République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Dr. Tahar Moulay de Saida
Faculté de Technologie

Département Informatique

Support de cours du module : Réseaux Informatiques

Réalisé par : Dr. Fadia TALEB

Année universitaire : 2017-2018

Avant-propos

Ce cours vise à donner aux étudiants de master des universités un certain nombre de bases et de notions sur les réseaux informatiques. Pour l'élaboration de ce cours nous nous sommes basé principalement sur de nombreux cours de Cisco Networking Academy, leader modial de la technologie de l'information et des réseaux, ainsi que quelques autres livres disponibles en bibliothèque. Afin de limiter les prérequis nécessaires à la compréhension de ce cours, nous avons pensé à expliquer tout ce qui a pu être mentionné. Quelques exemples concrets sont aussi présentés afin d'aider les étudiants à mieux comprendre et acquérir les notions.

Mis à part les deux premiers chapitres, qui donnent des notions de base sur les réseaux informatiques (terminologies, organisation des couches du modèle OSI et TCP/IP), l'organisation du reste des chapitres suit le cheminement logique d'un processus d'encapsulation des données à transmettre (passage par la couche réseau, couche liaison de données puis couche physique).

J'invite le lecteur qui aurait des questions liées au sujet du cours de m'en faire part à l'adresse mail suivante : taleb.fadia@gmail.com

Table des matières

Table des figures

Liste des symboles

Paramètres :

$Q(x)$: polynôme générateur de coéfficients $a_r...a_0$.

$P(x)$: polynôme associé aux données binaires à transmettre $b_0...b$.

$R(x)$: polynôme reste de la division Euclidienne de coéfficients $c_r...c_0$.

r : ordre de $Q(x)$.

Sigles et abréviations :

LAN : Local Area Network.

MAN : Metropolitan Area Network.

WAN : Wide Area Network.

MAC : Media Access Control

OSI : Open Systems Interconnection.

IEEE : Institute of Electrical and Electronics Engineers.

TIA : Telecommunications Industry Association.

EIA : Electronic Industries Alliance.

ITU : International Telecommunication Union.

FDDI : Fiber Distributed Data Interface.

RNIS : Réseau Numérique à Intégration de Services.

DSL : Digital Subscriber Line.

RPC : Remote Procedure Call.

ISO : International Organization for Standardization.

TCP : Transmission Control Protocol.

UDP : User Datagram Protocol.

IP : Internet Protocol.

LLC : Logical Link Control.

ROM : Read Only Memory.

RAM : Random Access Memory.

PDU : Protocol Data Unit.

HTTP : Hypertext Transfer Protocol.

SMTP : Simple Mail Transfer Protocol.

DNS : Domain Name Server.

TFTP : Trivial File Transfer Protocol.

FTP : File Transfer Protocol.

IGRP : Interior Gateway Routing Protocol.

EIGRP : Enhanced Interior Gate-way Routing Protocol.

OSPF : Open Shortest Path First.

EGP : Exterior Gateway Protocol.

RIP : Routing Information Protocol.

TEB : Taux d'erreur Binaire.

CPU : Central Processing Unit.

LLC : Logical Link Control.

FCS : Frame Check Sequence.

ACK : ACKnowledged.

CRC : Code de Redondance Cyclique.

CSMA/CD : Carrier Sense Multiple Access/Collision Detection.

ARP : Address Resolution Protocol.

ASCII : American Standard Code for Information Interchange.

VRC : Vertical Redundancy Check.

LRC : Longitudinal Redundancy Check.

CNA : Convertisseur Numérique Analogique.

CAN : Convertisseur Analogique Numérique.

NRZ : Non Return to Zero.

NRZI : Non Return to Zero Inverted.

ASK : Amplitude Shift Keying.

FSK : Frequency Shift Keying.

PSK : Phase Shift Keying.

TDMA : Time Division Multiple Access.

FDMA : Frequency Division Multiple Access.

CDMA : Code Division Multiple Access.

Introduction générale

Le concept de réseau est né de la nécessité de faire communiquer les utilisateurs entre eux à des fins bien spéci

ques (permettre le partage des ressources, échange de données, accès à des services distants...). Le besoin grandissant des utilisateurs a poussé les réseaux informatiques à grandir et à se développer. Cette évolution est en bonne partie liée aux techniques et aux supports de communication utilisés. Les technologies actuelles permettent aussi de transmettre des trafics de données plus volumineux et à plus grande vitesse tout en réduisant les coûts. Un bon nombre des technologies est abordé dans ce cours. Il est organisé comme suit :

Chapitre 1 : " Vue d' ensemble et terminologies". Présente aux étudiants les différents dispositifs physiques pouvant être utilisés dans un réseau ainsi qu'un bon nombre de terminologies servant à mieux comprendre les chapitres suivants.

Chapitre 2 : " Modèle OSI et TCP/IP". Description des couches du modèle de protocole OSI et expliquer les liens entre couches OSI et TCP/IP.

Chapitre 3 : " Les concepts de base du routage". Ce chapitre présente les principes couramment utilisés dans les différents protocoles de routage.

Chapitre 4 : " Technologie Ethernet". Ce chapitre explique les principes de base de la technologie de réseau local dominante mondialement. Nous donnons en détail le format de base des trames Ethernet et nous prenons un exemple concret d'échange de trame Ethernet entre deux ordinateurs.

Chapitre 5 : "Transmission du signal". Nous abordons au cours de ce chapitre les différentes techniques utilisées au niveau de la couche physique afin d' adapter le signal à transmettre au support de transmission.

Chapitre 1

Vue d'ensemble et terminologies

I Introduction

Un réseau est un ensemble d'équipements connectés afin de réaliser des tâches bien précises (échange de fichiers, partage de ressources...).

Au milieu des années 80, les réseaux présentaient un problème d'incompatibilité. Une des premières solutions a été d'élaborer des normes de réseau de petite taille (LAN). Quelques temps après ces réseaux se sont avérés insuffisants et des réseaux plus grands ont été crées (MAN et WAN).

Un équipement est tout matériel pouvant être connecté à un segment du réseau. Deux catégories d'équipement éxistent :

- Equipements d'utilisateur final ou hôte : fournissent des services à l'utilisateur. Nous citons les ordinateurs, scanneurs, imprimantes...etc.

- Equipements de réseau : representent tous les équipements qui servent à connecter les équipements d'utilisateurs entre eux afin de leur permettre de communiquer. Nous citons les répéteurs, les concentrateurs, les ponts, les switches...etc.

Un équipement hôte est relié au média grâce à un adaptateur réseau (carte réseau). Tous ces équipements [1] seront plus détaillés au cours de ce chapitre et nous évoquerons aussi quelques notions de base [1] qui vont

nous permettre de mieux comprendre les chapitres qui suivent.

II Équipements de réseau

II.1 Répéteurs

Un répéteur est un équipement réseau qui possède généralement deux ports, il reçoit un signal sur le port d' entrée, le régénère et le transmet vers le port de sortie. Cela permet aux signaux de voyager sur de plus longues distances à travers le média. La règle 5-4-3 stipule qu'entre deux noeuds du réseau, on ne peut avoir que cinq segments aux maximum reliés grâce à quatre répéteurs. Trois de ces segments peuvent contenir des connexions utilisateur.

II.2 Concentrateurs

Un concentrateur ou Hub est considéré comme un répéteur multiport. En effet, un concentrateur a la même fonction qu'un répéteur à la différence qu'il possède entre 4 et 24 ports. Les données qui arrivent sur le port d'entrée sont répétées sur tous les ports de sortie. De cette manière, tous les équipements raccordés au concentrateurs reçoivent toutes les données qui y transitent. Ce type d'équipement permet de changer de topologie. Une topologie en bus laisse place à une topologie en étoile.

Il existe trois types de concentrateurs :

Passif

Un concentrateur passif parmet uniquement de partager le média. Il ne permet ni de visualiser le trafic, ni de le nettoyer, ni de l'amplifier. Ce type d'équipement n'a pas besoin d'une alimentation éléctrique.

Actif

Ce type de concentrateur permet d'amplifier le signal reçu et le transmet vers tous les ports de sortie connectés. Il nécéssite donc une alimentation éléctrique.

Intelligent

Ils ont un fonctionnement similaire à celui des concentrateurs actifs. Ils possèdent un microprocesseur et des fonctions de diagnostic qui les rendent plus efficaces dans les dépannages.

Les répéteurs et les concentrateurs sont des équipements de la couche physique, par conséquent, ils ne lisent pas les adresses physiques de la couche liaison de données.

II.3 Ponts

Un pont ou un bridge est un équipement qui sert a diviser un réseau LAN de taille importante en de plus petits réseaux ou segments. Un pont classique possède deux ports qui permettent de relier deux segments du réseau. A condition de le placer de manière stratégique, cet équipement améliore nettement les performances du réseau et facilite sa gestion, en effet gérer des segments de petites tailles est bien plus facile que de gérer un réseau de grande taille. Il permet aussi de diminuer le trafic, grâce aux décisions intelligentes qu'il doit prendre : "transmettre ou pas des données au segments suivant auquel il est relié".

Cet équipement se situe au niveau de la couche liaison de données du modèle OSI. En fonction de l'adresse MAC de la trame à transmettre, il détermine l'opération qu'il doit effectuer et qui correspond à l'une des trois opérations suivantes :

Filtrage : si l'équipement de destination se trouve au niveau du même segment que l'équipement source, le pont ne transmet pas la trame au segment suivant.

Diffusion : si le pont ignore l'adresse de destination, il diffuse la trame à tous les segments qui lui sont reliés.

Si l'équipement de destination se trouve au niveau d'un autre segment, le pont transmet la trame au segment approprié.

La figure 1-1 montre des icones représentatives des équipements réseaux cisco.

II.4 Commutateurs

Un commutateur ou switch est aussi un équipement de la couche 2, il est considéré comme un pont multiport. En effet, cet équipement comporte plusieurs ports, suivant le nombre de segments qu'il doit relier. Cet

FIG. 1-1 –Représentation des équipements réseaux. (a) répéteur, (b) concentrateur, (c) pont, (d) commutateur, (e) routeur.

équipement réalise principalement deux fonctions : commutation des trames et la gestion des fonctions de commutation. La première fonction correspond à l'acheminement des trames qui arrivent sur un média d'entrée vers un autre média de sortie. La seconde fonction représente la constitution des tables de commutation qui aident à la commutation. En utilisant les informations contenues dans les trames qu'il reçoit, un commutateur constitue une table de commutation qui va lui servir à sélectionner le port auquel est connecté l'équipement de destination (Figure 1-2).

Un commutateur permet d'allier les fonctions de connectivité d'un concentrateur et de régulation de trafic d'un pont et donc par conséquent, il permet de réduire la congestion dans les réseaux locaux.

II.5 Routeur

Un routeur est un équipement de couche 3 du modèle OSI. C'est un dispositif qui véhiculent les données sur le réseau vers leur destinataire en fonction des adresses logiques. Les données qui sont destinées à un ordinateur se situant sur le même réseau local ne franchissent pas le routeur. Les données qui sont destinées à un ordinateur qui se situe sur un réseau extérieur au réseau local vont être envoyées au routeur qui se chargera de leur acheminement. Le mécanisme de routage sera traité plus bas au niveau du chapitre 3.

III Domaine de collision (collision domain) et de diffusion (Broadcast domain)

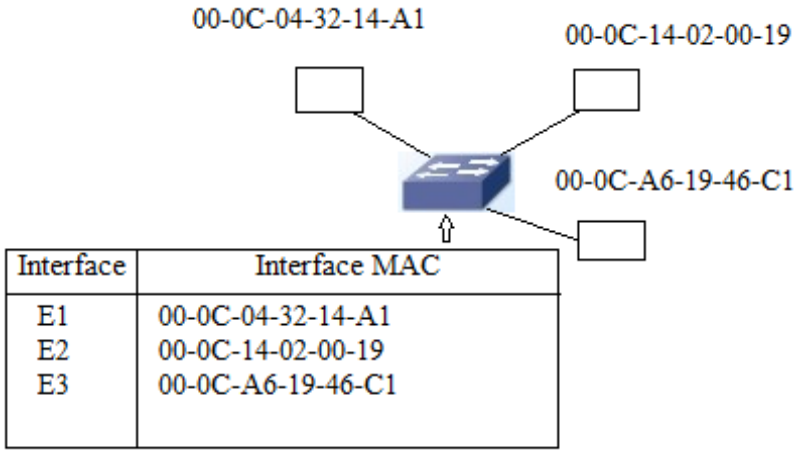


FIG. 1-2 – Table de commutation.

On parle de domaine de collision pour décrire un ensemble d' équipements informatiques (ordinateurs, imprimantes, serveurs...) connectés à un équipement central, dépourvu d'intelligence (concentrateur ou Hub en anglais). Toutes les données envoyés par un équipement arriveront à l'équipement central puis seront envoyées vers tous les autres équipements sans exception. Un réseau où se produit beaucoup de collision a des effets négatifs sur le bon fonctionnement de ce réseau. La segmentation consiste à diviser le domaine de collision en des domaines de collisions plus petits en rajoutant un équipement intelligent (commutateur 'switch' et pont 'bridge').

Pour expliquer le domaine de diffusion ou de broadcast, rappelons qu'une entité réseau peut transmettre des données en unicast, en multicast ou en broadcast. Supposons que nous sommes dans le cas d' une transmission en broadcast. Si les données transmises traversent un Hub, un pont ou un switch, elles seront diffusées sur tous les ports de ces équipements étant donnée que le Hub est incapable de filter les données reçues et qu'un pont et un switch diffuserons les données reçues si l'adresse de destination est une adresse de broadcast(FF :FF :FF :FF :FF :FF). L'utilisation d' un routeur va par contre exploser le domaine de diffusion,

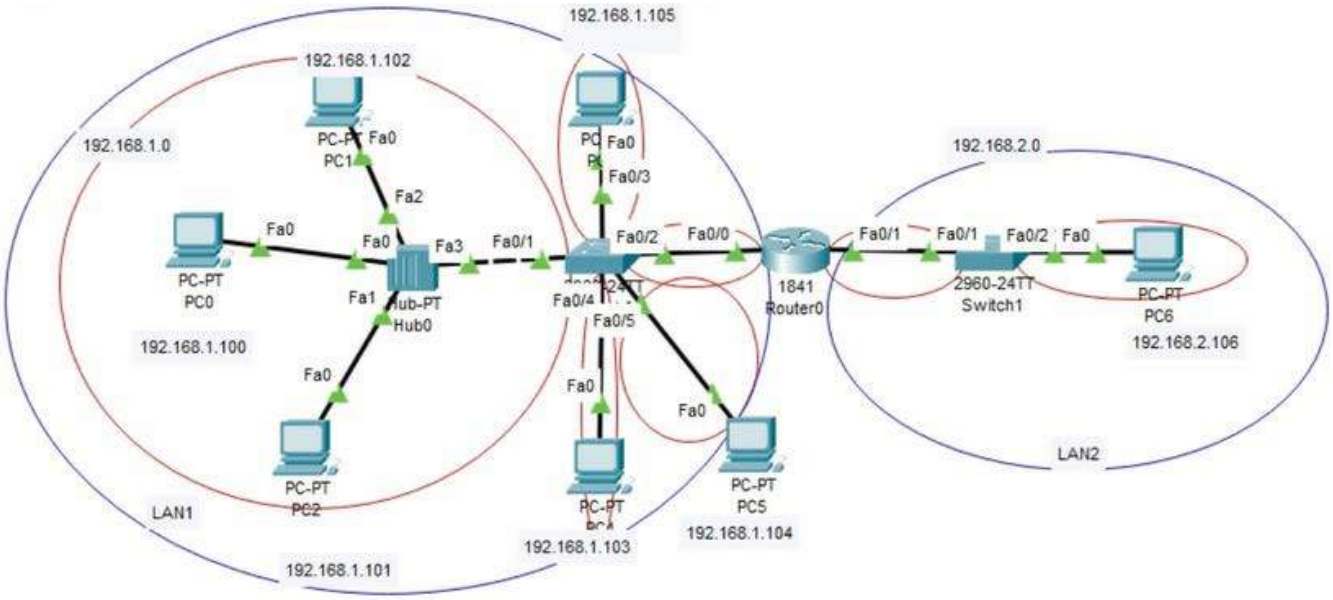


FIG. 1-3 – Domaine de collision.

puisque cet équipement est incapable de lire les adresses physiques (MAC) et ne transmettra pas les données en broadcast par conséquent.

IV Topologie de réseau

La topologie d'un réseau est définie par deux types de topologies ; la topologie physique, qui représente la façon avec laquelle les équipements sont interconnectés et donc la configuration réelle du câblage. Nous avons plusieurs topologies physiques (Figure 1-4) :

- Topologie en bus : où tous les hôtes sont reliés à un seul câble terminé aux deux extrémités et appelé backbone.
- Topologie en anneau : où chaque hôte est relié à son voisin, le premier et le dernier hôte sont reliés ensemble afin de créer un anneau physique.
- Topologie en étoile : tous les hôtes sont reliés à un équipement central.
- Topologie en étoile étendue : permet d'étendre le réseau par rapport à la topologie en étoile simple. L'équipement central du réseau étendu est reliés aux équipements centraux appartenant à d'autres étoiles individuelles. La topologie hiérarchique est pratiquement semblable, la seule différence est que l'équipement central de l'étoile étendue est cette fois-ci un ordinateur chargé de contrôler le trafic.
- Topologie maillée : chaque hôte du réseau est connecté à tous les autres hôtes. Cette topologie permet de

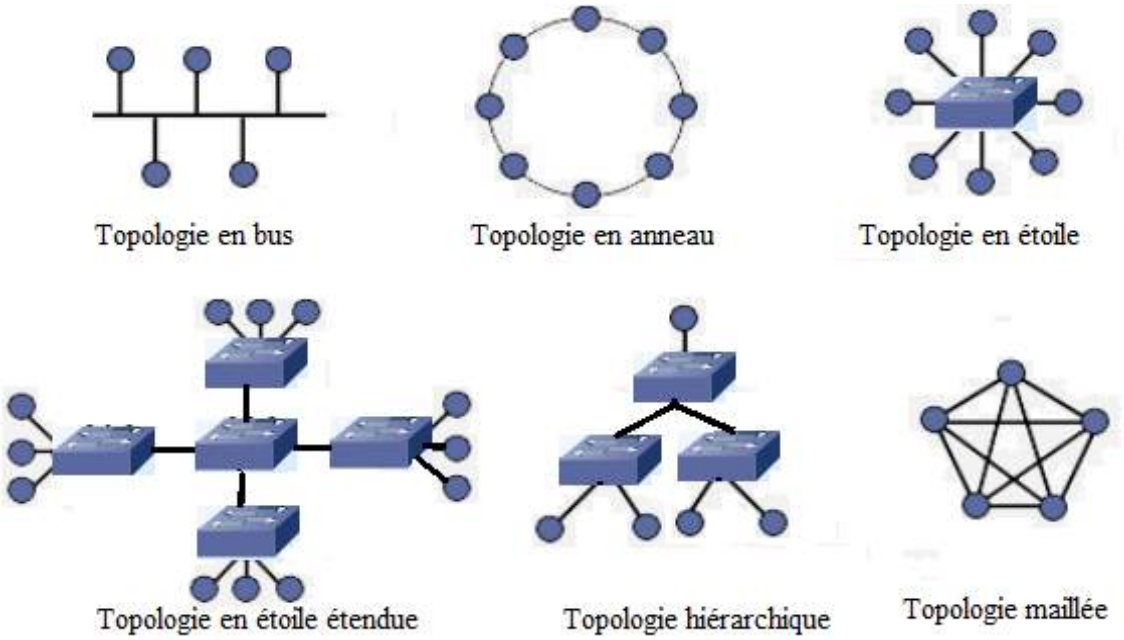


FIG. 1-4 – Topologies physiques.

remédier de façon optimale au problème d'interruption de service. La topologie du réseau internet est plus proche de cette topologie mais n'est pas complètement maillée.

L'autre type de topologie est la topologie logique qui représente la manière avec laquelle les hôtes accèdent au média physique. Les deux principales topologies logiques sont le broadcast et le passage de jeton. Dans la première, chaque hôte désirant transmettre, envoie ses données à tous les autres hôtes appartenant au même réseau. Dans la seconde, un jeton circule d'un hôte à un autre afin de leur permettre de transmettre des données sur le réseau. Un hôte désirant transmettre, garde le jeton pendant un temps déterminé, transmet ses données puis envoie le jeton à l'hôte suivant. Un hôte qui n'a pas de données à transmettre, envoie directement le jeton à l'hôte suivant et ainsi de suite.

V Qu'est ce qu'un protocole ?

Un protocole est un ensemble de règles et de conventions établies, par un grand nombre d' organisations et de comités (IEEE, TIA, EIA, ITU...), afin de régir les communications entre équipements sur le réseau. Un protocole gère plusieurs aspects des communications :

- Comment les ordinateurs se connectent.
- Le contenu et le format des données à transmettre sur le réseau.
- Comment gérer la chronologie dans la communication des données.
- Comment envoyer les données.
- Comment contrôler les erreurs de transmission...

VI Réseaux locaux (LAN)

LAN signifie Local Area Network. Il s'agit d' un réseau de très petit étendu qui va permettre de relier un ensemble d' ordinateurs qui appartiennent à une même entreprise ou organisation. Il rend ainsi possible les communications locales, telles que: partage de fichiers, partage de ressources...etc. Il contient des équipements hôtes et bien entendu des équipement de réseau. Les technologies les plus courantes pour les réseaux locaux sont : Ethernet, Token ring et FDDI.

VII Réseaux métropolitains (MAN)

Un réseau métropolitain est un réseau qui couvre une zone métropolitaine (ville ou banlieue) et qui permet à au moins deux réseaux LAN de communiquer entre eux. Cela peut servir dans le cas ou par exemple plusieurs agences d'une banque veulent communiquer entre elles.

VIII Réseaux étendus (WAN)

WAN est l'acronyme de Wide Area Network qui signifie réseau à large étendu. Ce type de réseau permet d'interconnecter plusieurs réseaux locaux géographiquement dispersés, d'accéder à des serveurs de fichiers distants

et de partager des ressources (imprimantes, ordinateurs et autres équipements pouvant être reliés à un réseau LAN). De cette façon les entreprises éventuellement distantes peuvent communiquer entre elles, séchanger des fichiers, partager des ressources...etc. Les utilisateurs de ce réseau doivent pouvoir communiquer et accéder aux ressources distantes en temps réel. Les technologies les plus courantes pour les réseaux étendus sont : RNIS, DSL, Frame Relay...

IX Bande passante et débit

La bande passante représente la quantité d'informations qui peut circuler sur une connexion réseau en un temps donnée. Elle dépend principalement des propriétés physiques du média utilisé et des technologies LAN et WAN utilisées pour placer l'information sur le média. En effet, il existe des différences entre les caractéristiques physiques des différents supports, tels que : câble coaxial, câble à paires torsadées blindées ou non blindées, fibre optique...etc, ces différences engendrent différentes capacités de transfert des informations (10Mbits/s pour un câble coaxial, 100Mbits/s pour une certaine catégorie de câble à paires torsadée non blindées...etc) . Quelque soit le support utilisé, la bande passante reste une valeur finie.

La fibre optique offre actuellement une bande passante quasiment illimitée, cependant aucune technologie ne permet d'exploiter pleinement son potentiel. La bande passante ne cesse de croître afin de satisfaire les besoins des applications (téléphonie IP...) qui ne cessent d'augmenter eux aussi. Mesurer la bande passante permet d'analyser les performances des réseaux, elle constitue aussi un facteur essentiel dans la conception du réseau. L'unité de base de la bande passante est le bit/s.

Le débit représente quant à lui la bande passante réelle mesurée. Il est souvent inférieur à la bande passante pour de diverses raisons, telles que : PC du client, le serveur, le nombre d'utilisateurs sur le réseau, le routage, la topologie utilisée, type de données transmises et l'heure du jour à laquelle se fait le transfert de données.

X Réseau d'égal à égal (peer to peer) et réseau client-serveur

Deux ordinateurs interagissent gâces à des protocoles de requêtes et de réponse. L'un agit comme client et l'autre comme serveur.

Suivant le type de réseau, les ordinateurs adoptent des rôles bien précis. Si nous sommes dans un réseau d'égal à égal, chaque ordinateur peut assumer le rôle de client ou de serveur et peut contôler ses propres ressources. Les ordinateurs du réseau sont ainsi des partenaires égaux. Les avantages de ce type de réseau est qu'il est nullement nécessaire d'ajouter un quelconque équipement et il n'est pas nécessaire d'avoir un administrateur. Cependant, ce type de réseau reste très peu évolutif (extension très difficile et décroit leur efficacité) et sa sécurité est sa sécurité est difficile à assurer.

Dans un réseau client-serveur, les ordinateurs de type 'ordinateur de bureau' jouent le rôle de client. Le ou les ordinateurs plus puissants, plus onéreux aussi, sont dotés d'une plus grande mémoire, d'une plus grande puissance de calcul et d'un système d'éxploitation approprié remplissent la fonction de serveur. Les services rendus par ces derniers peuvent de différents types : messagerie, web,...etc. Les clients disposent généralement d'un identificateur et d'un mot de passe qui va leur permettre d'accéder aux ressources du serveurs et d'envoyer les réquêtes. Ce mécanisme d'authentification permet de protéger et de sécuriser l'accès au serveur. Ce type d'architecture facilite la gestion et la sécurité des données mais l'aspect centralisé fait que le serveur constitu un point de défaillance unique. Un administrateur est indispensable dans ce type de réseau pour assurer son bon fonctionnement (administration et maintenance).

RPC est l'acronyme de Remote Procedure Call, c'est justement une technique client serveur qui consiste à faire des appels de procédure distantes en se basant sur des requêtes et des réponses. Elle permet de développer un bon nombre d'applications client-serveur. Une procédure RPC est identifiable par trois paramètres qui sont : numéro du programme, numéro de la version et enfin numéro de la procédure.

XI Conclusion

Ce chapitre nous a permis d'introduire l'étudiant à différentes notions de base en réseaux informatiques, nous avons commencé pour cela a décrire les différents équipements hôtes et réseaux que nous évoquerons dans les chapitres suivants, ensuite nous avons décrit les différentes topologies existantes et défini les terminologies de bases qui serviront à faciliter la compréhension des chapitres suivants.

Chapitre 2

Modèle OSI et TCP/IP

I Introduction

Le modèle OSI (Open System Interconnection) [1] a été créer par l'ISO (International Organization for Standardization) afin de remédier au problème d'incompatibilité entre les réseaux qui existait au milieu des années 80. Ce modèle sert de principale référence aux différents constructeurs pour créer des réseaux compatibles avec les réseaux existants. Ce modèle est également utilisé à des fin pédagogiques, puisqu'il se présente sous forme de plusieurs couches ce qui aide à comprendre le fonctionnement du réseau et le rend plus gérable. En effet, il se compose très éxactement de sept couches, chacune remplie une fonction bien précise. Son avantage majeur est qu'une modification apportée à l'une de ses couches n'affecte aucunement les autres couches. Dans ce qui suit, nous expliquons le rôle de chaque couche du modèle OSI et nous passons ensuite au modèle TCP/IP [1] qui est la norme de base du réseau internet.

II Couches OSI

Comme mentionné précédemment, le modèle OSI se compose de sept couches. Les trois couches supérieures sont plus orientées application, tandis que les quatre couches inférieures sont orientées communication et trans-

port des données. La figure 2-1 illustre ces sept couches.

II.1 Couche application

Est une interface qui assure l'accès des applications au réseau. C'est en quelque sorte un point d'accès aux services réseau.

II.2 Couche présentation

Lorsque différents ordinateurs veulent s'échanger des informations, certaines conversions sont nécéssaires. Cette couche a pour rôle de s'assurer que les informations envoyées par la couche application du système émetteur soient parfaitement lisibles par la couche application du récepteur. De cette façon, les informations sont indépendantes du type du système d'exploitation ou du microprocesseur. Elle effectue également la compression et le cryptage des données à transmettre (sens descendant) ainsi que la décompréssion et le décryptage des données reçues (sens montant).

II.3 Couche session

Cette couche a pour but d'établir des sessions, de les maintenir et de les terminer en fin de communication. Si plusieurs applications en cours d'exécution sur un ordinateur utilisent le même réseau et acheminent les données au travers d'une même carte réseau, le système d'éxploitation doit être en mesure de différencier les différents paquets reçus en réponse aux éventuelles requêtes des différentes applications. C'est grâce au principe de sessions séparées que cela peut se faire.

II.4 Couche transport

Cette couche segmente les données reçues de la couche session. Elle est aussi responsable du transfert fiable des différents segments obtenus et cela de bout en bout. La notion de fiabilité veut dire que cette couche est capable d'assurer la détection et la correction des erreurs (récupération sur erreur). Elle contrôle aussi le

séquencement des segments et le flux d'informations qui permet d'envoyer une quantité de données gérable par le récepteur et ne pas dépasser sa capacité.

Les protocoles utilisés au niveau de cette couche sont TCP (Transmission Control Protocol) et UDP (User Datagram Protocol). C'est l'un ou l'autre de ces protocoles qui est utilisé, suivant l'application utilisée.

II.5 Couche réseau

Elle se charge de l'adressage logique (adresse IP) qui est différent de l'adressage physique effectué au niveau de la couche liaison de données. Elle détermine la manière avec laquelle les paquets sont acheminés (routage des paquets) entre extremités.

II.6 Couche liaison de données

Cette couche fournit un service d'adressage physique aux couches supérieures. L'adresse physique est en l'occurence l'adresse MAC (Media Access Control). Elle s'occupe de la topologie du réseau, de l'accès au réseau, détecte et gère les erreurs de transmission. Les technologies Ethernet et Token ring sont implémentées au niveau de cette couche. Elle se divise en deux sous couches : la sous couche LLC (Logical Link Control) et la sous couche MAC (Media Access Control).

Adresse MAC

Une carte réseau est un équipement de la couche liaison de données qui permet de contrôler l'accès de l'hôte au réseau. Chaque carte réseau est identifiée par une adresse unique appelé adresse MAC. Ces dernières ont une longueur de 48 bits exprimées sous la forme de douze nombres héxadécimaux. Les six premiers héxadécimaux identifient le fabricant (identificateur OUI). Les six derniers héxadécimaux constituent le numéro de série de l'interface ou une autre valeur gérée par le fabricant. Les adresses MAC sont inscrites de manière définitive en mémoire ROM (Read Only Memory) et sont copiées dans la RAM (Random Access Memory) lors de l'initialisation de la carte réseau.

II.7 Couche physique

Cette couche permet de convertir les bits en signaux afin de les envoyer sur un média physique. Elle determine le voltage, la périodicité, le débit...etc des données physiques grâce aux différentes opérations telles que : codage, modulation...etc. Il existe différentes spécifications pour cette couche suivant le type de réseau LAN ou WAN.

III Communication d'égal à égal

Afin de permettre un transfert d'informations entre deux ordinateurs, chaque couche appartenant au modèle OSI de l'ordinateur source doit communiquer avec sa couche homologue du modèle OSI de l'ordinateur de destination. Ce type de communication est appelé d'égal à égal. Les couches homologues s'échangent ainsi des informations appelées PDU (Protocol Data Unit). Lors d'un transfert de données, en partant de la couche application vers la couche physique, chaque couche place les PDU reçues de la couche supérieures dans son propre champ de données, des en-têtes et des en-queues de PDU sont ajoutés ensuite afin de permettre à chaque couche de réaliser ses fonctions. Ce processus est appelé encapsulation et est schématisé en niveau de la figure 2-1. Par exemple, au niveau de la couche liaison de données, l'en-tête ajoutée au PDU de la couche réseau contient les adresses physiques source et destination nécessaire à l'exécution de la fonction de la couche liaison de données.

Au niveau de l'ordinateur de réception, en partant de la couche physique vers la couche application, chaque couche effectue le processus inverse en enlevant l'en-tête et eventuellement l'enqueue ajoutés par sa couche homologue au niveau de l'émetteur et en envoyant la partie données à la couche supérieure. Ce processus est appelé désencapsulation.

IV Modèle TCP/IP

Afin d'assurer une transmission fiable à 100% des paquets, le ministère américain de la défense à crée le nouveau modèle TCP/IP (figure 2-2). Celui-ci comporte quatre couches (application,transport, internet et accès

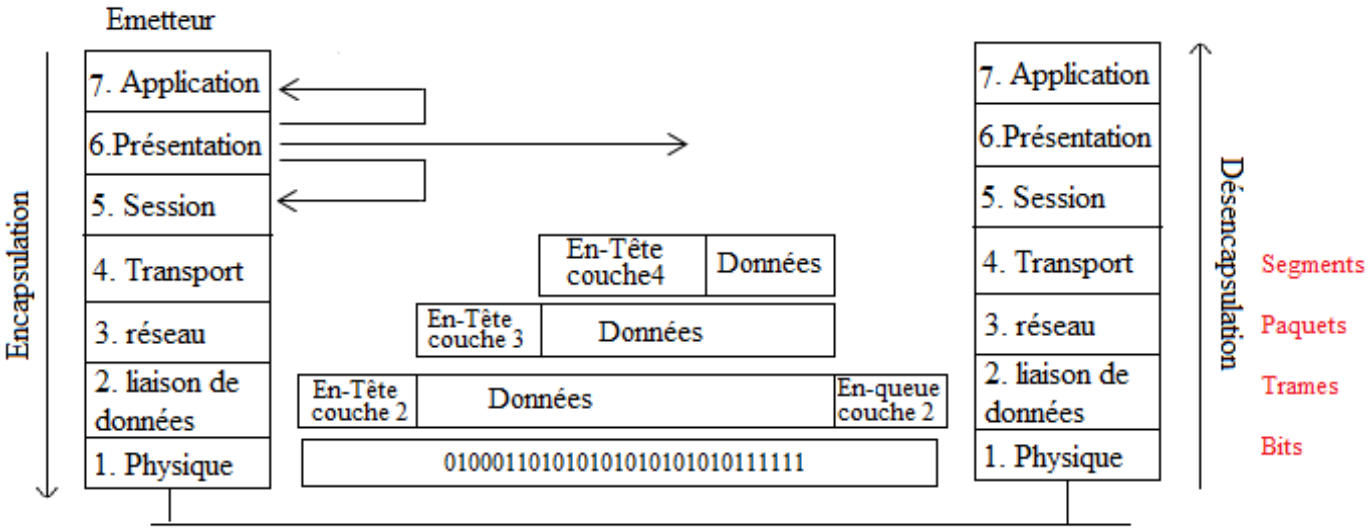


FIG. 2-1 – Processus d'encapsulation et de désencapsulation.

au réseau) au lieu des sept couches du modèle OSI. Bien que certaines couches des deux modèles portent le même nom, elles n'ont pas pour autant les mêmes fonctions.

IV.1 Couche application

La couche application du modèle TCP/IP comprend les détails des couches présentation et session du modèle OSI. Elle gère donc la présentation des données et verifie que les données sont bien préparées pour la couche suivante. Elle s'occupe aussi du contrôle du dialogue et de tous les aspects liés aux applications.

IV.2 Couche transport

La couche transport est chargée d'assurer la fiabilité du transfet d'information, le contrôle du flux et des erreurs. Là aussi, UDP et TCP sont les principaux protocoles de cette couche. Le premier est non orienté connexion, ce qui veut dire qu'il n'établie aucune connexion au préalable d'un échange, les données sont expédiées au destinataire sans avertir que la transmission est en route, ainsi nous avons un contrôle d'erreur

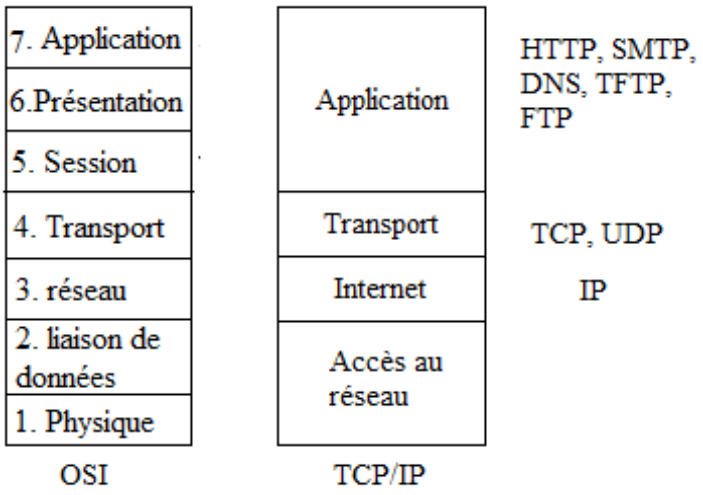


FIG. 2-2 – Modèle TCP/IP.

très rudimentaire, le destinataire reçoit éventuellement les données sans rien en dire à l'expéditeur. Le second protocole est orienté connexion, ce qui veut dire qu'une connexion est établie et maintenue entre l'émetteur et le récepteur pendant toute la durée du dialogue. Au début de cette connexion, pendant qu'il prépare les informations reçus de la couche application en segments, des segments de couche 4 sont échangés entre les deux ordinateurs dans le but de s'assurer de l'existence logique de la connexion (établir une connexion de bout en bout). Les segments préparés sont ensuite envoyés et le récepteur envoie un accusé de réception des données reçues.

IV.3 Couche Internet

La couche internet permet de préparer les segments de la couche transport en paquets, cela en y rajoutant un adressage logique qui va permettre de faire transiter les paquets sur des réseaux d'architecture très diverses. Cette couche se charge du choix du meilleur chemin qui permet d'atteindre une destination et de la commutation de paquets.

IV.4 Couche d'accès au réseau

La couche d'accès au réseau englobe les fonctionnalités des couches physique et liaison de données du modèle OSI. Elle compend ainsi les details des technologies LAN et WAN (Ethernet, FDDI, Fast Ethernet...), elle assure l'interface physique avec le réseau grâce à des composants logiques et physiques tels que : pilotes, modems et autres équipements. Elle assure l'encapsulation des paquets issus de la couche réseau en trames en y rajoutant les adresses matérielles physiques des équipements concernés par cet échange. Cette couche effectue aussi le contrôle d'erreur au niveau des données.

Remarque : Un réseau WAN fonctionne sur la couche physique et sur la couche liaison de données. Cela ne veut pas dire que les cinq autres couches du modèle OSI sont absentes d'un réseau WAN, mais simplement que les caractéristiques qui distinguent un réseau WAN d'un réseau LAN se situent en général au niveau de la couche physique et de la couche liaison de données. Autrement dit, les normes et les protocoles des couches 1 et 2 des réseaux WAN sont différents de ceux des mêmes couches des réseaux LAN.

V Adressage IP

Une machine doit être identifiée par une adresse physique (MAC) et une adresse logique (IP) pour pouvoir procéder à un quelconque échange de données. Une machine connectée à plusieurs réseaux doit disposer d'autant de cartes réseaux que de connexions aux réseaux et par conséquent d'une adresse IP pour chaque connexion. L'adresse IP intervient comme cité précédemment au niveau de la couche réseau du modèle OSI. Elle se présente sous la forme d'une séquence de 32 bits, exprimée pour pour plus de facilité sous la forme de quatre nombres décimaux séparés par des points. Elle se compose en deux parties : partie réseau et partie hôte. La première partie identifie le réseau auquel est connectée la machine et la seconde partie identifie la machine. Le nombre de bits attribué à chacune des deux parties permettra de connaitre la classe de l'adresse IP utilisée.

En effet, plusieurs classes éxistent suivant le nombre de bits dédié à la partie réseau et à la partie hôte. Le fait de réserver un plus grand nombre de bits à la partie hôte permettra d'avoir un nombre de réseaux réduit en nombre mais de très grande de taille, l'inverse est aussi vrai. Le tableau suivant regroupe les différentes classes

d' adresses IP.

Classe	Bits partie réseaux	Nb réseaux	Bits supérieures	Plage d'adresse	Nb Hôtes
A	8	126	0	0-127*	16 777 216
B	16	16 384	10	128-191	65 535
C	24	2 097 152	110	192-223	254
D	28	S.O	1110	224-239	S.O

Une des problèmatiques qui se posent à nous est celle de la pénurie des adresses IP. Plusieurs solutions ont été proposées dont : les adresses IP publiques et privées (NAT), le découpage en sous réseau et l'adressage IPV6, le CIDR (Classless InterDomain Routing), le VLSM (Variable Length Subnet Mask).

V.1 Découpage en sous réseaux

Exercice 01

1) Soit l'adresse 192.16.5.133/29. Combien de bits sont utilisés pour identifier la partie réseau et combien de bits sont utilisés pour identifier la partie hôte ? Quel est le masque de sous réseau correspondant ?

Partie réseau : 29 bits.

Partie hôte : 3 bits.

Masque de sous réseau : 11111111.11111111.11111111.11111000=255.255.255.248

Exercice 02

Pour configurer l'interface d'un hôte qui doit se connecter à un réseau existant, on nous donne l'adresse 172.16.19.40/21 :

- Quel est le masque réseau de cette adresse ?

La notation /21 indique que la partie réseau de l'adresse occupe 21 bits. On décompose ces 21 bits en 8 bits. 8 bits. 5 bits ; ce qui donne 255.255.248.0

- Combien de bits ont été réservés pour les sous réseaux privés relativement à la définition historique de classe ?

La valeur du premier octet de l'adresse étant comprise entre 128 et 192, il s'agit d'une adresse de classe B. Le masque réseau d'une classe B étant 255.255.0.0, 5 bits ont été réservés sur le troisième octet pour constituer

des sous réseaux.

- Combien de sous réseaux privés sont disponibles relativement à la définition historique de classe ?

Le nombre de valeurs codées sur 5 bits est de 2^5 soit 32. Suivant la génération du protocole de routage utilisé, on applique deux règles différentes :

1) On exclu le premier (all-zeros) et le dernier (all-ones) sous réseau conformément au document de 1985. Dans ce cas, le nombre de sous réseaux utilisable est 30 (Classful).

2) Dans les réseaux contemporains, on retient l'ensemble des sous réseaux. Dans ce cas le nombre de sous réseaux est 32 (Classless).

- Combien d'hôtes peut contenir chaque sous réseau ?

Les adresses des hôtes sont codées sur les bits à 0 du masque réseau. Avec le masque /21, il reste 32-21= 11 bits donc 2^11=2048. Chaque sous réseau peut contenir 2046 hôtes. On a retiré la valeur 0 puisqu'elle sert à identifier l'adresse du réseau et non celle d'un hôte ainsi que la valeur avec les 11 bits à 1 qui sert à la diffusion sur les sous réseaux.

- Quelle est l'adresse du sous réseau de l'exemple ?

Le troisième octet est partagé entre partie réseau et partie hôte, si on le convertit en binaire, on obtient : 00010011. En faisant un ET logique avec la valeur binaire correspondant 5 bits réseau (11111000), on obtient : 00010000 ; soit 16 en décimal. L'adresse du sous réseau est donc 172.16.16.0.

- Quelle est l'adresse de diffusion du sous réseau de l'exemple ?

Le quatrième octet étant compris dans la partie hôte, il suffit de le remplacer par 255.

Le troisième octet est partagé entre partie réseau et partie hôte (00010011), On effectue cette fois ci un OU logique avec la valeur binaire correspondante aux trois bits d'hôte à un (00000111), on obtient : 00010111 soit 23 en décimal. L'adresse de diffusion du sous réseau est donc 172.16.23.255.

V.2 adresses publiques/privées et NAT

Les adresses publiques sont utilisées pour se connecter à internet tandis que les adresses privées sont utilisées en interne (entreprise).

Dans un système ou les adresses IP sont privées, chaque hôte doit avoir une adresse IP unique, les hôtes privés qui ne veulent pas se connecter à internet peuvent très bien utiliser n'importe quelle adresse IP privée du moment quelle est unique (pas affectée à une autre machine du même réseau privé).

Il y a trois plages d'adresses IP privées :

Classe	Plage d'adresse IP Privée
A	10.0.0.0-10.255.255.255
B	172.16.0.0-172.31.255.255
C	192.168.0.0-192.168.255.255

Toutes ces adresses ne sont pas acheminées dans le réseau internet. Les routeurs sont tous configurés pour éliminer les adresses privées. Elles ne sont donc pas routables sur internet.

Dans un intranet privé, il est plutôt conseillé d'utiliser des adresses privées. Lorsque des hôtes de cet intranet privé veulent se connecter à internet, il faudra faire une translation d'adresses privées en adresses publiques. Cette translation s'appelle le NAT (Network Adresse Translation). Le périférique réseau qui s'occupe de cette translation est le routeur.

Les adresses IP publiques sont utilisées par des hôtes qui doivent être accessibles depuis internet. Chaque adresse publique doit être unique sur internet pour qu'il soit stable. C'est l'organiqme IANA qui se charge de s'assurer qu'il n'y a aucun doublant. Pour obtenir une IP publique, il faut solliciter un FAI (fournisseur d'accès Internet).

Voici les plages d'adresse publiques :

Classe	Plage d'adresse IP publique	
A	1.0.0.0-9.255.255.255	11.0.0.0-126.255.255.255
B	128.0.0.0-172.15.255.255	172.32.0.0-191.255.255.255
C	192.0.0.0-192.167.255.255	192.169.0.0-223.255.255.255

Dans les petites entreprises, il est plus pratique d'utiliser des adresses privées, ce qui permet une plus grande

flexibilité pour la conception du réseau et une croissance plus facile. Cependant, deux entreprises peuvent avoir les mêmes adresses privées. Pour qu'elles puissent communiquer entre elles ou pour qu'elles puissent se connecter à internet, le NAT intervient.

Il y a deux types d'adresses importantes dans le NAT, l'inside local (adresse privée de l'hôte sur le réseau interieur) et l'inside globale (adresse traduite à l'interieur du réseau local ou nouvelle adresse IP natée de l'hôte pour pouvoir se connecter à internet). Inside signifie le réseau interne de l'entreprise. C'est le routeur qui change l'adresse Inside Local en adresse Inside Globale.

Le réseau Outside est tout ce qui est extérieur au réseau Inside. L'adresse IP outside globale est l'adresse IP qui réside dans la partie extérieur du réseau et que l'hôte interne souhaite joindre (adresse IP de destination). L'adresse IP outside locale est l'adresse IP externe de destination. En principe, elle est identique à l'adresse à l'adresse Outside globale.

Il existe trois types de NAT :

NAT statique :

NAT dynamique :

PAT (Port address translation) NAT Overload

VI Conclusion

Ce chapitre nous a permis de comprendre les différents rôles des couches du modèle de base OSI et leur relation avec les couches du modèle TCP/IP. Nous avons aussi expliqué le système d'adressage IP ainsi que les différentes classes d'adresses existantes. Le choix de la classe d'adresse IP à utiliser dependra principalement de la taille du réseau que nous voulons configurer.

Chapitre 3

Les concepts de base du routage

I Introduction

Le routage [3] consiste à faire circuler des données au travers d'un interréseau entre une source et une destination. Celui-ci s'effectue au niveau de la couche réseau (couche trois du modèle OSI).

Le routage implique deux activités principales : premièrement, la détermination du chemin optimal pour le transferts des groupes d'informations (paquets) entre la source et la destination et deuxièmement, le transfert proprement dit des paquets a travers le réseau (commutation de paquets).

Les protocoles de routage correspondent à l'implémentation des algorithmes de routage, il en existe plusieurs : IGRP (Interior Gateway Routing Protocol), EIGRP (Enhanced Interior Gateway Routing Protocol), OSPF (Open Shortest Path First), EGP (Exterior Gateway Protocol), RIP (Routing Information Protocol)...etc. Dans la suite de ce chapitre, nous allons expliquer les principes de base du routage et ensuite décrire le protocole de routage IGRP.

II Détermination du chemin optimal

Les protocoles de routage déterminent le meilleur chemin en se basant sur des métriques. Ces dernières correspondent à des mesures utilisées par l'algorithme de routage pour déterminer le chemin optimal qui permettra d'acheminer les paquets jusqu'à la destination. Des tables de routage sont maintenues par l'algorithme de routage, elles permettent de garder des informations sur les routes et aident ainsi à la détermination du chemin optimal. Ces tables conservent[1] entre autres les informations suivantes : destination / prochain saut. Ces dernières indiquent au routeur ayant reçu le paquet qu'une destination donnée est atteinte en envoyant le paquet à un autre routeur qui représente le "prochain saut". En d'autres termes, grâce aux tables de routage, lorsqu'un routeur reçoit un paquet, il tente d'associer à son adresse de destination un prochain saut.

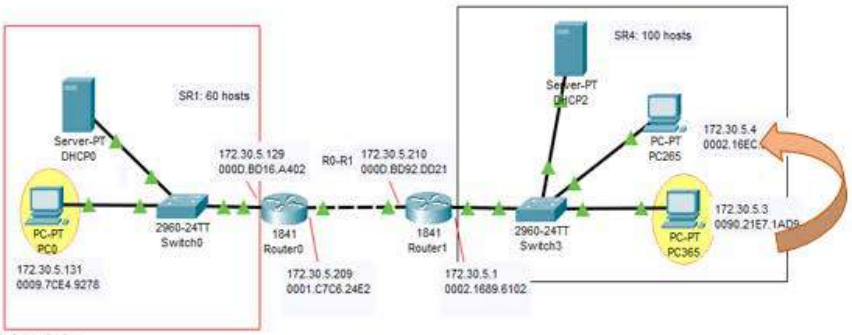
Les routeurs peuvent comparer plusieurs métriques utilisées par différents algorithmes de routage pour déterminer le chemin optimal. Les routeurs s'envoient aussi des mises à jour des tables de routage, elles sont constituées d'une partie ou de l'intégralité de la table.

III La commutation

L'algorithme de commutation est pratiquement le même pour tous les algorithmes de routage. Généralement, lorsqu'un hôte veut envoyer des paquets à un hôte distant et après avoir obtenu l'adresse du routeur auquel il est directement relié, l'hôte source envoie le paquet avec l'adresse physique (adresse MAC) du routeur et l'adresse logique (adresse IP) de l'hôte de destination. Le routeur en question examine le paquet reçu et détermine à l'aide de l'adresse IP de destination s'il peut lui attribuer un saut suivant, autrement le paquet est rejeté. Dans le premier cas, le routeur remplace l'adresse physique de destination par celle du saut suivant et envoie le paquet. Dans le cas où l'hôte de destination est encore loin, d'autres routeurs exécutent cette même procédure, comme montré sur la figure 3-1.

La fonction principale d'un routeur consiste à acheminer des paquets vers leur destination. Il faut pour cela faire appel à la fonction de commutation, qui est le processus utilisé par un routeur pour recevoir un paquet sur une interface et l'envoyer depuis une autre interface. La fonction de commutation a pour responsabilité

[1] Une table de routage conserve les informations suivantes : Destination réseau, Masque réseau, Adresse passerelle, Adresse Interface ou Nom de l'interface, Métrique.



Envoie du message

PC365

Layer 3: IP Header Src. IP: 172.30.5.3, Dest. IP: 172.30.5.4 ICMP Message Type: 8
Layer 2: Ethernet II Header 0090.21E7.1AD9 >> 0002.16EC.9483
Layer 1: Port(s): FastEthernet0

PC265

Layer 3: IP Header Src. IP: 169.254.26.217, Dest. IP: 169.254.148.131 ICMP Message Type: 8
Layer 2: Ethernet II Header 0090.21E7.1AD9 >> 0002.16EC.9483
Layer 1: Port FastEthernet0

Layer 3: IP Header Src. IP: 169.254.148.131, Dest. IP: 169.254.26.217 ICMP Message Type: 0
Layer 2: Ethernet II Header 0002.16EC. 9483 >> 0090.21E7.1AD9
Layer 1: Port(s): FastEthernet0

Réponse au message

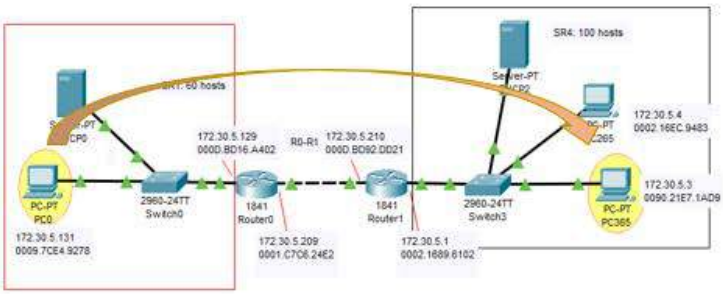
PC265

Layer 3: IP Header Src. IP: 169.254.26.217, Dest. IP: 169.254.148.131 ICMP Message Type: 8
Layer 2: Ethernet II Header 0090.21E7.1AD9 >> 0002.16EC.9483
Layer 1: Port FastEthernet0

Layer 3: IP Header Src. IP: 169.254.148.131, Dest. IP: 169.254.26.217 ICMP Message Type: 0
Layer 2: Ethernet II Header 0002.16EC. 9483 >> 0090.21E7.1AD9
Layer 1: Port(s): FastEthernet0

PC365

Layer 3: IP Header Src. IP: 172.30.5.4, Dest. IP: 172.30.5.3 ICMP Message Type: 0
Layer 2: Ethernet II Header 0002.16EC. 9483 >> 0090.21E7.1AD9
Layer 1: Port FastEthernet0



- **Envoie du message**

PC0

Layer 3: IP Header Src. IP: 172.30.5.131, Dest. IP: 172.30.5.3 ICMP Message Type: 8
Layer 2: Ethernet II Header 0009.7CE4.9278 >> 000D.BD16.A402
Layer 1: Port(s): FastEthernet0

Router0

Layer 3: IP Header Src. IP: 172.30.5.131, Dest. IP: 172.30.5.3 ICMP Message Type: 8
Layer 2: Ethernet II Header 0001.C7C6.24E2 >> 000D.BD92.DD21
Layer 1: Port(s): Ethernet0/0/0

Router1

Layer 3: IP Header Src. IP: 172.30.5.131, Dest. IP: 172.30.5.3 ICMP Message Type: 8
Layer 2: Ethernet II Header 0002.1689.6102 >> 0090.21E7.1AD9
Layer 1: Port(s): FastEthernet0/1

PC365

Layer 3: IP Header Src. IP: 172.30.5.3, Dest. IP: 172.30.5.131 ICMP Message Type: 0
Layer 2: Ethernet II Header 0090.21E7.1AD9 >> 0002.1689.6102
Layer 1: Port(s): FastEthernet0

- **Réponse au message**

PC 365

ayer 3: IP Header Src. IP: 172.30.5.3, est. IP: 172.30.5.131 ICMP Message ype: 0
ayer 2: Ethernet II Header 090.21E7.1AD9 >> 0002.1689.6102
ayer 1: Port(s): FastEthernet0

Router1

Layer 3: IP Header Src. IP: 172.30.5.3, Dest. IP: 172.30.5.131 ICMP Message Type: 0
Layer 2: Ethernet II Header 000D.BD92.DD21 >> 0001.C7C6.24E2
Layer 1: Port(s): Ethernet0/0/0

Router0

Layer 3: IP Header Src. IP: 172.30.5.3, Dest. IP: 172.30.5.131 ICMP Message Type: 0
Layer 2: Ethernet II Header 000D.BD16.A402 >> 0009.7CE4.9278
Layer 1: Port(s): FastEthernet0/1

PC0

Layer 3: IP Header Src. IP: 172.30.5.3, Dest. IP: 172.30.5.131 ICMP Message Type: 0
Layer 2: Ethernet II Header 000D.BD16.A402 >> 0009.7CE4.9278
Layer 1: Port FastEthernet0

Fig. 3-1: Le processus de commutation (cas de la remise directe et indirecte)

principale d' encapsuler les paquets dans le type de trame liaison de données adéquat pour la liaison de données de sortie.

Remarque : dans ce contexte, le terme « commutation » désigne littéralement les paquets se déplaçant d'une source vers une destination. Il ne faut pas le confondre avec la fonction d' uncommutateur de couche 2.

Une fois que le routeur a déterminé l'interface de sortie à l'aide de la fonction de détermination du chemin, le routeur doit encapsuler le paquet dans la trame liaison de données de l'interface de sortie.

Que fait un routeur d'un paquet qu'il a reçu d'un réseau et qui est destiné à un autre réseau ? Le routeur effectue les trois étapes principales suivantes :

Étape 1. Il désencapsule le paquet de couche 3 en supprimant l'en-tête et le code de fin (trailer) de la trame de couche 2.

Étape 2. Il examine l'adresse IP de destination du paquet IP pour trouver le meilleur chemin dans la table de routage.

Étape 3. Si le routeur trouve un chemin vers la destination, il encapsule le paquet de couche 3 dans une nouvelle trame de couche 2 et transfère la trame à l'interface de sortie.

Comme l'illuste la figure (Fig 3-1), PC0 est configuré avec l'adresse IPV4 172.30.5.131 et l'adresse MAC 0009.7CE4.9278. Lorsqu'un paquet circule du périphérique source au périphérique de destination finale, les adresses IP de couche 3 demeurent identiques. Cependant, les adresses de couche 2 changent à chaque saut, lorsque le paquet est désencapsulé puis encapsulé dans une nouvelle trame par chacun des routeurs. Il est très probable que le paquet soit encapsulé dans un type de trame de couche 2 différent de celui dans lequel il a été reçu. Par exemple, une trame Ethernet encapsulée peut être reçue par le routeur sur une interface FastEthernet, puis traitée pour être transmise par une interface série. Dans l'image, nous considérons que toutes les trames sont de type Ethernet.

IV Objectifs des algorithmes de routage

Les algorithmes de routage doivent répondrent aux objectifs suivants

- Un algorithme de routage doit avoir un fonctionnement optimal. Ceci se résume à sa capacité à choisir le meilleur chemin. Un algorithme peut par exemple prendre en considération plusieurs métriques dans ses calculs, comme le nombre de sauts et les périodes d'attente...etc. Différents coéfficients peuvent être attribués aux métriques, ce qui leur donne un rôle plus ou moins décisifs dans le choix du chemin optimal.
- Un algorithme de routage doit être conçu de la manière la plus simple possible, il ne doit causer aucune lourdeur d'utilisation et avoir une charge de travail très réduite. Il doit être efficace afin de pouvoir fonctionner sur des ressources physiques limitées.
- Il doit être robuste et réagir de manière efficace face aux imprévus comme : problème matériel, panne des routeurs, implémentation incorrecte, grosses charges de travail...etc.
- Les algorithmes de routage doivent converger le plus rapidement possible et arriver à conclure un accord avec tous les réseaux concernant les routes optimales. Si par exemple de nouvelles routes sont mises en service, cela provoquerai un nouveau calcul des routes optimales et forcerai les routeurs à conclure un accord sur l'emprunt de ces nouvelles routes.
- Les algorithmes de routage doivent faire preuve d'une certaine flexibilité face à certains changements survenus au niveau de la bande passante, des temps de latence, de la taille des files d'attente des routeurs, de l'état d'un segment du réseau...etc. Si par exemple, un segment du réseau est interrompu, les algorithmes de routage doivent rapidement choisir un autre chemin optimal pour chaque route qui utilisait ce segment.

V Les différents types d'algorithme de routage

Il existe plusieurs classifications pour les algorithmes de routage, nous citons ici quelques-unes.

- Les algorithmes statiques (non adaptatif) et dynamiques (adaptatif) : Les algorithmes statiques sont équivalents à des tables de routage définies par l'administrateur du réseau avant le commencement du routage. Ils fonctionnent bien dans des réseaux de petites tailles, simples et dont le trafic est prévisible. Ils ne peuvent pas réagir automatiquement aux modifications au sein du réseau tant que l'administrateur n'a pas intervenu. Ils sont inappropriés dans les grands réseaux. Les algorithmes dynamiques s'adaptent quant à eux aux changements du réseau, cela en analysant les messages de mise à jour de routage qui

y circulent. Si les messages indiquent qu'il y a eu des modifications dans le réseau, le logiciel de routage recalcule les routes optimales et envoie d'autres messages de mise à jour qui vont inciter d'autres routeurs à recalculer leurs routes et modifier par conséquent leurs tables de routage. Le routage statique peut être utilisé en complément du routage dynamique, afin de définir des routeurs de dernier recours par exemple.

- Les algorithmes à trajet unique et à trajets multiples : certains algorithmes à trajets multiples utilisent plusieurs routes pour atteindre une même destination. Ceci permet de multiplexer du trafic sur plusieurs liaisons ce qui offre un bien meilleur débit et une meilleure fiabilité.
- Les algorithmes à état des liens et les algorithmes à vecteur de distance : les algorithmes à état des liens font partie de la catégorie des algorithmes centralisés. Ils transmettent les informations de routage à tous les noeuds de l'interréseau, cependant, les routeurs n'envoient que l'état de leurs propres liens. Chaque routeur du réseau construit une image complète du réseau dans sa table de routage (petites mises à jour partout). Dans les algorithmes à vecteur de distance qui font partie de la catégorie des algorithmes distribués, chaque routeur envoie une partie ou l'intégrité de sa table de routage uniquement aux routeurs voisins (mises à jour importantes aux voisins). Le premier type d'algorithme est plus gourmand en terme de CPU et de mémoire.

VI Les métriques de routage

Certains algorithmes utilisent une seule métrique, d'autres combinent plusieurs, dont :

Longueur du chemin : nombre de passage des paquets au travers des dispositifs (routeurs).

Fiabilité : elle s'exprime en taux d'erreur binaire (TEB) dans la transmission des bits. Certains liens peuvent être plus défaillants que d'autres.

Délais de routage : durée nécessaire pour transférer un paquet d'une source à une destination.

Bande passante : capacité d'une liaison à transferer des données.

Charge : degré d'activité d'une ressource ou d'un équipement réseau (routeur).

Coût : bien que le délais de transfert de certaines liaisons peut être important, certaines entreprises préfèrent les utiliser car elles sont moins coûteuses.

VII Conclusion

Le routage est le mécanisme par lequel des chemins sont sélectionnés dans un réseau pour acheminer les données d'un expéditeur jusqu'à un ou plusieurs destinataires. Ce chapitre nous a permis d'aborder les principes de base du routage.

Chapitre 4

Technologie Ethernet

I Introduction

Ethernet [1] est une technologie de réseau local qui est la plus répandue. La majeure partie du flux de données qui circule sur internet est issue d' un réseau Ethernet et aboutie sur un réseau Ethernet. Avec l'avancement des technologies (Fibre optique...), Ethernet assure maintenant de meilleurs débits ce qui lui permet d' être maintenant une norme des réseaux MAN et WAN. IEEE a publié la norme Ethernet sous le numéro 802.3. Toutes les autres normes Ethernet qui offrent de meilleures bandes passantes (100Mbits/s et plus) sont compatibles avec la norme Ethernet de base. Elles sont publiées par IEEE sous forme de suppléments à la norme 802.3. Exemple : 802.3u

Le principe d'Ethernet est de permettre à plusieurs hôtes d'utiliser un même média de transmission sans aucune interférence (accès multiple). Elle repose sur la transmission en bande de base, qui permet de transmettre le signal directement sur le média.

La norme Ethernet est compatible avec le modèle OSI et opère au niveau de la couche physique et de la partie inférieure de la couche liaison de données (MAC), elle doit donc répondre scrupuleusement aux besoins de ces deux couches.

II Verouillage de trame

Le verouillage de trame correspond au processus d'encapsulation qui s'effectue au niveau de la couche liaison de données du modèle OSI. La structure générique d'une trame (Figure 4-1) est composée de champs, chaque champ est un ensemble d'octets. Ils sont nommés comme suit :

- Champ de début de trame : est une séquence d'octets qui permet aux hôtes de signaler qu'ils s'apprêtent à transmettre une trame.
- Champ d'adresse : ce sont les informations d'identification (adresse MAC source et adresse MAC de destination).
- Champ de longueur ou type : le champ longueur indique où la trame doit se terminer, ainsi nous avons la longueur exacte de la trame en octets. Le champ type permet de préciser le protocole de la couche réseau utilisé par l'hôte source.
- Champ de données : représente les données d'application que doit envoyer l'utilisateur. Afin d'atteindre la longueur de trame minimale, des octets peuvent être ajoutés à ce champ. La sous couche LLC peut elle aussi y ajouter des informations de contôle qui permettent de faciliter l'acheminent du paquet jusqu'à la destination.
- Champ FCS (séquence de contrôle de trame) : une trame transmise peut contenir plusieurs erreurs dont les causes sont très variées. Ce champ contient un numéro appelé séquence de contrôle, celle-ci est calculée par l'ordinateur source de nombreuses façons à partir du contenu de la trame en cours. Après réception, cette séquence est recalculée et comparée à la séquence qui se trouve au niveau de la trame, la corruption d'un seul bit de la trame entrainera une différence entre les deux séquences de contrôle. Si les deux numéros concordent, il n'y a pas d'erreur de transmission. Dans le cas contraire, la trame est abondonnée par le récepteur et une nouvelle transmission est lancée grâce aux protocole orientés connexion de la couche transport. En effet, étant donné que ces protocoles ne reçoivent pas l'ACK attendu ils relancent la transmission.

Si nous revenons à la technologie Ethernet, la structure de la trame est pratiquement identique pour chacune des vitesses existantes. La structure de la trame pour la technologie Ethernet 802.3 est représentée dans la figure

A	B	C	D	E
Début de trame	Adresse	Type ou longueur	Données	FCS

FIG. 4-1 – Structure d'une trame générique

Préambule	SFD	Destination	Source	Type ou longueur	Données | Remplissage	FCS

FIG. 4-2 – Structure de la trame Ethernet 802.3

4-1.

- Préambule : est codé sur 7 octets. Il correspond à une suite de 1 et de 0 et permet d'établir la synchronisation.
- Délimiteur de début de trame : codé sur 1 octet. Correspond à la séquence de bits 10101011 et permet de marquer la fin du préambule.

  Remarque : les 8 octets précédents permettent aux version asynchrones d'Ethernet (10Mbits/s et moins) de synchroniser le circuit de réception avec les données reçues. Dans les versions synchrones (100Mbits/s et plus) ces octets sont toujours transmis par souci de compatibilité.
- Adresse MAC de destination : codée sur 6 octets. Elle peut être unicast, multicast ou broadcast.
- Adresse MAC source : codée sur 6 octets. L'adresse de l'hôte qui a transmis la trame.
- Champ longueur/Type : codé sur 2 octets. Si la valeur de ce champ est inférieure à 0x0600 (1536 en notation décimale), alors il permet d'indiquer la longueur de la trame 'nombre d'octets de données qui suit ce champ'. Si au contraire, la valeur de ce champ est supérieure ou égale à 1536 alors il permet d'indiquer le type de protocole de couche supérieure.
- Données : prend entre 46 et 1500 octets. Si la taille des données est inférieure à 46 octets une quantité de données appelées données de remplissage est insérée après les données de l'utilisateur afin d'assurer une

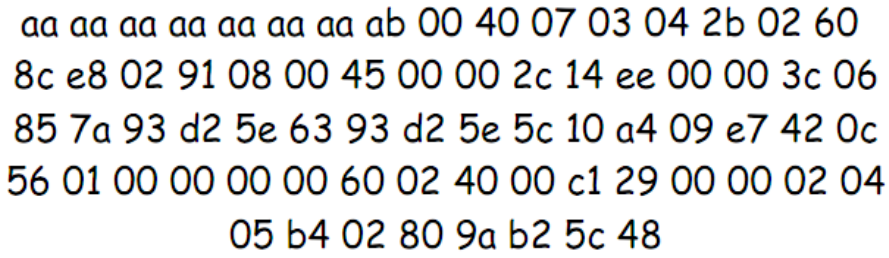


FIG. 4-3 – Exemple de trame Ethernet

longueur minimale de la trame. Inversement, les données ne doivent pas excéder 1500 octets afin de ne pas entrainer un dépassement de la taille maximale de la trame. Celle-ci doit être comprise entre 64 et 1518 octets.

– FCS : codé sur 4 octets. Calculé de part et d'autre afin de vérifier la validité de la trame. Contient le code de redondance cyclique (CRC), qui représente une des façons de calculer le numéro de séquence de contrôle de trame. Il consiste à exécuter des calculs sur les données.

Exemple

Voici une trame Ethernet :

- Que représente les 8 octets de début ?
- Donnez les adresses MAC du destinataire et de l'émetteur ?
- Donnez le protocole encapsulé dans la trame ?
- Que resprésentent les 4 octets de la fin ?

Corrigé

Préambule : aa aa aa aa aa aa aa ab

MAC destinataire : 00 40 07 03 04 2b

MAC source : 0260 8c e8 02 91

Type du protocole de couche supérieure : IP(0800)

9a b2 5c 48 représentent le CRC-32

III Principe de fonctionnement d'un réseau Ethernet

Sur un réseau, tous les équipements connectés sont dotés d'une adresse MAC pour chacune de leurs interfaces. Lorsqu'un hôte veut transmettre des données, il rajoute un en-tête comportant l'adresse MAC de l'hôte de destination. Il existe deux types de protocole MAC qui permette de gérer l'accès au média : déterministe et non déterministe.

Dans les protocoles déterministes, les différents hôtes sont disposés en anneau, un jeton circule d'un hôte à un autre afin de leur donner le droit d'émettre des données. Quand un hôte dispose du jeton et désire transmettre des données, il saisit le jeton, transmet les données pendant un temps bien préci et envois le jeton à l'hôte suivant sur l'anneau. Ce type de protocole est dit sans collision puisqu'une transmission au plus peut se faire à chaque instant. Token Ring et FDDI sont des exemples de protocoles déterministes.

Les protocoles non déterministes se basent sur le principe du premier arrivé premier servi. La méthode CSMA/CD (Détection de porteuse avec accès multiple et détection de collision) représentée sur la figure 4-4 est une méthode d'accès qui se base sur ce type de protocole. La technologie Ethernet utilise cette méthode d'accès pour accéder au media. La carte réseau de l'hôte qui désire transmettre des données guette l'absence de transmission ou de signal sur le média ' écoute de la porteuse', si le média est occupé l'hôte en question se mets en mode écoute et retante la transmission après un laps de temps aléatoire. Dans le cas où le média est libre, l'hôte commence sa transmission. Pour toutes les vitesses de transmission d'Ethernet, une transmission doit durer une tranche de temps au minimum pour aller jusqu'au point le plus éloigné du domaine de collision (point ou se produit une collision au dernier moment possible), retourner les fragments d'une éventuelle collision à la station émettrice afin de lui permettre de détecter la collision avant d'avoir fini d'envoyer sa trame. La tranche de temps est de 512 temps de bit pour Ethernet 10 et 100Mbits/s et elle est de 4096 temps de bit pour Ethernet 1000Mbits/s (cette tranche de temps est calculée en fonction de la longueur de câble maximale dans l'architecture de réseau légale la plus étendue).

Si deux hôtes transmettent au même moment (à cause par exemple du délai que met un signal à parcourir un câble ou du temps de latence qu'il faut au répéteur pour transmettre un signal d'un port à l'autre...) une collision survient. Après que chaque noeud émetteur reçoit les fragments de collision (rebuts), il tronque la transmission et envoie un signal de bourrage 32 bits (constitué de n'importe quelle séquence de bits tant qu'elle ne représente pas un FCS valide pour ce qui a déja été transmis) ce qui augmente l'amplitude du signal présent

sur le média et permet aux autre équipements du réseau de détecter la collision. Dans ce cas, l'algorithme de réemission temporisée est exécuté, les deux noeuds arrêtent de transmettre pendant un temps aléatoire définit par ce même algorithme et chaque hôte peut ensuite retenter la transmission. Les équipements impliqués dans une transmission sont nullement prioritaires lors d'une nouvelle tentative de transmission. Si après plus de 16 tentatives, la sous couche MAC n'arrive pas a transmettre les données, elle abondonne et envoie un message d'erreur à la couche réseau.

Une fois les données transmises sur le media, soit du premier coup, soit après plusieurs tentatives (<16), chaque équipement ou hôte du réseau va vérifier si l'adresse physique de destination transportée par la trame de données correspond à sa propre adresse physique. En présence de correspondance, la carte réseau de l'équipement effectue une copie de la trame et la transmet ensuite aux couches supérieures du modèle OSI. Dans le cas contraire, l'équipement ignore la trame. Cette opération de vérification ne nécessite aucun temps CPU, ce qui permet de réduire les temps de communication sur un réseau Ethernet.

IV Espacement intertrame

Lorsqu'une trame est envoyée, toutes les autres stations du réseau doivent attendre une durée de 96bits (soit 9,6 microsecondes dans un réseau Ethernet 10Mbits/s, ce temps est réduit proportionnellement à la vitesse du réseau) appelé écart d'espacement avant de transmettre la trame qui suit. Cet espacement est justement prévu pour donner le temps à toutes les stations de traiter la trame précédente et se préparer pour la trame suivante. Lorsqu'une collision survient et que toutes les stations attendent la fin de l'espacement intertrame, les stations à l'origine de la collision doivent observer un délai supplémentaire avant de tenter à nouveau de transmettre la trame entrée en collision. Ce délais est aléatoire afin que les stations impliquées dans la collision ne retransmettent pas leur trame une nouvelle fois au même moment, ce qui entrainera d'autres collision. L'intervalle qui sert a calculer ce délais est étendu à chaque tentative de retransmission.

V Types de collisions

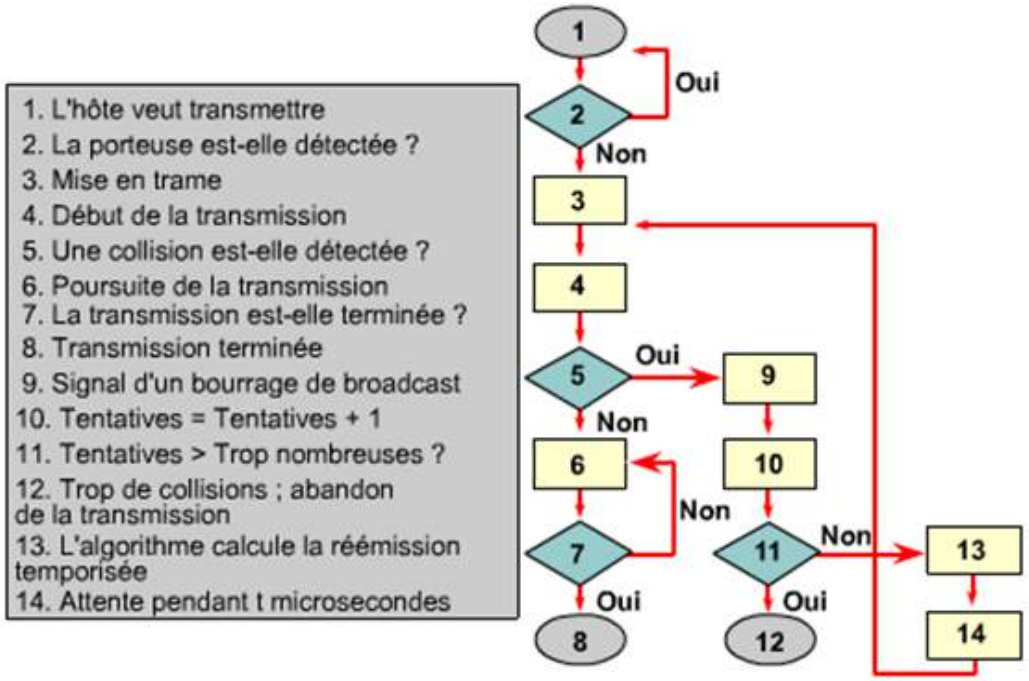


FIG. 4-4 – Organigramme le la méthode d'accès CSMA/CD [1].

Les trois types de collision sont les suivants : locale, distante et tardive.

Collision locale : sur du câble coaxial, le signal circule sur le câble jusqu'à ce qu'il rencontre un signal de l'autre station. Les ondes se chevauchent alors, annulant certaines parties du signal ou dédoublant d'autres parties. Le dédoublement du signal élève le niveau de tension de ce dernier au-delà du maximum autorisé. Cette condition de surtension est ensuite ressentie par toutes les stations du segment de câble local comme une collision. Sur un câble UTP, les collisions ne sont reconnues que lorsque la station fonctionne en mode half duplex. Si la station n'est pas en train de transmettre, elle ne peut pas détecter une collision locale. Une défaillance du câble due à une diaphonie excessive peut faire percevoir à une station sa propre transmission comme une collision locale (un signal est détecté en même temps à la réception et à la transmission). La carte réseau Ethernet retransmettra automatiquement une trame entrée en collision locale.

Collision distante : collision où la taille de la trame est inférieure à la longueur minimum d'octets et dont la somme de contrôle FCS est invalide, mais qui ne manifeste pas de signe de collision locale tel qu'une surtension ou une activité de réception/transmission simultanée. Cette sorte de collision résulte habituellement de collisions qui se produisent du côté éloigné d'une connexion répétée. Un répéteur ne transmettra pas un état de surtension.

Collisions tardives : ce sont les collisions qui se produisent après que les 64 premiers octets de données ont été envoyés. La carte réseau n'effectuera pas de retransmission pour ce type de collision.

VI Protocole ARP (couche réseau)

Quand un paquet est envoyé à la couche liaison de données pour être encapsulé dans une trame, le nœud consulte une table stockée dans sa mémoire pour connaître l'adresse de couche liaison de données qui est mappée à l'adresse IP de destination. Cette table est appelée table ARP ou cache ARP. La table ARP est stockée dans la mémoire vive (RAM) du périphérique. Chaque entrée, ou ligne, de la table ARP relie une adresse IP à une adresse MAC. La relation entre les deux valeurs s'appelle un mappage. Autrement dit, si vous choisissez une adresse IP dans la table, vous trouverez l'adresse MAC correspondante. La table ARP stocke temporairement (dans la mémoire cache) le mappage des périphériques du réseau local.

Pour lancer la procédure, un nœud émetteur tente de trouver l'adresse MAC associée à une adresse IPv4

de destination. Si ce mappage se trouve dans la table, le nœud utilise l'adresse MAC comme destination MAC dans la trame qui encapsule le paquet IPv4. La trame est ensuite codée sur le support réseau.

Mise à jour de la table ARP

La table ARP est mise à jour de manière dynamique. Un périphérique dispose de deux méthodes pour obtenir des adresses MAC. La première consiste à surveiller le trafic sur le segment du réseau local. Quand un noeud reçoit des trames en provenance du support, il enregistre les adresses IP source et MAC dans la table ARP sous forme de mappage. Au fur et à mesure que les trames sont transmises sur le réseau, le périphérique remplit la table ARP de paires d'adresses.

L'envoi d'une requête ARP permet également d'obtenir une paire d'adresses, comme l'illustre l'exemple suivant.

La commande arp-a permet de connaitre le contenu de la table ARP sous windows.

VI.1 Exemple concret

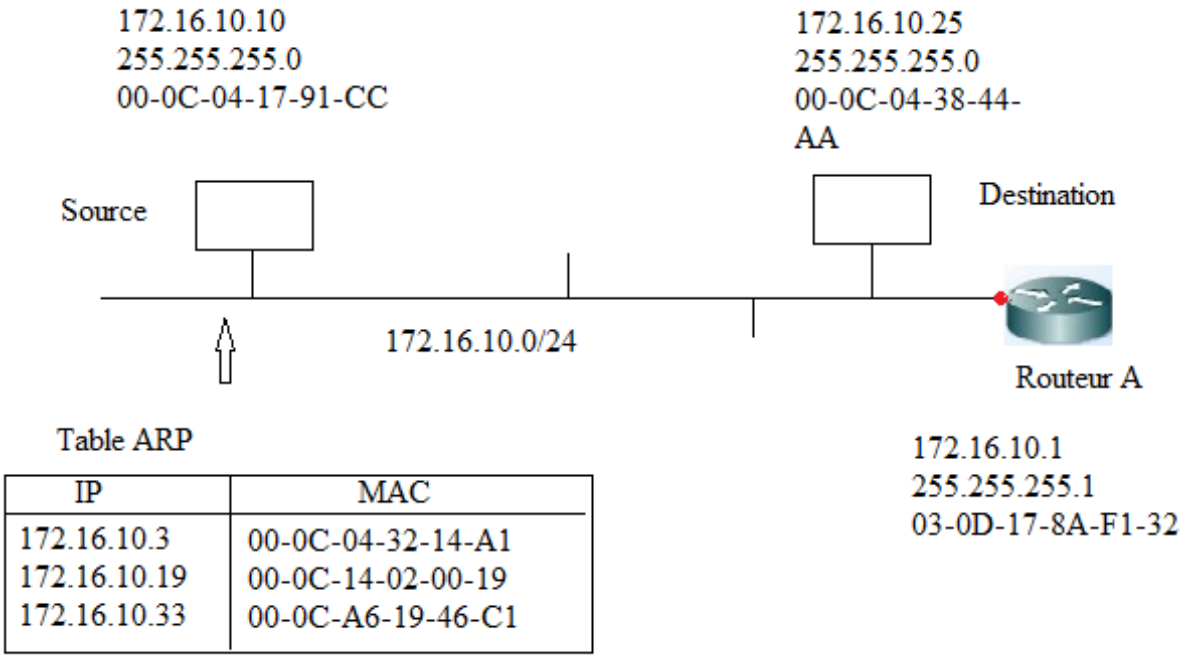
Au niveau de cette sous-section, nous allons voir concrêtement comment se font les échanges de trames Ethernet. Nous prenons pour cela deux cas : un premier cas ou l'hôte de destination se trouve sur le même réseau LAN que l'hôte source et un deuxième cas ou les hôtes source et destination se trouvent sur des réseaux LAN distants.

La figure 4-5 représente un réseau Ethernet. Supposons que l'hôte source ayant l'adresse IP 172.16.10.10 veuille communiquer avec l'hôte de destination 172.16.10.25.

L'hôte source doit pouvoir déterminer si l'adresse IP de destination finale se situe sur le même réseau que lui. Pour cela, l'hôte source compare la partie réseau de son adresse IP avec la partie réseau de l'adresse IP de l'hôte de destination moyennant son propre masque de sous-réseau, comme suit :

	172.16.10.10	172.16.10.25
ET	255.255.255.0	255.255.255.0
	172.16.10.0	172.16.10.0

Le résultat montre bien que nous sommes sur le même réseau. L'hôte source peut envoyer directement son



IP	MAC
172.16.10.3	00-0C-04-32-14-A1
172.16.10.19	00-0C-14-02-00-19
172.16.10.33	00-0C-A6-19-46-C1

FIG. 4-5 – Exemple de réseau LAN (remise directe)

paquet à l'hôte de destination, nous parlons dans ce cas de remise directe.

L'hôte source connait bien a ce stade les deux adresses IP source et destination, il a cependant besoin de l'adresse MAC de destination pour pouvoir encapsuler le paquet IP qu'il veut envoyer dans une trame Ethernet. Il commence par chercher tout d'abord l'adresse IP de destination dans sa table ARP (qui ne garde que les adresses du même réseau/ sous réseau). Dans cet exemple, l'adresse IP de destination ne figure pas au niveau de la table ARP. L'hôte source envoie donc une requête ARP portant sur l'adresse IP 172.16.10.25, comme suit :

En-tête Ethernet		
@MAC dest	@MAC source	Type de trame
FF-FF-FF-FF-FF-FF	00-0C-04-17-91-CC	0x806

Données Ethernet - requête/réponse ARP 28 octets				
... En tête ARP	@MAC source	@IP source	@MAC dest	@IP dest
$op = 1$	00-0C-04-17-91-CC	172.16.10.10		172.16.10.25

Indication : pour le champ "En tête ARP", les codes sont comme suit :

Requête ARP $op = 1$

Réponse ARP $op = 2$

Requête RARP $op = 3$

Réponse RARP $op = 4$

La réponse ARP est la suivante :

En-tête Ethernet		
@MAC dest	@MAC source	Type de trame
00-0C-04-17-91-CC	00-0C-04-38-44-AA	0x806

Données Ethernet - requête/réponse ARP 28 octets				
... En tête ARP	@MAC source	@IP source	@MAC dest	@IP dest
$op = 2$	00-0C-04-38-44-AA	172.16.10.25	00-0C-04-17-91-CC	172.16.10.10

L'hôte source reçoit de cette façon l'adresse MAC de l'hôte de destination qu'il rajoute dans sa table ARP. L'hôte source peut maintenant encapsuler le paquet IP dans une trame Ethernet et envoyer les données.

En-tête Ethernet			
@MAC dest	@MAC source	Autre Inf	...
00-0C-04-38-44-AA	00-0C-04-17-91-CC		

			Données	En-queue Ethernet
Inf d'en-tête IP	@IP source	@IP dest	Données	FCS
	172.16.10.10	172.16.10.25		

Si les deux hôtes se situent sur des réseaux différents. comme sur la figure 4-6.

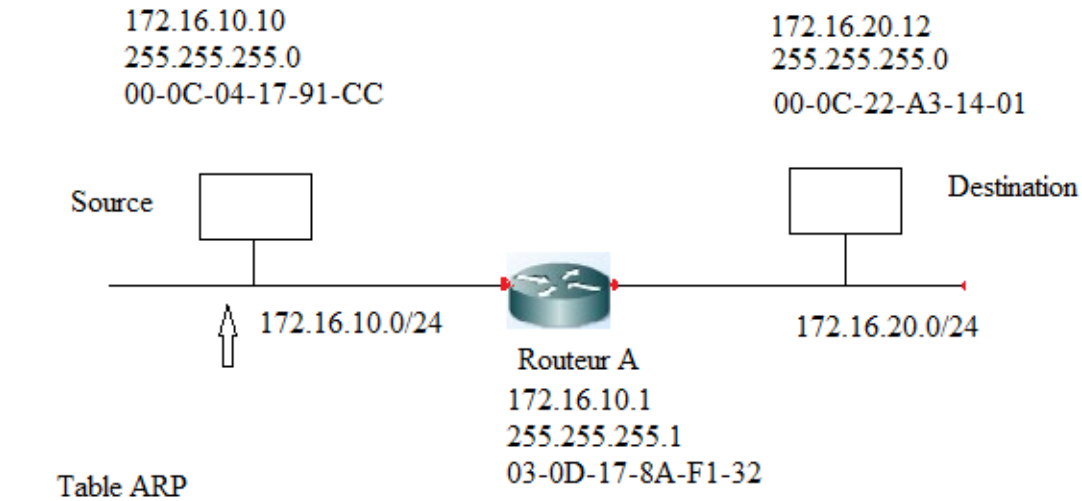


Table ARP

IP	MAC
172.16.10.3	00-0C-04-32-14-A1
172.16.10.19	00-0C-14-02-00-19
172.16.10.33	00-0C-A6-19-46-C1

FIG. 4-6 - Exemple de remise indirecte.

L'émetteur doit déterminer si l'@IP de destination finale se situe sur le même réseau que lui. Si la destination

se trouve sur un réseau distant, l'émetteur ne peut pas envoyer directement le paquet, il va donc chercher l'adresse IP de la passerelle par défaut. En général les hôtes disposent dans leur configuration de l'@IP de la passerelle par défaut (routeur). L'émetteur cherche l'@IP de la passerelle dans sa table ARP pour connaitre son adresse MAC. Si elle est présente, il encapsule le paquet IP dans la trame Ethernet et envoie la trame à la passerelle par défaut. Sinon, il envoie une requête ARP pour connaitre l'adresse MAC de la passerelle par défaut.

	172.16.10.10	172.16.20.12
ET	255.255.255.0	255.255.255.0
	172.16.10.0	172.16.20.0

L'hôte source sait maintenant que l'hôte de destination se trouve sur un réseau distant. Il va donc chercher l'adresse IP de la passerelle dans sa table ARP. Elle ne s'y trouve pas, donc l'hôte source envoie (diffuse) une requête ARP.

En-tête Ethernet		
@MAC dest	@MAC source	Type de trame
FF-FF-FF-FF-FF-FF	00-0C-04-17-91-CC	0x806

Données Ethernet - requête/réponse ARP 28 octets				
En tête ARP	@MAC source	@IP source	@MAC dest	@IP dest
$op = 1$	00-0C-04-17-91-CC	172.16.10.10		172.16.10.1

La réponse ARP est la suivante :

En-tête Ethernet		
@MAC dest	@MAC source	Type de trame
00-0C-04-17-91-CC	03-0D-17-8A-F1-32	0x806

Données Ethernet - requête/réponse ARP 28 octets				
En tête ARP	@MAC source	@IP source	@MAC dest	@IP dest
$op = 2$	03-0D-17-8A-F1-32	172.16.10.1	00-0C-04-17-91-CC	172.16.10.10

L'hôte source entre l'adresse IP et l'adresse MAC de la passerelle dans sa table ARP. Il dispose maintenant de tous les éléments pour encapsuler le paquet IP dans une trame Ethernet.

En-tête Ethernet		
@MAC dest	@MAC source	Autre Inf
03-0D-17-8A-F1-32	00-0C-04-17-91-CC	

Données				En-queue Ethernet
Inf d'en-tête IP	@IP source	@IP dest	Données	FCS
	172.16.10.10	172.16.20.12		

Maintenant le routeur A achemine le paquet en fonction du destinataire vers une de ses interfaces s'il le peut.

VII Calcul de la somme de contrôle

Lors d'une transmission de données sur un support de transmission, des erreurs peuvent se produire. Pour cette raison, des mécanismes sont mis en place pour vérifier la validité des trames reçues.

Comme nous l'avons dit précédemment, une redondance est rajoutée en fin de trame (FCS). Cette redondance est calculée moyennant un procédé de calcul spécifique [4] [5]. Le récepteur vérifie à l'aide du même procédé de calcul que le message qu'il a reçu est bien le message qui a été envoyé.

Plusieurs procédés de calcul de redondance existent, nous citons ici quelques uns.

VII.1 Codes à contrôle de parité

VRC (Vertical Redundancy Check) : en code ASCII, les caractères sont définis sur 7 bits. Un huitième bit sera rajouté et représentera la parité du caractère. Si le nombre de bits de données à 1 est pair, le bit de parité est donc positionné à 0, sinon il est positionné à 1. Ce bit permet de savoir si un nombre impair d'erreur s'est produit.

LRC (Longitudinal Redundancy Check) : son principe est similaire à celui du VRC, excepté que la parité sera calculée pour l'ensemble des bits de même rang de tous les caractères.

Exemple

Supposons que le message à transmettre est "HELLO".

Lettre	Lettre codée	VRC
H	0001001	0
E	1010001	1
L	0011001	1
L	0011001	1
O	1111001	1
LRC	0100001	0

La trame que nous transmettrons sera la suivante :

		0001001 0 1010001 1 ...	LRC :0100001 0

Si deux bits (ou un nombre pair de bits) venaient à se modifier simultanément lors d'une transmission de données, aucune erreur n'est alors détectée. Ce système de contrôle ne permet que de détecter les erreurs en nombre impair, il détecte alors que 50% des erreurs.

VII.2 Codes polynômiaux

Appelés aussi CRC (Cyclic Redundancy Check), ils sont utilisés par la plupart des protocols du moment. Ils permettent de détecter les erreurs sur plusieurs bits.

Ils se basent sur l'utilisation d'un polynôme $G(x)$ d'ordre $'r'$, connu de l'émetteur et du récepteur, il s'écrit sous la forme :

$$G(x) = a_r x^r \bigoplus a_{r-1}.x^{r-1} \bigoplus ... \bigoplus a_0$$

où

$$\forall i \in \{0...r\}, a_i \in \{0,1\}$$

Nous avons aussi un polynôme $B(x)$ associé aux données binaires à transmettre. Soient $b_n...b_0$ ces derniers. Le polynôme s'écrit alors sous la forme :

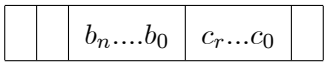
$$B(x) = b_n x^n \bigoplus ... \bigoplus b_0 x^0$$

$R(x)$ correspond au polynôme reste qui va être calculé et rajouté en fin de trame. $R(x)$ est le reste de la division Euclidienne de $x^r B(x)$ par $G(x)$. Tel que :

$$R(x) = x^r B(x) \bmod G(x) = c_r x^r \bigoplus ... \bigoplus c_0 x^0$$

Les bits $c_{r-1}...c_0$ correspondent aux champs FCS qui sera rajouté en fin de trame.

La trame à transmettre est équivalente à :



Etant donné que pendant la transmission, la trame peut subir quelques dégradations, la trame reçue se présente comme suit :

		$b_n^{'}....b_0^{'}$	$c_r^{'}...c_0^{'}$	

Le récepteur peut calculer l'expression suivante afin de vérifier la validité des données reçues :

$$(x^r B^{'}(x) + R^{'}(x))/G(x)$$

Si le reste de ce calcul est nul alors il y a absence d'erreurs. Si par contre, le reste n'est pas nul, il y a erreur. Il faut dans ce dernier cas demander la retransmission de la trame.

Exemple

ATM : CRC-8 $G(x) = x^8 + x^2 + x + 1$

Ethernet : CRC-32 $G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$

1) Message à transmettre : M=1101.

$B(x) = x^3 \bigoplus x^2 \bigoplus 1$.

Le polynôme générateur choisi est $G(x) = x^3 \bigoplus x \bigoplus 1$. Il est d'ordre $r = 3$.

La division euclidienne de $x^r B(x)$ par $G(x)$ donne $x^3 \bigoplus x^2 \bigoplus x \bigoplus 1$.

2) Quelle est la clé associée au Message à transmettre M=110111, sachant que le polynôme générateur est : $G(x) = x^2 + x + 1$

$B(x) = x^5 + x^4 + x^2 + x + 1$

$B(x).x^2 = x^7 + x^6 + x^4 + x^3 + x^2$

La division euclienne de $B(x).x^2$ par $G(x)$:

La clé est donc 11. Le mot à envoyer est 110111 **11**.

VIII Conclusion

Ce chapitre nous a permis de nous familiariser avec la technologie Ethernet, qui est la plus répandue actuellement. Nous avons abordé les principaux champs d'une trame Ethernet ainsi que le principe de fonctionnement

de ce type de réseau. L'exemple pris nous a permis de voir un réel échange de trame Ethernet et de mieux comprendre. Enfin nous avons traité différents façons de calculer le champs de redondance cyclique, qui rappelons le permet de s' assurer de l'intégrité des données reçues et d' y remedier en cas d' erreur de transmission.

Chapitre 5

Transmission du signal

I Introduction

La couche physique reçoit l'information à transmettre sous forme d'une suite de bits représentés sous forme de nombres écrits en binaire (0 et 1). Si les distances à parcourir sont faibles (réseau LAN), il est possible de représenter cette suite de bits sous forme d'un signal éléctrique numérique à transmettre. Cette transmission est dite en bande de base [2], ce qui veut dire que le signal est envoyé directement sans procéder à une quelconque modulation et sans aucune transposition de fréquence. Un signal éléctrique numérique se présente comme une suite de niveaux de tension ayant des amplitudes choisies parmi un nombre restreint de possibilités d'amplitudes. De plus, un signal numérique est un signal variant de façon discontinue dans le temps. Il est possible d'augmenter légèrement les distances en ayant recours à des répéteurs.

Le codage en bande de base ne peut être utilisé pour la transmission à des vitesses très élevées ou sur de très grandes distances. Dans ces cas, il faut transformer le signal numérique en signal analogique grâce à la modulation. Un signal analogique est un signal qui vari de manière continue dans le temps.

Un signal numérique peut être transformé en un signal analogique (CNA : convertisseur numérique analogique), inversement, un signal analogique peut être numérisé au moyen d'échantillonage, de quantification (CAN : convertisseur analogique numérique) et de codage. Dans ce cas, l'aspect numérique du signal ne sert

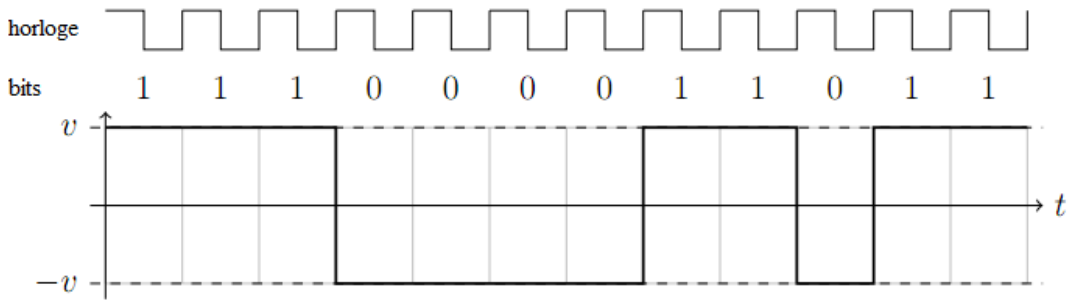


FIG. 5-1 – Chronogramme du code NRZ binaire.

qu'au stockage et au traitement des données puisque cet aspect est plus facile à travailler.

II Codage

La valence représente le nombre de niveaux de tension possibles.

II.1 Codage NRZ

La valence du codage NRZ vaut 2. Un bit ayant une valeur égale à 1 est traduit par une tension $+v$. Un bit ayant une valeur 0 est traduit par une tension $-v$.

Exemple

II.2 Codage NRZI

La valence de ce type de codage est 2. Un bit ayant une valeur égale à +1 est traduit par une tension inverse de celle du bit précédent. Un bit ayant une valeur égale à -1 est traduit par une tension similaire à celle du bit précédent, en d'autres termes, la tension précédente est conservée.

Exemple

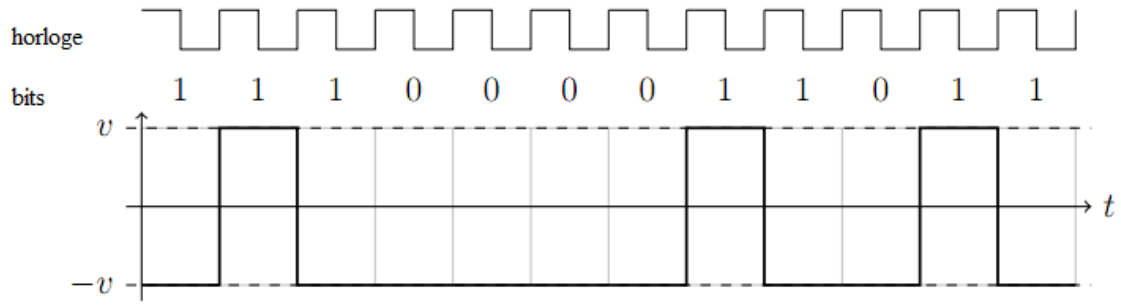


FIG. 5-2 – Chronogramme du code NRZI.

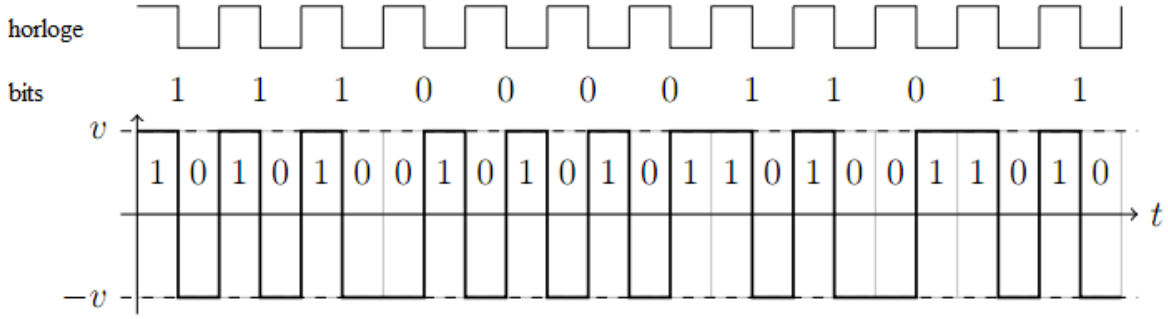


FIG. 5-3 – Chronogramme du code Manchester.

II.3 Codage Manchester

Ce code a une valence de 2. Dans ce type de codage, le principe est de faire une transition du signal d'un niveau de tension à un autre pour chaque bit transmis. Un bit ayant une valeur de 1 provoque une transition de $+v$ à $-v$. Un bit ayant une valeur 0 provoque une transition de $-v$ à $+v$.

Exemple

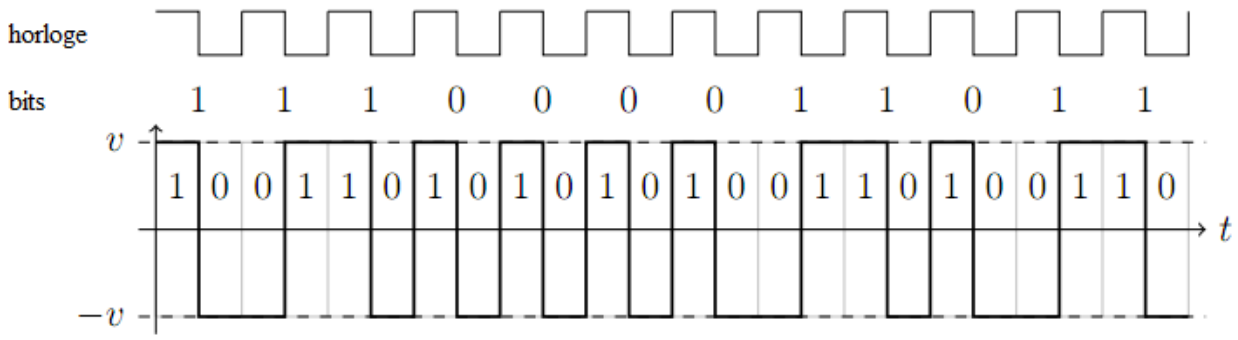


FIG. 5-4 – Chronogramme du code Manchester differentiel.

II.4 Codage Manchester differentiel

Ce code a une valence de 2. Un bit ayant une valeur de +1 est traduit par une transition inverse d'un niveau de tension à un autre par rapport à la transition du bit précédent. Un bit ayant une valeur 0 conserve la même transition du bit précédent.

Exemple

Exercice

- Ethernet est basé sur le codage Manchester (simple).

- Tensions -0.85 et +0.85 volts.

Coder en Manchester et Manchester différentiel la séquence 10000101111.

III Modulation

Au moment d'une transmission sur de grandes distances, l'antenne d'émission transforme le signal éléctrique numérique en onde éléctromagnétique, l'antenne de réception effectue l'opération inverse, le récepteur sélectionne la fréquence porteuse et démodule l'information qui y est inscrite. La fréquence porteuse est générallement une fréquence beaucoup plus grande que celle du signal d'entrée, ce qui implique une transposition de fréquence. Il existe plusieurs types de modulation [4] dont :

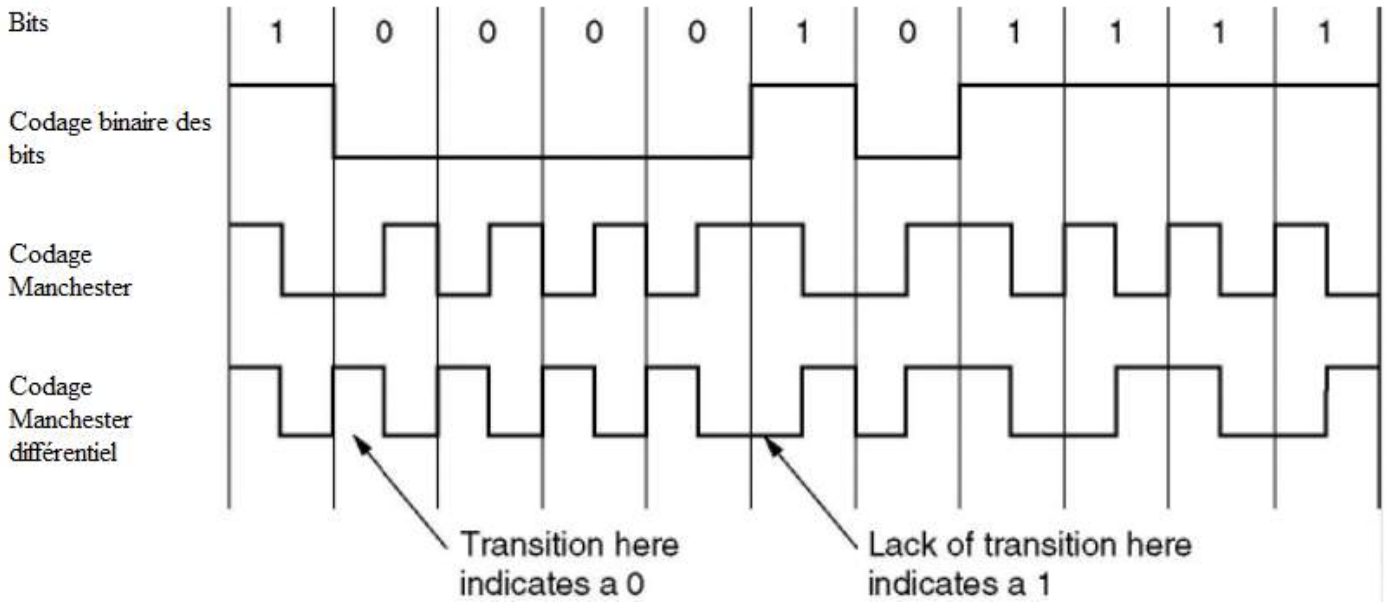


FIG. 5-5 – Codage Manchester et Manchester différentiel.

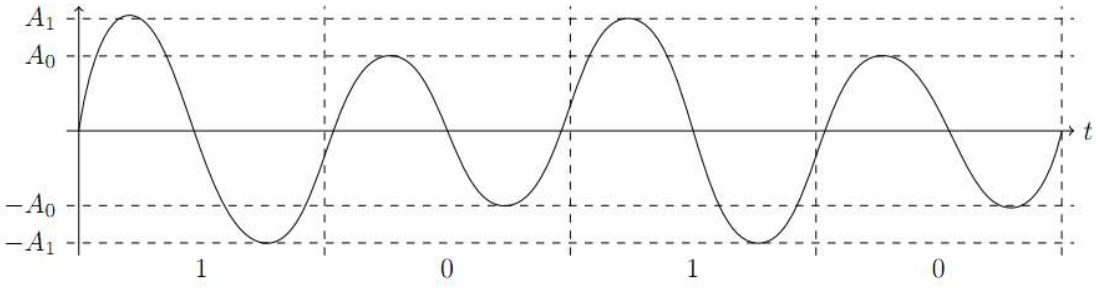


FIG. 5-6 – Modulation d'amplitude.

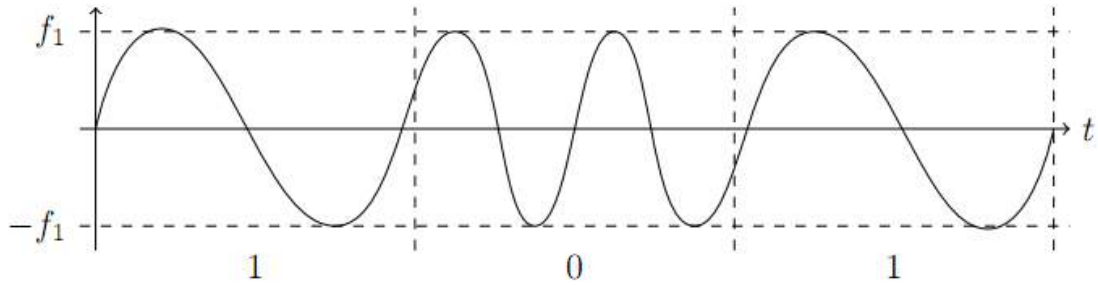


FIG. 5-7 – Modulation de fréquence.

III.1 Modulation d'amplitude (ASK : Amplitude Shift Keying)

Dans cette modulation, nous avons au moins deux niveaux d'amplitude A_0 et A_1, comme montré sur la figure 5-6.

III.2 Modulation de fréquence (FSK : Frequency Shift Keying)

Comme montré sur la figure 5-7, les deux niveaux logiques 0 et 1 sont représentés par deux fréquences opposées f_1 et $-f_1$.

III.3 Modulation de phase (PSK : Phase Shift Keying)

Elle associe à une valeur binaire 0 ou 1 une valeur de phase de la porteuse.

Des combinaisons plus complexes sont utilisées pour optimiser le débit vis-à-vis de la bande passante.

IV Multiplexage

Le multiplexage consiste à transmettre sur une voie de communication unique des signaux provenant de plusieurs voies, ainsi, plusieurs utilisateurs peuvent partager une même ressource. Nous avons principalement trois techniques de multiplexage : TDMA (Time Division Multiple Access), FDMA (Frequency Division Multiple Access) et CDMA(Code Division Multiple Access).

IV.1 TDMA

Cette méthode de multiplexage(figure 5-8) regroupe plusieurs canaux bas débit sur un seul canal à débit plus élevé. Le principe consiste à allouer à chaque utilisateur un time slot spécifique durant lequel il transmettra ses données. Un utilisateur qui transmettra durant son time slot occupera la bande spectrale disponible en totalité.

La TDMA requièrt de transmettre une séquence de référence périodiquement, celle-ci permet de définir les trames et de réaliser la synchronisation. Une trame est composée de plusieurs time slots. Ces derniers sont alloués à différents utilisateurs pour tansmettre leur données. Chaque time slot fini avec un interval de guarde qui permet d'éviter la perte de données et les interférences avec le prochain utilisateur. La séparation des utilisateur est faite donc dans le domaine temporel.

Exemple

Regrouper 24 voies à 64 kbits/s en une voie à 1.544 Mbits/s.

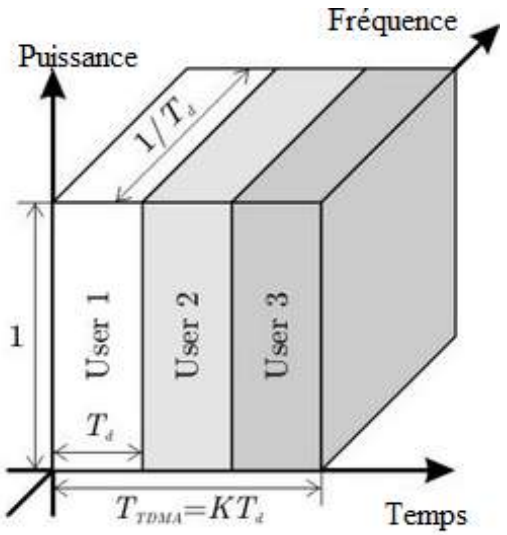


FIG. 5-8 – Principe de la TDMA.

IV.2 FDMA

Dans cette technique de multiplexage (figure 5-9), chaque utilisateur transmet ses données dans une petite portion de la bande spectrale disponible. La transmission n'a cependant aucune limite dans le temps. Les différents utilisateurs sont séparés dans le domaine fréquentiel.

Pour faire cela, la bande de fréquence disponible est divisée en un certain nombre de sous bandes ou sous canaux. Chaque sous bande est affectée à un utilisateur de manière exclusive suivant le besoin.

Exemple

Une ligne téléphonique possède une bande passante d'environ 1Mhz dont seulement 4 Khz exploités pour la communication téléphonique. ADSL a justement été créer dans le but d'utiliser les Khz restants en se basant sur le multiplexage fréquentiel FDMA.

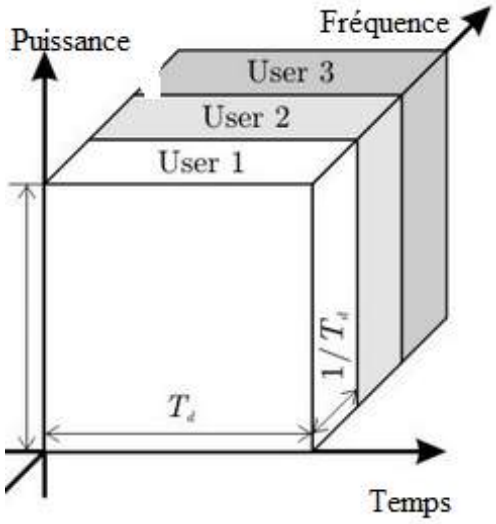


FIG. 5-9 – Principe de la FDMA.

IV.3 CDMA

La technique de multiplexage CDMA (figure 5-10) permet la transmission simultanée de plusieurs canaux, grâce au principe de l'étalement par code (DS-SS : Direct Sequence Spread Spectrum). Cet étalement se fait en utilisant des codes pseudo-orthogonaux ou orthogonaux (Walsh-Hadamard, Gold...). Ces derniers favorisent une interférence nulle entre utilisateurs.

Les signaux à transmettre sont étalés est réparti sur l'ensemble du temps et des fréquences disponibles. La somme de tous ces signaux va être transmise sur un seul et même canal de transmission.

V Conclusion

Ce chapitre nous a permi de comprendre le principe des opérations qui se font au niveau de la couche physique, dont : la modulation, le codage, le multiplexage. Le choix de la technique dependra du type de réseau et du support de transmission.

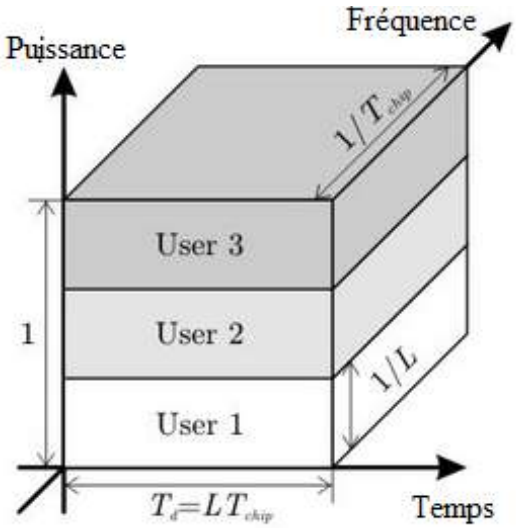


FIG. 5-10 – Principe de la CDMA.

Bibliographie

[1] Cisco Certified Network Associate Routing & Switching (CCNA) .

[2] M. Joindot, A. Glavieux, "Introduction aux communications numériques", DUNOD, Paris, 2007.

[3] Cisco Systems, et al, "Technologies des interconnexions réseaux", Cisco Press, 2001.

[4] L. Petrucci, "Cours de réseaux", IUT de Villetaneuse, 2012.

[5] N. Baudru, " Protocole de liaison de données", ESIL, 2010-2011.