adresse ethernet multicast correspond au format suivant:

CHAMP	SIGNIFICATION	COMMENTAIRES
Bits 0 à 23	Identifiant mode multicast	Cet identifiant correspond à la valeur hexadécimale: 0x01005E
Bit 24		Le bit 24 est nul
Bits 25 à 47	Groupe multicast	Le numero du groupe multicast est le même que celui qui est libellé dans l'adresse multicast IP

EXEMPLE: l'adresse IP multicast 224.0.0.25 sera résolue par l'adresse ethernet 01:00:5E:00:00:25

IV.3.3 CONTRÔLE DU LIEN (COUCHE LLC: LINKER LAYER CONTROL):

La couche LLC assure le contrôle point à point entre deux noeuds physiques adjacents. Les protocoles de liaison de données, permettent:

- De segmenter-réassembler l'information en messages élémentaires
- Contrôler l'intégrité des informations transmises.

Les principaux protocoles de liaison en séries de la sous-couche LLC sont le protocole B.S.C.(liaison synchrone) et le protocole H.D.L.C:

IV.3.3.1 PROTOCOLE B.S.C (BINARY SYNCHRONOUS COMMUNICATION):

Le protocole BSC est un protocole permettant d'échanger des octets en série sur une liaison de données. Il est «orienté caractères», ce qui signifie qu'il utilise un certain nombre de caractères particuliers pour structurer les messages:

- Caractère SYN: Caractère de synchronisation en début de message.
- Caractère SOH: Start Of Header
- Caractère STX: Start Of Text => synchro trame
- Caractère ETX: End Of Text

Ces caractères structurent le flot d'octets représentant une trame B.S.C. De la manière suivante:

[SYN] [SYN] .... [SYN] ----->
----> [SOH] <caractères composant le header> ----->
----> [DLE] [STX] <caractères composant le texte du message> ----->
----> [DLE] [ETX] [CRC]

Les caractères [SYN] en début de message servent à synchroniser le récepteur sur le début de message. Le caractère CRC suivant le caractère de fin de texte (ETX) est un caractère de contrôle permettant de vérifier l'intégrité des données transmises (C.R.C: Contrôl Range Caracter). Le CRC est calculé par l'émetteur par division de la suite de bits composant le message par un polynôme de contrôle cyclique. Il est vérifie par le récepteur de la même manière.

Le protocole B.S.C possède un mode dit "Transparent", qui permet l'envoi de données binaires dans la partie texte, en utilisant le caractère D.L.E (Data Link Escape). Ce caractère a 2 significations:

- En dehors de la zone de texte, il précède les caractères de contrôle.
- Dans la partie "texte", lorsqu'une configuration binaire correspondant à DLE apparaît, elle est automatiquement doublée dans le message émis (sauf, bien sûr, le DLE précédant ETX).

Le message: .... [octet i = DLE][octet i+1 = DLE][octet i+2].....[DLE][ETX]
devient en émission: .... [DLE] [octet i = DLE][DLE] [octet i+1 = DLE][octet i+2].....[DLE][ETX]

En réception, il suffit de supprimer tous les DLE doublés pour retrouver le message initial:

IV.3.3.2 PROTOCOLE H.D.L.C (HIGHT LEVEL DATA LINK CONTROL):

H.D.L.C. est un protocole de liaison de données permettant de transmettre des configurations binaires (pas nécessairement divisables en octets). La structure d'une trame HDLC est la suivante:

[FLAG][ADR][CMD]<données transmises (suite de bits)>[FCS (16 ou 32 bits)][FLAG]

- FLAG: Fanion délimiteur de trame (Octet de valeur 0x7E, soit la valeur binaire 01111110)
- ADR: Octet adresse du destinataire (non utilisée en point à point)
- CMD: Octet type de trame (3 types: information/supervision/non numérotée)

- FCS: Frame Check sequence (16 ou 32 bits): code de vérification d'erreurs (CRC)

REMARQUES:

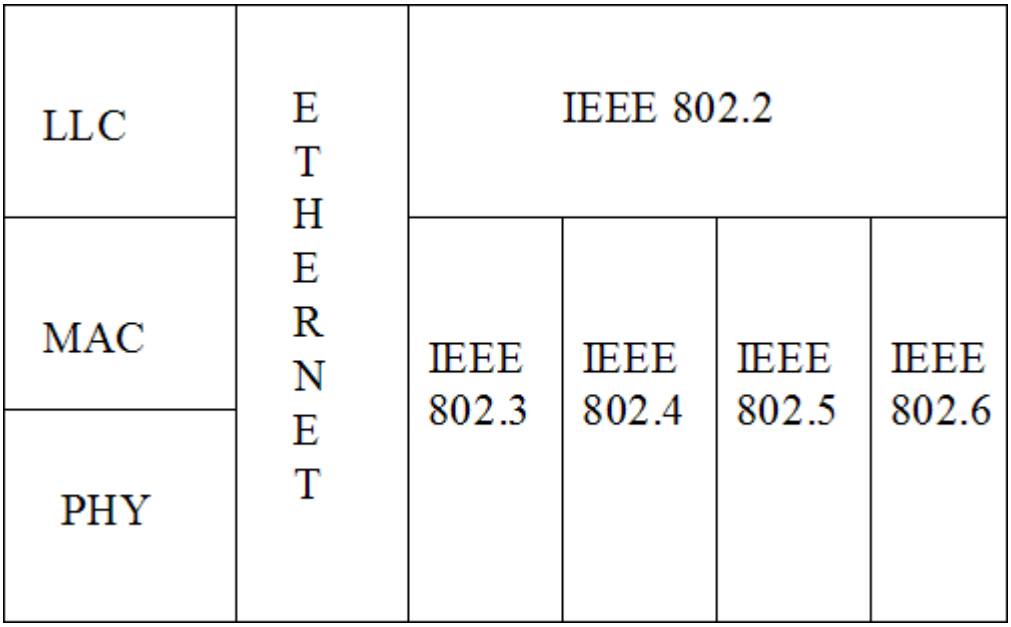
- Des trames HDLC peuvent être concaténées. Dans ce cas, le flag de fin de l'une sert de flag début de l'autre.
- Pour éviter toutes confusion entre octet fanion et données, chaque fois que dans la partie «données transmises» apparaît une configuration de 5 bits à 1 consécutifs, un bit à zéro est ajouté à la fin avant émission. Ces bits à zéro sont éliminés à la réception.

2.5.3.NORMALISATION IEEE DES COUCHES BASSES DE L'O.S.I:

Les normes de L'Institute of Electrical and Electronics Engineers (I.E.E.E) ne recoupent pas totalement le modèle O.S.I:

- La norme IEEE 802.2 correspond à peu près à la sous-couche LLC.
- Chacune des normes IEEE 802.3 à 802.6 normalise la couche physique est la sous-couche MAC pour une méthode d'acces donnéé.
  - 802.3: C.S.M.A / CD
  - 802.4: Token Bus
  - 802.5: Token Ring
  - 802.6: Slotten Ring.
- La norme IEEE 802.11 concerne les réseaux locaux sans fil. Elle concerne les couches 1 et 2 du modèle OSI.

D'autre pa rt le standard ETHERNET recouvre à la fois les couches physique et liaison:



IV.4 PROTOCOLES DE LA COUCHE RESEAU:

IV.4.1 PROTOCOLE IP (INTERNET PROTOCOL):

GENERALITES:

Le protocole IP correspond sensiblement à la couche 3 de l'ISO. Il permet la communication entre deux hôtes, le cas échéant via un intermédiaire (routeur). Les P.D.Us de la couche IP sont appelés **paquets** (s'ils font partie d'un message fragmenté) ou **Datagrams** (si le message n'a pas été fragmenté)

SERVICES FOURNIS PAR IP:

REDIRECTION ET ROUTAGE:

Ce service permet de communiquer entre 2 hôtes hébergés sur un même réseau physique (Intra-Networking) ou sur deux réseaux interconnectés entre eux (InterNetworking).

IP a été conçu pour permettre l'interconnexion de réseaux dont les protocoles basses couches sont différents. Ces derniers sont connectés à des passerelles hébergeant une couche réseau IP pour assurer le transcodage d'un protocole à l'autre.

GESTION DE LA DUREE DE VIE DES DONNEES:

A chaque paquet peut être associé une «durée de vie» (Time To Live-TTL), qui est en fait le nombre de routeurs d'équipements d'interconnexion que ce paquet est autorisé à franchir. A chaque franchissement d'un de ces équipements, le TTL est décrémenté. S'il est trouvé nul, le paquet est éliminé.

VERIFICATION D'INTEGRITE DES DONNEES:

Les P.D.U.s IP contiennent une "Checksum" comprise dans l'en-tête IP. Celui-ci permet la mise en oeuvre d'un système de correction d'erreurs.

L'ADRESSAGE LOGIQUE IP:

Au niveau des couches basses (1 et 2), chaque station est repérée par une adresse physique, ou adresse MAC (***exemple***: adresse ethernet). L'adressage logique permet de faire abstraction de la structure physique (il ne serait pas pratique, en effet, d'avoir à se préoccuper des répercussions d'un changement d'adresse physique d'un hôte, consécutif au changement d'un contrôleur ethernet).

La couche IP met donc en oeuvre son propre système d'adressage logique, accompagné d'un mécanisme permettant d'assurer en permanence la résolution des adresses IP en adresses physiques.

Une adresse IP courante (Ipv4) est représentée par une configuration de 32 bits (4 octets). Pour libeller une adresse IP, il existe deux moyens:

- Soit écrire les valeurs décimales des 4 octets, séparées par des points (Exemple: 202.41.1.50).
- Soit écrire la valeur hexadécimale de l'adresse (8 chiffres hexadécimaux). Par exemple, l'adresse précédente s'écrit: 0xCA290232.

Une adresse IP peut être divisée en deux champs: le premier représente l'adresse du réseau sur lequel l'hôte est implanté, le deuxième représente l'adresse de l'hôte dans le réseau. Suivant la classe à laquelle appartient l'adresse, le champ «réseau» est plus ou moins long et la champ d'adressage de l'hôte ajusté en conséquence.

EXEMPLE: 202.41.1.50 est une adresse dite de classe C. Dans cette adresse, 202.41.50 représente l'adresse du réseau et 50 représente l'adresse de l'hôte dans ce réseau.

Pour plus de détails, voir plus loin le chapitre concernant l'adressage I.P.

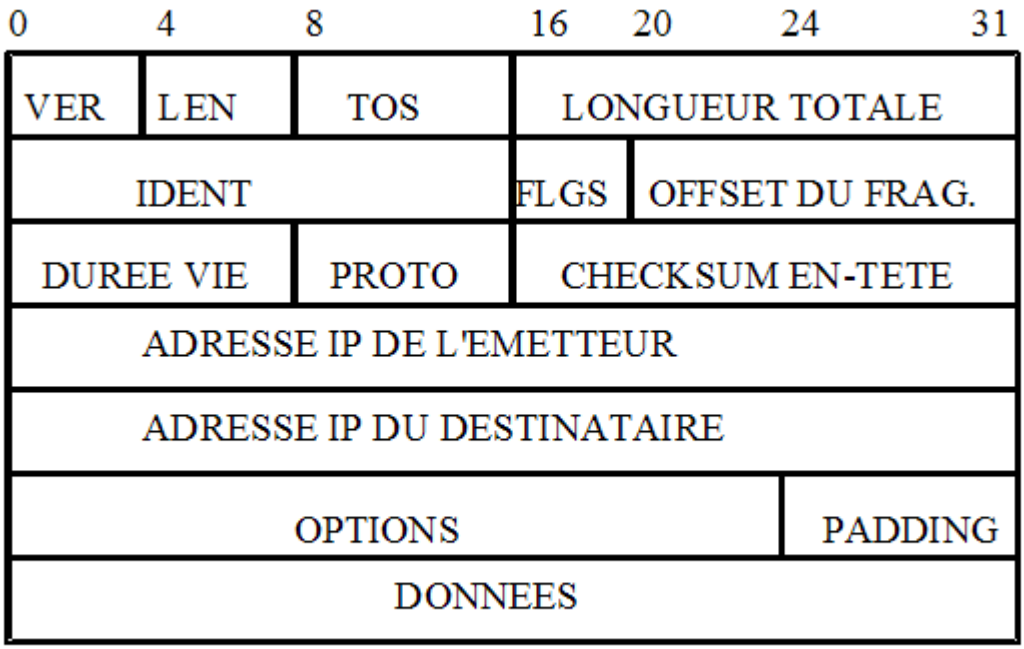
REMARQUE: *Une nouvelle norme d'adressage (Ipv6) est en cours de déploiement.*

EN-TETE IP:

Le schéma suivant décrit l'en-tête d'un paquet IP:

COMMENTAIRES:

- VER: N° Version IP (actuellement=4)
- LEN: Longueur de l'en-tête (en mots de 32 bits)
- TOS: Type Of Service (définit les besoins du service activé par les couches supérieures)
- LONGUEUR TOTALE: Longueur en octets du Datagram.
- IDENT: Identification des fragments d'un même Datagram (fournie par couches superieures).
- FLGS: Valide ou non la fragmentation et indique si d'autres fragments suivent.
- PROTO: Identifie le protocole supérieur (TCP, UDP, etc .....).
- OPTIONS: Permet par ex. de définir la route a utiliser (maintenance).
- PADDING: Suite de 0 (alignement sur 32 bits).



FORMAT DE L'EN-TÊTE IP

IV.4.1.1 AUTRES PROTOCOLES DE LA COUCHE IP:

PROTOCOLE ARP (Adress Resolution Protocole).

Ce protocole permet de rechercher dynamiquement l'adresse MAC qui correspond à une adresse logique (adresse IP). Lorsque la couche réseau d'un hôte doit transmettre un paquet à un destinataire, elle a besoin de connaître l'adresse MAC de celui-ci pour construire l'en-tête du S.D.U qu'elle va transmettre à la couche liaison.

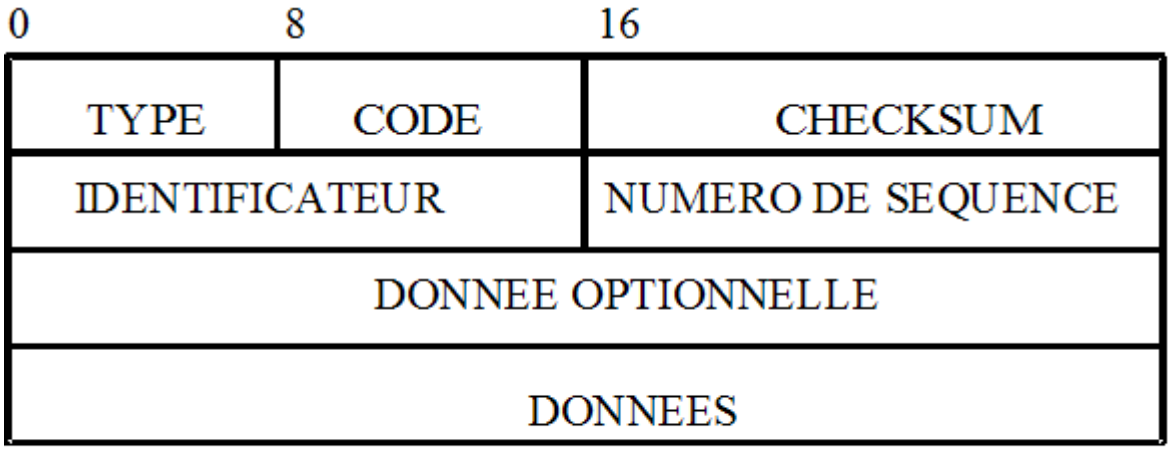
Pour cela, elle va d'abord vérifier le contenu d'une table appelée «masque ARP». Si cette table contient la correspondance entre l'adresse IP du destinataire et son adresse MAC, la question est résolue. Sinon, la couche 3 émet un paquet en mode broadcast (donc, destiné à tous les hôtes du réseau local) pour demander au destinataire (désigné par son adresse IP), de lui transmettre son adresse physique (adresse MAC). Cette adresse est ensuite transmise à la sous-couche MAC qui l'utilise pour construire et entretenir

PROTOCOLE RARP:

Il propose le service inverse de ARP. Ce service est utilisé pour certaines stations "DiskLess", qui ne disposent au boot que de leur adresse Ethernet. Un message en broadcast leur permet de demander au serveur de leur donner leur adresse IP.

PROTOCOLE ICMP (Internet Control Message Protocol):

Ce protocole est utilisé essentiellement pour des fonctions de maintenance. Il supporte des primitives de test du réseau (exemple: primitive PING).



FORMAT D'UN MESSAGE ICMP

COMMENTAIRES:

- TYPE: Type du message et format du reste du paquet
- CODE: Infos supplémentaires sur le type
- CHECKSUM: Contrôle d'erreurs
- IDENTIFICATEUR, NUMERO DE SEQUENCE, etc... champs utilisés pour réponse

IV.5 PROTOCOLES DE LA COUCHE TRANSPORT:

IV.5.1 LE PROTOCOLE TCP (TRANSPORT CONTROL PROTOCOL):

IV.5.1.1 GENERALITES:

T.C.P. est un protocole de transport de données **sécurisé** en mode **connecté**. Il permet à des **processus**, pouvant appartenir à des hôtes différents d'un réseau étendu, d'échanger des **messages de gros volume** segmentés en paquets de données, en effectuant un **contrôle de bout en bout** de la transmission.

Le protocole TCP est du modèle CLIENT-SERVEUR. En effet, un processus communicant par TCP doit être déclaré en tant que **client TCP** ou **serveur TCP.** C'est le processus client qui demande à se connecter à un processus serveur. Le serveur attend des demandes de connexion et les accepte (ou non). Un serveur peut être connecté à plusieurs clients. L'inverse n'est pas vrai.

IV.5.1.2 SERVICES FOURNIS PAR LE PROTOCOLE TCP:

DETECTION D'ERREURS ET SECURISATION DES TRANSMISSIONS:

Les données transmises sont garanties sans perte ni duplication, grâce à la mise en oeuvre d'un mécanisme d'acquittement positif (Positive Acknowledgement-l'acquittement est dit positif, car il a toujours lieu, même lors d'une réception correcte). La couche TCP du récepteur émet une trame d'acquittement pour chaque paquet reçu ou une trame de time-out en cas de dépassement du délais de réception. Ces trames sont utilisées par l'émetteur pour activer, le cas échéant, un mécanisme de réémission.

CONTROLE DES FLUX:

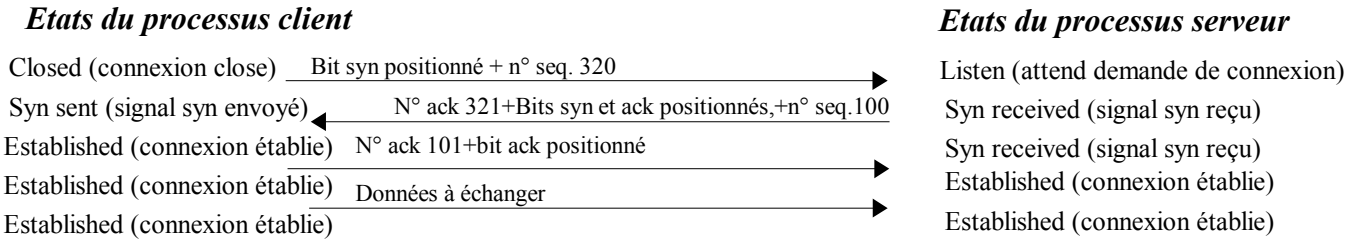
Les trame d'acquittement, émises par le récepteur, indiquent le nombre d'octets que celui-ci est capable de recevoir dans son buffer. L'utilisation de ces données par l'émetteur lui permet de prévenir les surcharges du réseau que les réémissions peuvent provoquer.

MULTIPLEXAGE, NOTIONS DE PORT ET DE SOCKET:

La couche T.C.P. d'un hôte est capable de gérer simultanément la communication de plusieurs processus de cet hôte avec des hôtes externes ou internes. Un processus récepteur est identifié par un **NUMERO DE PORT** (nombre entier de 1 à 32768). Un couple [Adresse IP , numero de PORT] identifie donc d'une manière unique un processus dans un hôte donné. Ce couple est appelé **SOCKET TCP/IP**.

CONNEXION TCP:

TCP est un protocole de transport en **mode connecté** qui établit **entre deux sockets** des **circuits virtuels de transfer de données** au niveau Transport. La connexion par circuit virtuel permet de s'assurer de la synchronisation des systèmes émetteurs et récepteurs lors d'une transmission. Le schéma suivant décrit une procédure de connexion:

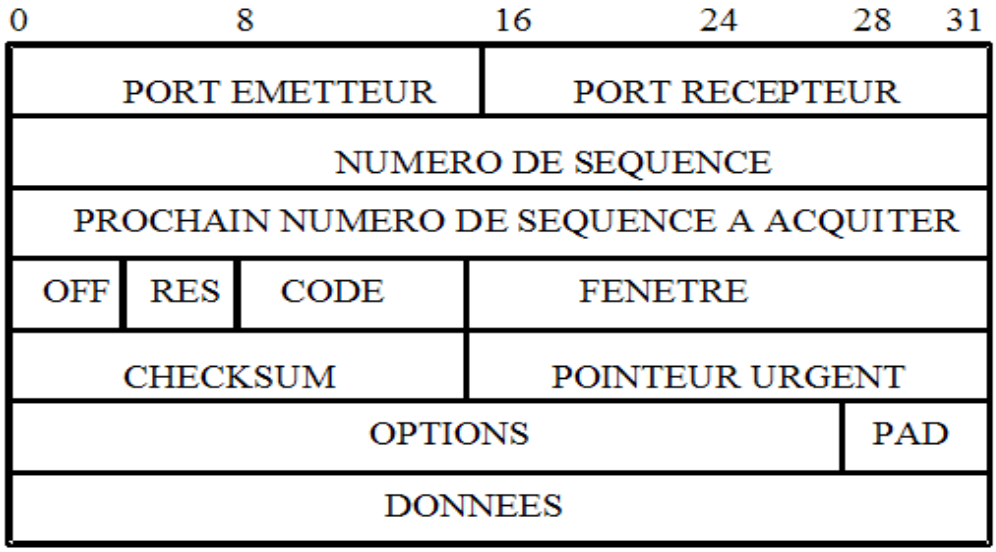


TRANSMISSION PAR PAQUETS:

Le protocole T.C.P. Incluse un mécanisme élaboré de transmission par paquets avec segmentation et réassemblage sécurisés. Chaque paquet de données envoyé comporte dans son en-tête:

- Un N° de séquence qui identifie l'ordre du paquet dans le message..
- Un numéro d'acquittement permettant de valider la réception des paquets précédemment envoyées.
- Des données permettant la réémission de trame sur Time-Out de réception d'un paquet.
- Une Checksum permettant de vérifier l'intégrité des informations transmises.

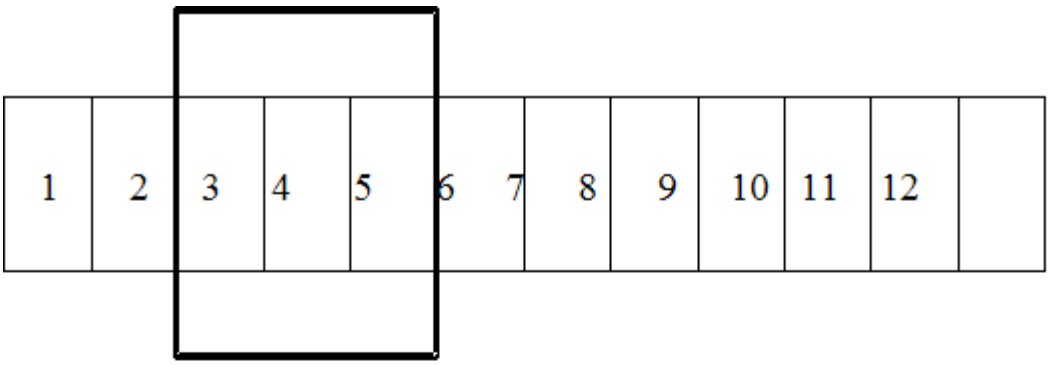
FORMAT D'UN PAQUET TCP:



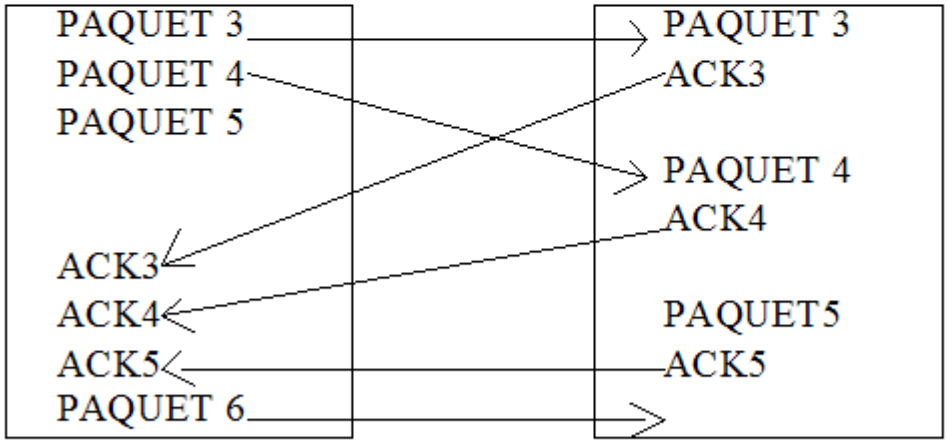
COMMENTAIRES:

PORT EMETTEUR:	Identificateur du processus émetteur
PORT RECEPTEUR:	Identification du processus récepteur
NUMERO DE SEQUENCE:	Numéro d'ordre du paquet
PROCHAIN NUMERO DE SEQUENCE A ACQUITTER:	Valeur du prochain numéro de séquence que l'émetteur s'attend à recevoir.
OFF:	Longueur en mots de 32 bits de l'en-tête TCP
RES:	Réservé
CODE:	Flags: -URG: Paquet urgent -PSH: N° de séquence significatif -RST: Réinitialisation connexion -SYN: Demande de connexion -FIN: Fin d'émission
FENÊTRE:	Largeur en octets de la fenêtre d'émission
CHECKSUM:	Somme en complément à 1 de tous les mots de 16 bits du paquet.
POINTEUR URGENT:	Validé par URG: nombre d'octets urgents dans DONNEES
OPTIONS:	Variable.
PAD:	Alignement sur un multiple de 32 bits.

Dans le but d'optimiser le trafic, TCP met en oeuvre un système d'acquittement par fenêtre, permettant d'émettre un certain nombre de paquets avant d'avoir reçu les acquittements des paquets précédents:



Fenêtre →
glissant en fonction des ack. reçus



MECANISME D'ACQUITTEMENT PAR FENETRE GLISSANTE

IV.5.2 LE PROTOCOLE UDP (USER DATAGRAM PROTOCOL):

IV.5.2.1 GENERALITES:

U.D.P. est un protocole de transport de données **non sécurisé** en mode **non connecté**. Il permet à des **processus**, pouvant appartenir à des hôtes différents d'un réseau étendu, d'échanger des messages constitués d'un seul paquet d'informations.

IV.5.2.2 SERVICES FOURNIS PAR UDP:

SECURITE:

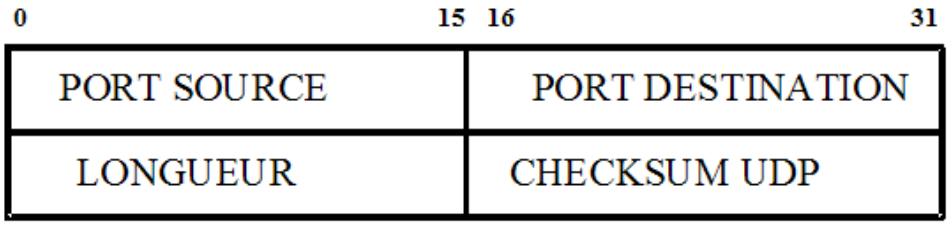
- UDP est un protocole non connecté: la synchronisation entre émetteur et récepteur n'est donc pas assurée. En particulier, la disparition du processus récepteur ne peut pas être détectée par l'émetteur.
- UDP est un protocole de type DATAGRAM, ce qui veut dire qu'il n'assure pas la sécurité des échanges. En particulier, les messages ne sont pas acquittés par le récepteur.
- UDP n'assure pas l'ordre d'arrivée des messages ni leur séquencement. Les messages sont donc limités à un seul paquet d'informations. En particulier, la taille d'un message sur un réseau éthernet BUS est limitée à celle d'un paquet Ethernet (1500 octets).

PERFORMANCES:

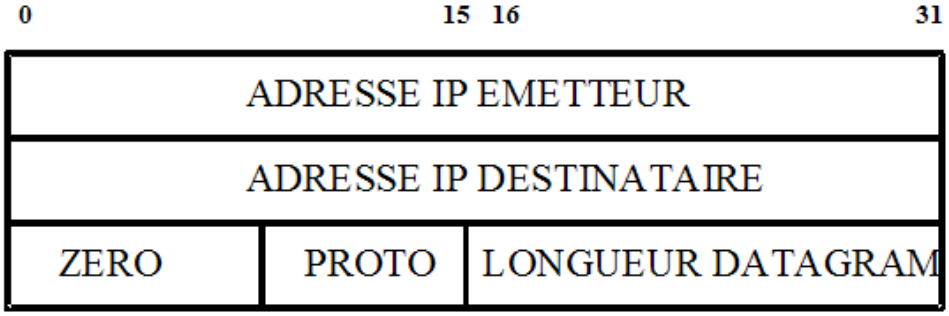
UDP ne bufferisant pas les messages à émettre, l'émission est donc immédiate. De ce fait, les dates d'émission et de réception sont plus déterministe que dans le cas d'une transmission TCP. UDP convient donc plutôt aux cas où la date d'acheminement est impérative, mais où la perte d'informations n'est pas rédhibitoire (par exemple, traitement de mesures en temps réel).

De ce fait, UDP est employé en sous-couche de nombreuses applications (NFS par exemple). En effet, pour des raisons de performance et de maîtrise des timings, on a parfois intérêt à ne pas utiliser les mécanismes TCP et à sécuriser les échanges au niveau de l'application.

IV.5.2.3 FORMAT DE L'EN-TÊTE UDP:



HEADER U.D.P.



PSEUDO-HEADER UDP (CALCUL DE LA CHECKSUM)

COMMENTAIRES:

PORT SOURCE:	Identificateur du processus émetteur
PORT DESTINATION:	Identification du processus récepteur
LONGUEUR:	Longueur du datagram UDP
PROTO:	Numéro du protocole supérieur (ici: UDP).
ZERO:	Octet nul

Le pseudo-header n'est pas transmis. Il est formé par la couche transport et ajouté au message UDP pour calculer le checksum avant de transmettre le paquet à la couche IP, puis il est éliminé. A la réception, il est reformé par la couche TCP et utilisé de la même manière pour vérifier la valeur du ckecksum reçu.

IV.6 PROTOCOLES DES COUCHES HAUTES DE L'I.S.O:

IV.6.1 INTRODUCTION:

La plupart des applications réseau courantes font directement appel aux services de là couche transport. Cette situation est largement dûe au quasi-monopole du standard TCP-IP, du moins pour les applications «grand public», et en particulier sur internet. En effet, le «modèle» TCP-IP ne distingue pas les mécanismes de session et de présentation de ceux de la couche application.

De ce fait, les protocoles que nous aborderons dans ce sous-chapitre se positionnent directement en dessus de la couche transport et encapsulent les mécanismes des couches 5 et 6 de l'ISO.

IV.6.2 LE PROTOCOLE HTTP:

IV.6.2.1 GENERALITES:

Le protocole H.T.T.P. (Hyper Text Transfer Protocol) est un protocole client-server essentiellement utilisé pour gérer le communication entre les navigateurs internet (clients HTTP) et les serveurs WEB (serveurs HTTP). Il tire son nom du fait que sa fonction principale est le téléchargement par le client de «pages web», sous formes de fichiers textes rédigés en HTML (Hyper Text Markup Langage). Dans le cas d'internet (et en fait, presque toujours), le protocole H.T.T.P s'appuie sur une couche transport implémentée par TCP. HTTP est une évolution du protocole FTP (File Transfer Protocole), spécialisée dans les transfert de fichiers HTLM.

IV.6.2.2 MECANISME DE HTTP:

HTTP permet au client (navigateur) d'accéder au contenu d'une ressource identifiée par son U.R.L. Une U.R.L (Universal ressource Locator) est l'adresse d'une ressource sur le web. Le mécanisme correspond à l'algorithme suivant:

- Le navigateur Web ouvre une connexion TCP sur le port 80 (par défaut) avec la machine hôte (donc le serveur HTTP).
- Il envoie au serveur une requête concernant une ressource indentifiée par son U.R.L.
- SI (la ressource existe) ALORS
  Le serveur traite cette requête (par exemple, il renvoie vers le navigateur la page web qu'il demande)
- SINON
  Il renvoie vers le navigateur un message d'erreur (ex: ressource inconnue)
- FINSI
- Le navigateur Web demande alors la fermeture de la connexion TCP.

REMARQUE:
Dans les dernières versions de HTTP, le navigateur peut envoyer plusieurs requètes dans une même connexion.

IV.6.2.3 LES REQUETES HTTP:

FORMAT GENERAL:

Une requète HTTP est un texte composé de 3 parties:

- ***Une ligne de requète:*** <Methode> < URL> < Version HTTP utilisée>
- ***Des Champs d'en-tête (facultatifs):*** Sous la forme: <nom de champ> : <description>
- ***Lignes vides*** Plusieurs lignes vides.....
- ***Un Corps de Requète:*** <suite de lignes optionnelles dont le contenu dépend de la méthode>

LES DIFFERENTES METHODES:

NOM DE METHODE	*FONCTION*
GET	Demande l'envoi par le serveur de la ressource localisée par l'URL (Ex: GET d'une page web)
POST	Envoie des données au programme (situé sur le serveur) spécifié par l'URL. Par exemple, des données saisies sur un formulaire HTML.
HEAD:	Demande l'envoi par le serveur de l'EN-TETE de la ressource localisée par l'URL.
PUT	Envoi de données à l'URL sélectionné (diffèrent de POST)
DELETE	Demande de destruction la ressource pointée par l'URL

EXEMPLE: Demande d'envoi de la page d'accueil du site lesite.net:

```
GET http://www.lesite.net HTTP/1.0
Accept : text/html
User-Agent : Mozilla/4.0
```

IV.6.2.4 LES REPONSES AUX REQUETES HTTP:

FORMAT GENERAL

La réponse à une requète HTTP se présente sous la forme d'un texte structuré de la manière suivante:

- ***Ligne de statut:*** <version protocole utilisé><code d'état><texte explicant la signification du code>
- ***Champs d'en-tête (facultatifs):*** Sous la forme: <nom de champ> : <description>
- ***Lignes vides*** Plusieurs lignes vides
- ***Corps de la réponse:*** Contenu de la ressource demandée

EXEMPLE: réponse à une requète GET n'ayant abouti qu'à un transfer partiel de la page web:

HTTP/1.0 203 PARTIAL INFORMATION
Date : Wed, 3 april 2009 16:20:12 GMT

IV.6.3 LE PROTOCOLE F.T.P:

IV.6.3.1 GENERALITES:

Le protocole F.T.P (File Transfert Protocol) est un protocole de transfert de fichiers. Dans le «modèle» TCP/IP, il se situe immédiatement au dessus de la couche transport. Ce protocole permet à un CLIENT FTP d'effectuer diverses opérations sur le système de fichiers du SERVEUR FTP, quels que soient les systèmes de fichiers des deux machines (par exemple, un client Windows et un serveur linux):

- Transfer de fichier du client au serveur et vice-versa.
- Suppression de fichiers à distance.
- Obtenention de la liste des fichiers d'un répertoire
- etc...

La connexion entre client et serveur est sécurisée par un mot de passe.

IV.6.3.2 MECANISME:

Une connexion FTP utilise 2 connexions TCP:

- ***Une connexion de contrôle*** initialisée par le client sur le port 21, et qui lui permet d'envoyer au serveur des requètes FTP (requètes de transfert, de suppression, etc..).
- ***Une connexion de transfer de données*** initialisée par le client ou le serveur

D'autre part, la connexion de données peut s'effectuer:

- ***En mode ACTIF:*** le client détermine le port et le transmet au serveur, qui initialise la connexion.
- ***En mode PASSIF:*** c'est le serveur qui choisit le numero de port, le transmet au client et c'est le client qui initialise la connexion.

Le transfert de fichiers peut se faire en 2 mode:

- ***Mode BINAIRE:*** le transfert se fait sans modification du contenu
- ***Mode ASCII:*** FTP considère que le fichier est un fichier texte ASCII. De ce fait, si on communique entre machine Linux et machine Windows, il fait les modification qu'il faut pour passer d'une représentation de texte à l'autre.

REMARQUES:

- Le mode actif fonctionne difficilement avec une passerelle NAT (Network Adress Translation).
- Il est indispensable d'utiliser le mode texte pour échanger des fichiers textes. En revanche, il ne faut surtout pas le faire pour d'autres fichiers, car ils risquent de subir des modification intempestives.

V COMMUNICATION INTER-RESEAUX:

V.1 PRINCIPE GENERAL:

Pour établir une interconnexion entre deux réseaux, il faut les relier par un noeud capable de transformer les trames issues de l'un d'eux de manière à les rendre d'une part transportables par le média de l'autre et d'autre part exploitables par ses hôtes. Ceci suppose que l'équipement d'interconnexion soit capable d'intervenir au niveau de toutes les couches OSI pour lesquelles il existe des différences entre les deux réseaux interconnectés.

Dans le cas extrême ou aucune des couches OSI du premier réseaux n'est compatible les couches correspondantes de l'autre réseau, le commutateur doit être capable de relayer les messages au niveau application. Il devra donc, pour chacune des connexions physiques, posséder toutes les couches réseau compatibles avec le réseau connecté:

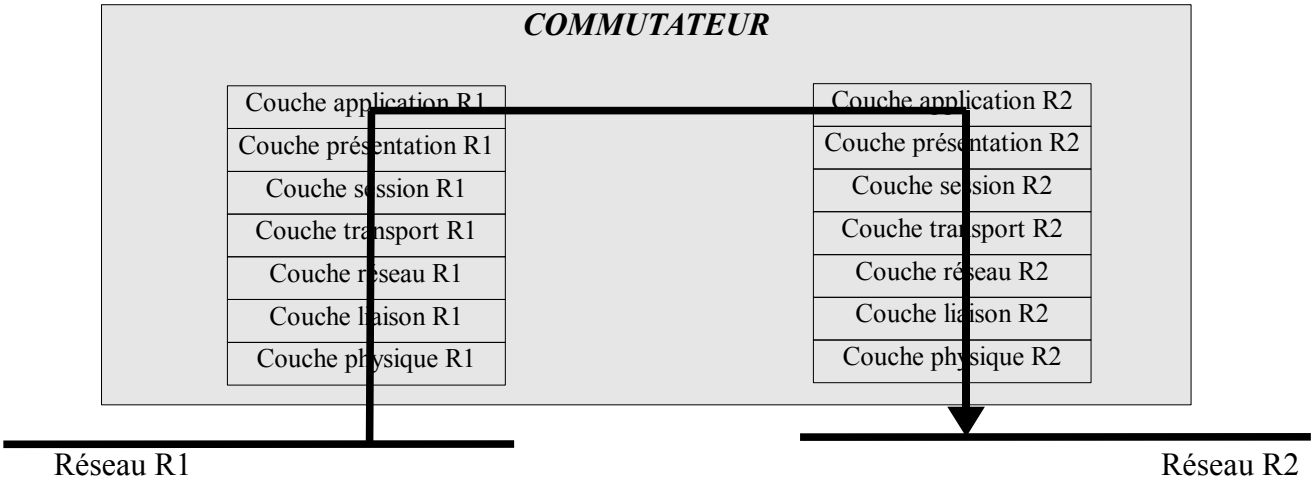


Schéma n° XXIV: Interconnexion de réseaux-problème général

Cependant, dans la plupart des cas, les différences se situent essentiellement dans les couches basses:

- Différences de nature du média (par exemple: R1 utilise la paire torsadée, R2 le câble coaxial)
- Différences de codage électrique (par exemple: R1 est codé en NRZI, R2 en Manchester)
- Différence dans les méthodes d'accès (R1 est un réseau éthernet, R2 un token ring)
- Etc.

En revanche, à partir de la couche réseau, on trouvera la plupart du temps les mêmes protocoles (suite TCP-IP). De ce fait, la plupart des organes d'interconnexion se situent au niveau des trois premières couches ISO.

EXEMPLE:

Supposons que R1 soit un réseau ethernet et R2 un réseau Token Ring, les couches 3 et 4 étant TCP-IP dans les deux cas:

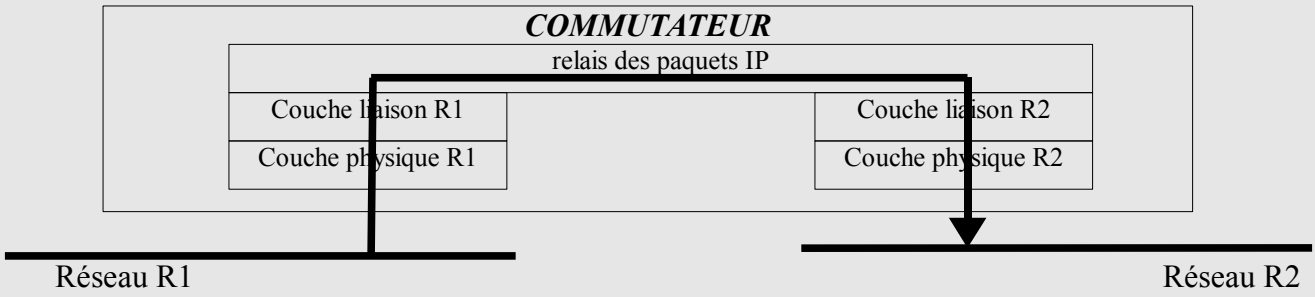


Schéma n° XXV: Interconnexion de réseaux couches basses

Dans ce cas, en dessus de la couche liaison, les P.D.Us sont des paquets IP qu'il suffit de relayer d'une connexion à l'autre.

D'une manière générale, le relais se fait au niveau où les P.D.U.s sont compatibles dans les deux réseaux.

V.2 LES EQUIPEMENTS D'INTERCONNEXION:

V.2.1 LES REPETEURS:

Un répéteur est un équipement capable de relayer une **trame physique** d'un réseau à un autre réseau. Ses seules fonctions sont:

- La régénération du signal
- L'adaptation du signal au média.

Il permet donc:

- De connecter deux réseaux identiques.
- De connecter deux segments d'un même réseau (afin de régénérer le signal).
- De passer d'un média à un autre (exmple: paire torsadée – coaxial)

Les répéreurs sont des relais qui se situent juste au dessus de la couche physique:

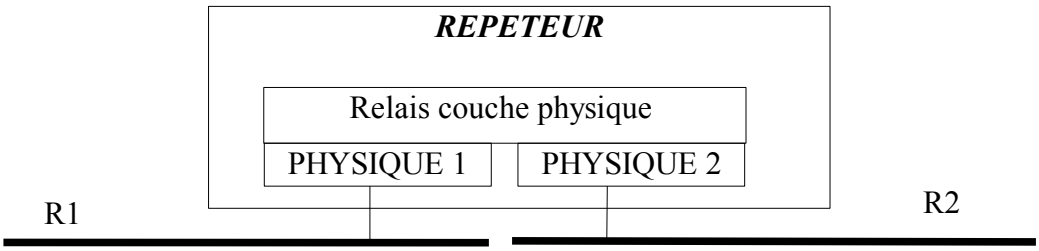


Schéma n° XXVI: Répéteur

V.2.2 LES CONCENTRATEURS (HUBs):

Un concentrateur (ou HUB) est un répéreur muni de plus de deux ports. Comme les répéteurs, les HUBs se contentent de relayer les trames reçues sur un port vers tous les autres ports, en régénérant le signal, et, le cas échéant, en l'adaptant au type de média correspondant au port. Un HUB peut donc offrir des ports d'interconnexion variés (port RJ45 pour paire torsadée, prise BNC pour câble coaxial, etc...).

Les HUBs permettent de relier entre eux plusieurs réseaux identiques (au média près) au plusieurs segments d'un même réseau (topologie en étoile passive):

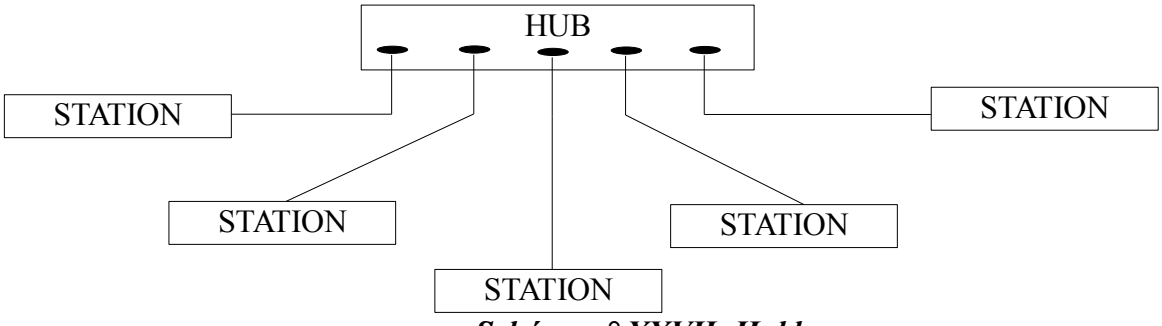


Schéma n° XXVII: Hubb

Les HUB peuvent être connectés en cascades (En général, jusqu'à 3 hubs):

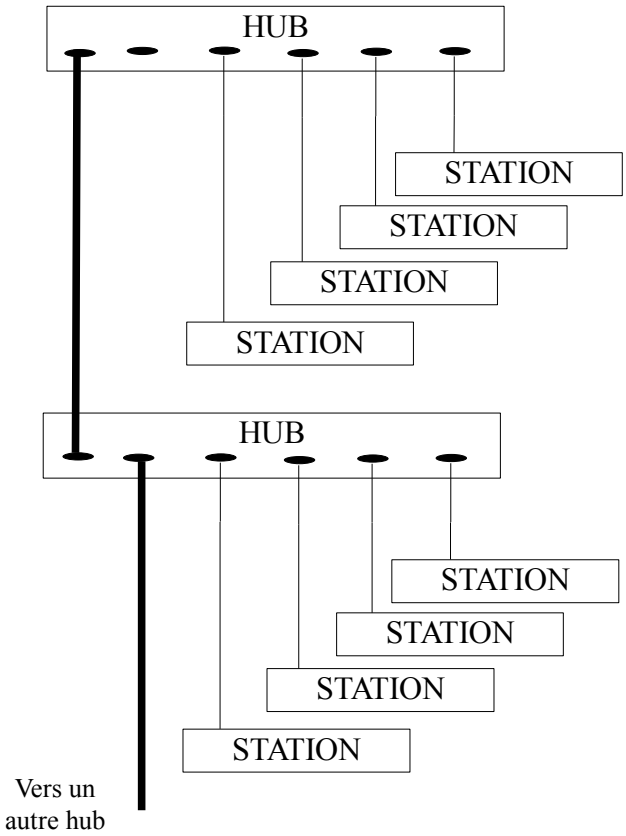


Schéma n° XXVIII: Hubbs en cascade

V.2.3 LES PONTS:

Les ponts (BRIDGES) sont des relais qui se situe juste au dessus de la couche MAC:

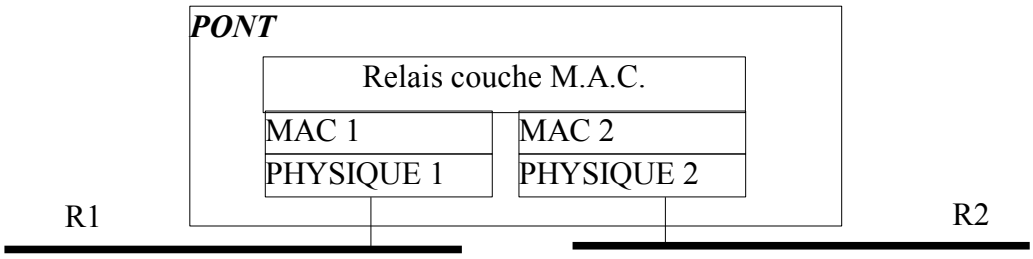


Schéma n° XXIX: Les ponts

De ce fait, ils permettent de relier entre eux des réseaux dont les technogies et protocoles de la couche physique et de la sous-couche MAC sont différents (par exemple, un éthernet et un token ring), mais dont les protocoles de niveau supérieurs sont identiques.

FONCTIONNEMENT:

Un pont est doté d'une fonction d'apprentissage des adresses MAC connectées à ses différents ports. Lorsqu'un pont reçoit sur un de ses ports une trame, il vérifie si l'adresse MAC du destinataire correspond à un port différent du port de réception. Dans l'affirmative, il transmet la trame à ce port. Dans la négative, il ne fait rien.

De plus, le logiciel embarqué des ponts permet d'offrir un certain nombre de services de traitement des flux:

- Possibilité de filtrage et blocage des trames (également basées sur les adresses MAC).
- Gestion de collisions
- ***Spaning tree:*** protocole B.P.D.U. de communication entre ponts permettant, en cas de défaillance d'un pont de trouver une autre chemin

V.2.4 LES COMMUTATEURS (SWITCHES):

Les commutateurs sont également des relais de la couche MAC. Cependant, ils possèdent des fonctions plus élaborées:

- Chaque port permet une liaison en full duplex, ce qui évite toute collision entre paire émettrice et réceptrice. Le flus est donc doublé.
- Les fonctions de filtrage sont plus élaborées (en particulier, les protocoles de niveau supérieur peuvent être analysés).
- Ils permet la définition de réseaux locaux virtuels (VLAN: Virtual Local Area Network). Un réseau virtuel est un groupe de ports isolés des autres. Cette capacité permet de définir plusieurs réseaux (virtuels) d'adressage couche 3 différents sur le même switch.

V.2.5 LES ROUTEURS:

Ils se situent au niveau de la couche 3 de l'O.S.I. (couche réseau). Ils permettent de relayer des paquets entre réseaux dont les technologies et protocoles

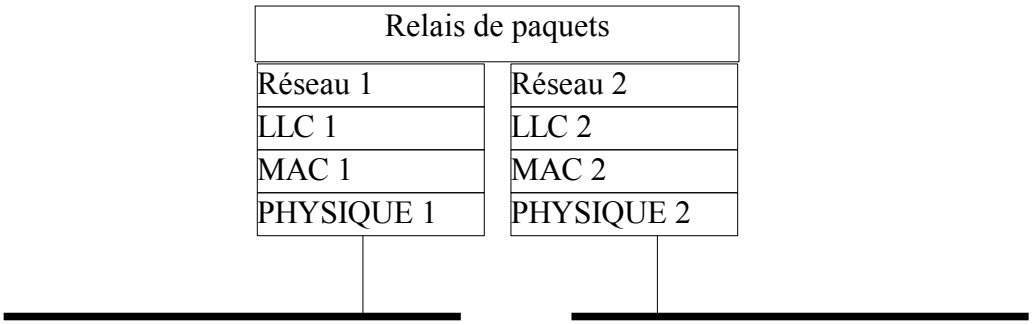


Schéma n° XXX: Les routeurs

- Travaillent sur les adresse IP (et non plus sur les adresses physiques)
- Permettent de relier des réseaux logiques (d'adresse IP différente)
- Multi protocoles (protocoles couches réseau et supérieures, sauf NETBEUI
- Multi interfaces (Ethernet, token ring, ATM...).

Remarque: les messages broadcasts IP ne passent pas les ponts (donc, ARP ne passe pas).

Les ROUTEURS permettent le routage au niveau IP. Le schéma suivant représente le mécanisme de routage des messages:

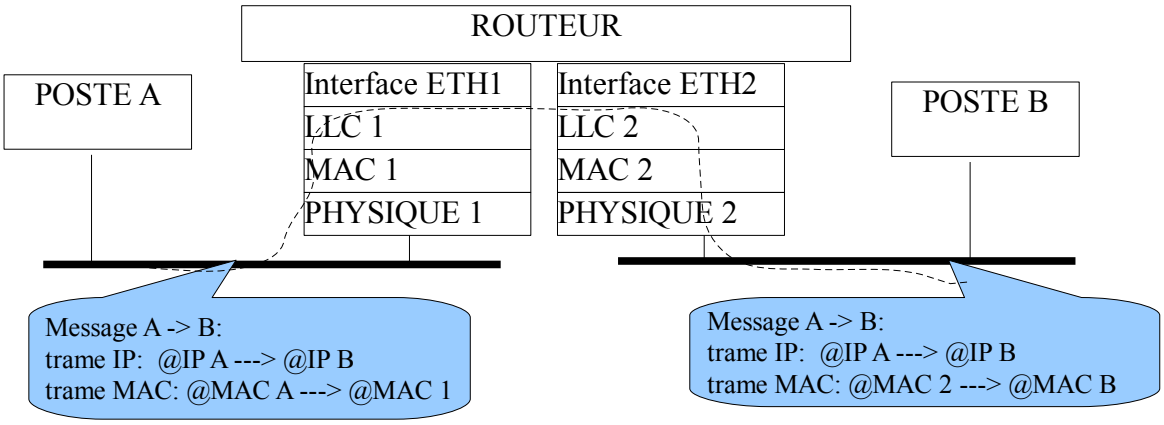


Schéma n° XXXI: Mecanisme de routage

Le mécanisme est basé sur l'existance dans le routeur d'une TABLE DE ROUTAGE. Cette table permet de mémoriser pour chaque adresse IP reçue par le routeur l'adresse MAC correspondante sur l'un ou l'autre des réseaux connectés au routeur. Au démarrage du routeur, celui-ci expédie sur chacun des réseaux qui lui sont connectés une requète du protocole A.R.P (Adress Resolution Protocole) demandant à chaque hôte de lui fournir son adresse IP est son adresse MAC. Avec les réponses obtenues, le routeur construit sa table de routage:

TABLE DE ROUTAGE	
Adresse IP	***Adresse MAC correspondante***
192.42.173.01	90.72.56.48.42.78
192.42.173.02	123.27.79.52.66.12
192.43.113.01	190.01.17.34.56.77
Etc....	

Par la suite, supposons que A veuille communiquer avec l'hôte B, situé sur un réseau différent:

- Le poste A émet un message vers le poste B, situé sur un réseau local interconnecté au sien par un pont routeur. L'enveloppe IP de ce message contient l'adresse IP de B, mais comme A ne connaît pas l'adresse MAC du destinataire, il place dans l'enveloppe MAC, à l'emplacement de l'adresse MAC de celui-ci, celle de la connexion du pont routeur avec le réseau de A. Le message est donc dirigé vers le pont.
- Le pont routeur récupère ce message. Il regarde dans la table de routage quelle adresse MAC correspond à l'adresse IP du destinataire (si cette adresse IP n'y figure pas, le routeur renvoie une requète ARP pour réactualiser sa table de routage).
- Lorsqu'il a pu obtenir l'adresse MAC du destinataire, le pont routeur place celle-ci dans l'enveloppe MAC du message, à l'emplacement de l'adresse du destinataire, puis réexpédie ce message sur le réseau de celui-ci.
- Si l'adresse MAC reste introuvable, le routeur renvoie un message d'erreur à l'émetteur.

V.2.6 LES ROUTEUR D'AGENCE:

Ceux-ci se placent au niveau 3 de l'OSI comme les routeurs classiques. Leur caractéristique principale est qu'ils permettent d'interconnecter des réseau locaux distants géographiquement (des agences d'une même entreprise, par exemple), par l'intermédiaire d'infrastructures publiques comme internet ADSL, RNIS, X25, etc:

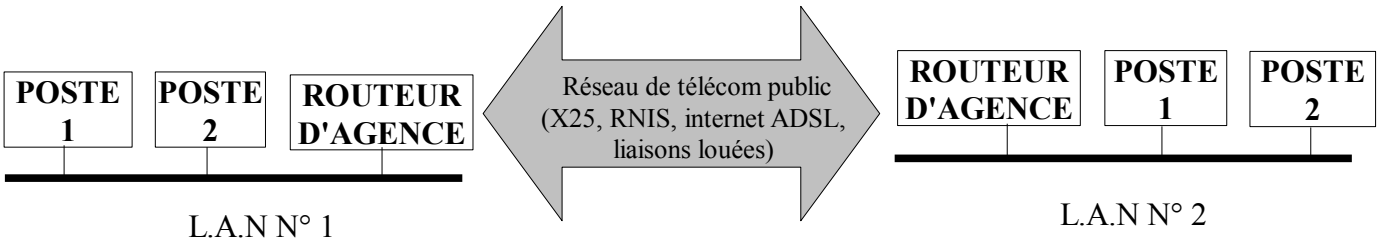


Schéma n° XXXII: interconnexion de deux LAN distants par une infrastructure publique

VI ANNEXES:

VI.1 STRUCTURE D'UNE TRAME ETHERNET:

OCTETS	*FONCTION*
1 à 8	Préambule: permet de synchroniser 2 stations en occupant le média avant d'émettre
9 à 14	Adresse ethernet du destinataire
15 à 20	Adresse ethernet de l'émetteur
21 à 22	Longueur du champ "Données"
23 à 23+n-1	Données encapsulées par les couches supérieures (taille mini=46 octets)
23+n à 23+n+3	FCS: Frame Check Sequence est un CRC permettant de détecter les erreurs de transmission

REMARQUE:

La technique de détection des collisions impose, dans les conditions de débit et de vitesse de propagation imposées par la structure physique, de limiter la longueur d'une trame ethernet à 1500 octets. Cette longueur est donc la taille limite d'un paquet (PDU) dans un réseau de ce type.

VI.2 ADRESSAGE IP:

VI.2.1 RAPPELS SUR LES NOTATIONS BINAIRES ET HEXADECIMALES:

VI.2.1.1 REPRESENTATION EN BASE 2 (VALEUR NUMERIQUE D'UN OCTET):

Un octet (configuration binaire de 8 bits) peut représenter des valeurs décimales de 0 à 255:

N° bit	Bit 0: 2^7	Bit 1: 2^6	Bit 2: 2^5	Bit 3: 2^4	Bit 4: 2^3	Bit 5: 2^2	Bit 6: 2^1	Bit 7: 2^0
Valeur décimale	128	64	32	16	8	4	2	1
exemple	1	0	1	1	0	0	0	1

EXEMPLES:

- L'octet: 101100012 en binaire est égal à: 128+32+16+1 = 17710 en décimal
- L'octet: 111111112 en binaire est égal à: 128+64+32+16+8+4+2+1 = 25510 en décimal

VI.2.1.2 REPRESENTATION EN BASE 16 (HEXADECIMAL):

La représentation hexadécimale utilise 16 chiffres de 0 à 15, et notés: 0, 1, 2, 3, 4 , 5, 6, 7, 8, 9, A(=10), B(=11), C(=12), D(=13), E(=14), F(=15). Pour les distinguer des nombres décimaux, on fait précéder les nombres hexadécimaux du préfixe «0x». Ainsi, en hexadécimal, le nombre 0x4A3 représente la valeur décimale $16^2*4 + 16*B + 3$, et comme B = 11:

0x4A3 = $16^2*4 + 16*B + 3 = 16^2*4 + 16*11 + 3$ = 1203 en décimal

Pour convertir un octet de binaire en hexadécimal, il suffit de le séparer en 2 groupes de 4 octets, chacun représentant un chiffre hexadécimal:

EXEMPLE: octet de valeur décimale 196:

196 = 128 + 64 + 4 = 1100 0100 en binaire
1100 en binaire = C en hexadécimal et 0100 en binaire = 4 en hexadécimal
Donc: 196 en décimal s'écrit 1100 0100 en binaire et 0xC4 en hexadécimal.

VI.2.2 REPRESENTATION DES ADRESSE IP (IPV4):

Un adresse IP (Ipv4) est codée sur 4 octets (soit 32 bits). La valeur d'une adresse IP peut être écrite:

- Soit sous forme de 4 valeurs décimales séparées par des points: 196.68.43.21
- Soit sous forme d'un nombre de 8 chiffres hexadécimaux: 0xC44A2B15

VI.2.3 CLASSES D'ADRESSES IP:

Les adresses IP sont partagés en 4 classes d'adressage, les classes A, B et C, plus des adresses «spéciales»

VI.2.3.1 RECONNAISSANCE DE LA CLASSE:

La valeur des 3 premiers bits du 1er octet permettent de déterminer la classe d'adresse:

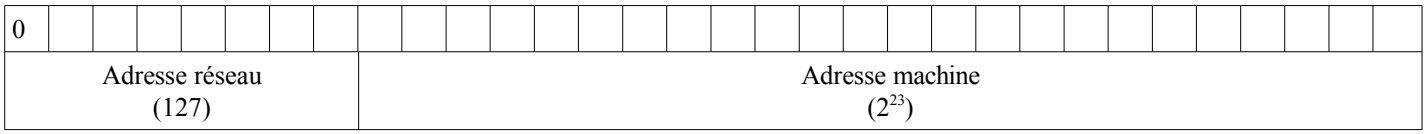
- Classe A = le premier bit est à 0 (donc, valeur du premier octet < 138)
- Classe B = le premier bit est à 1, le deuxième est à 0 (donc, 128<= valeur 1er octet < 192)
- Classe C = les 2 premier bits sont à 1, le 3eme est à 0 (donc, 192<= valeur 1er octet < 224)
- Valeurs premier octet supérieures ou égales à 224 (3 premiers bits à 1): Adressage spécial (groupes multicast, broadcast..)

De plus:

- Si le 1er octet vaut 127, l'adresse est celle de la BOUCLE LOCALE
- Si le 1er octet vaut 256 (111111112), on a affaire à une adresse BROADCAST

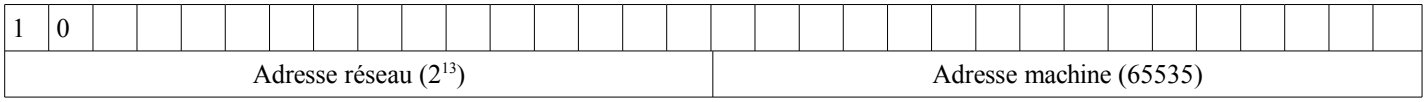
VI.2.3.2 FORMAT DE CHAQUE CLASSE:

CLASSE A:



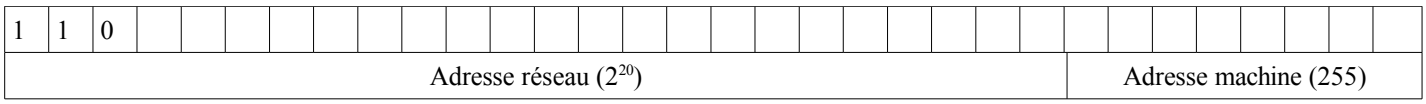
Adresses réseau de **1.**0.0.0 à **126**.255.255.255 (127 réservé pour boucle locale)
Masque: 255.0.0.0 ou 0XFF000000

CLASSE B:



Adresses réseau de **128.0**.0.0 à **191.255**.255.255
Masque: 255.255.0.0 ou 0XFFFF0000

CLASSE C:



Adresses réseau de **192.0.0**.0 à **223.255.255**.255
Masque: 255.255.255.0 ou 0XFFFFFF00

VI.2.4 LES MASQUES IP:

Un masque permet de récupérer dans une adresse IP tous les bits relatifs à l'adresse du réseau (en éliminant l'adresse machine), en faisant une opération ET (intersection de 2 nombres binaires):

RAPPEL : intersection bit à bit:
0 et 0 = 0
1 et 0 = 0
0 et 1 = 0
1 et 1 = 1

Ex: Adresse ip 192.68.43.21 (0xC4442B15) = 11000000 01000100 00101011 00010101
Cette adresse est de classe C (premier octet >= 192 => bits 0 et 1 à 1, bit 2 à 0)
Masque classe C = 255.255.255.0 = 11111111 11111111 11111111 00000000

Intersection masque – adresse:

```
              11000000 01000100 00101011 00010101
        Et    11111111 11111111 11111111 00000000
              11000000 01000100 00101011 00000000
```

`11000000 01000100 00101011 00000000 = **192.68.43.00**`
On obtient bien l'adresse réseau.

VI.2.5 MASQUES DE SOUS-RESEAUX:

Pour créer des sous-réseaux, il suffit, dans le masque de la classe, d'ajouter aux bits de la partie «adresse réseau» des bits de la partie «hôte» (machine).

EXEMPLE:
masque de classe 3:
`11111111 11111111 11111111 00000000` (255.255.255.0)
on ajoute 2 bits au masque:
`11111111 11111111 11111111 **11**000000` (255.255.255.192)

En fait, on ne peut pas ajouter un seul bit, car certains équipements ne le tolèrent pas. On ajoute donc au moins 2 bits.

A ce moment là, les machines qui ont une adresse inférieure à 192 seront sur un sous réseau, les machines dont l'adresse et supérieure ou égale à 192 seront sur un autre sous-réseau: on a crée 2 sous-réseaux.

EXEMPLES:
Machine d'adresse 12:

```
11000000 01000100 00101011 00001100  (192.68.43.12)
11111111 11111111 11111111 10000000
11000000 01000100 00101011 00000000
```

La machine 12 est sur le sous-réseau 192.68.43.0

Machine d'adresse 195:

```
11000000 01000100 00101011 11000101  (192.68.43.195)
11111111 11111111 11111111 11000000
11000000 01000100 00101011 11000000
```

La machine 130 est sur le sous-réseau 192.68.43.192

REMARQUE:

En théorie, la machine d'adresse 65 par exemple devrait se trouver sur un 3 eme réseau:

Machine d'adresse 65:

```
11000000 01000100 00101011 01000001  (192.68.43.65)
11111111 11111111 11111111 11000000
11000000 01000100 00101011 01000000
```

La machine 65 devrait donc se trouver sur le sous-réseau 192.68.43.64.

En fait, avec 2 bits, on ne crée que 2 sous réseaux, car les bits de masques supplémentaires 10 et 01 sont souvent traites comme les bits de masque supplémentaires 00 et de ce fait, la machine 65 est sur le réseau 192.68.43.00, comme toutes les machines d'adresse inférieure à 192

De ce fait:

- avec 2 bits on fait jusqu'à 2 sous-réseaux,
- avec 3 bits on fait jusqu'à 6 sous-réseaux,
- avec 4 bits on fait jusqu'à 14 sous-réseaux,
- Etc...

Avec N bits, on fait 2N-2 **sous-réseaux (Ex: 3 bits => 23-2 = 8-2 = 6).**

VI.2.6 NOTATION DES MASQUES DE SOUS-RESEAUX:

Une notation simplifiée du masque de sous-reseau associé à un réseau consiste à ajouter à la fin de l'adresse IP de réseau le nombre de bits du masque:

EXEMPLE:

194.25.12.00/26 signifie que le masque a 26 bits (2 bits supplémentaires par rapport au masque de classe c) Ce masque est donc: 255.255.255.192

VI.3 ETABLISSEMENT D'UNE CONNEXION TCP:

HOTE A		HOTE B
CLOSED		LISTEN
SYN-SEND	1- Bit SYN positionné N° séquence = m →	SYN-RECEIVED
ESTABLISHED	2- ACK m+1, Bit SYN et ACK positionnés, n° sequence n ←	SYN-RECEIVED
ESTABLISHED	3- ACK n+1, Bits ACK →	ESTABLISHED
ESTABLISHED	4- Envoi des données →	ESTABLISHED

- L'Hôte A (client) est à l'état «connexion CLOSED». L'Hôte B (serveur) est à l'état LISTEN (Il écoutesi un client veut se connecter)
- 1-Le client envoie au serveur une demande de connexion (SYN) accompagnée d'un numero de séquence.
- 2-A reception du SYN, le serveur passe à l'état SYN-RECEIVED (demande de connexion en cours). Il renvoie au client les bits SYN et ACK accompagnés du numéro de séquence client augmenté de 1 et de son propre n° de séquence.
- 3-A réception du message, le client passe à l'état ESTABLISHED (connexion établie). Puis il renvoie le bit ACK accompagné du N° séquence serveur augmenté de 1.
- A réception, le serveur passe aussi à l'état ESTABLISHED

La connexion est maintenant établie. Le client peut émettre ses données. Les numéros de séquence permettent de s'assurer qu'aucun message n'est perdu.