SOMMAIRE

REMERCIEMENT 2
CHAPITRE I : GENERALITES 3
INTRODUCTION 3
CLASSIFICATION DES RESEAUX 3
LE MODELE OSI DE L'ISO 4
Pourquoi une normalisation ? 4
Mode de travail du modèle OSI (modèle en 7 couches) 4
TOPOLOGIES RESEAUX 6
Câblage en bus 6
Câblage en anneau 6
Câblage en étoile 7
Avantages et inconvénients de chaque topologie 8
LE STANDARD ETHERNET 9
CHAPITRE II- LE MATERIEL 9
Les Câbles 9
Câbles blindés coaxiaux 9
Câbles paires torsadées 10
Câble fibres optiques 12
Les cartes réseaux 14
Les éléments actifs 14
HUB 14
SWITCH 15
Routeur 15
Chapitre III : Les normes logicielles 16
Architectures réseaux 16
Réseaux poste à poste (peer to peer) 16
Réseaux à serveurs dédiés 16
Les protocoles : 19
NetBEUI 19
IPX/SPX 19
AppleTalk 20
TCP/IP 20
Les classes des réseaux 22
Le masque sous réseaux 24
COMMENT FONCTIONNE UNE ADRESSE IP ? 28
VPN 31
CONCLUSION 33

Mrad Brahim

Remerciement

En préambule à ce mémoire, je souhaitais adresser mes remerciements les plus sincères aux personnes qui m'ont apporté leur aide et qui ont contribué à l'élaboration de ce mémoire ainsi qu'à la réussite de cette formidable année de formation.

Je tiens à remercier sincèrement Mme **Aycha Amri**, en tant que Directrice de Centre Sectoriel de formation en électronique de Sousse.

Mes remerciements s'adressent également à tous mes formateurs :

Mr M. Slama

Mr Med. Lahsini

Mr M. Rchid .

J'exprime ma gratitude à tous les consultants et internautes rencontrés lors des recherches effectuées et qui ont accepté de répondre à mes questions avec gentillesse.

Je n'oublie pas mes parents pour leur contribution, leur soutien et leur patience.

Enfin, j'adresse mes plus sincères remerciements à tous mes proches et amis, qui m'ont toujours soutenue et encouragée au cours de la réalisation de ce mémoire.

Merci à tous et à toutes.

Mrad Brahim

Chapitre I : Généralités

Introduction

Un réseau en général est le résultat de la connexion de plusieurs machines entre elles, afin que les utilisateurs et les applications qui fonctionnent sur ces dernières puissent échanger des informations.

En effet, dans un réseau on peut :

- S'échanger des messages,
- Discuter,
- Transférer des fichiers,
- Partager des imprimantes,
- Avoir accès à Internet à partir d'une seule connexion,
- Jouer,
- Faire de la téléassistance, …

Le terme réseau peut désigner plusieurs choses en fonction de son contexte (l'ensemble des machines, l'infrastructure informatique d'une organisation avec les protocoles qui sont utilisés, la façon dont les machines d'un site sont interconnectées,…).

Classification des réseaux

LAN (local area network) : Réseaux locaux dont l'étendue est faible géographiquement (Immeuble, Campus…)

MAN (métropolitain area network) : Permet d'interconnecter plusieurs réseaux locaux d'une ville, d'une région. Son étendue ne dépasse pas 100Km

WAN (wide area network) : Son étendue dépasse les 100Km exemple : Internet

Mrad Brahim

Le modèle OSI de l'ISO

Pourquoi une normalisation ?

De plus en plus d'entités ont besoin d'échanger des informations entre elles. Des gens ont eu l'idée d'essayer de recenser les différents problèmes que l'on trouvait lorsque que l'on veut mettre des machines en réseau. De cette réflexion est sortie le modèle OSI de l'ISO.

Mode de travail du modèle OSI (modèle en 7 couches)

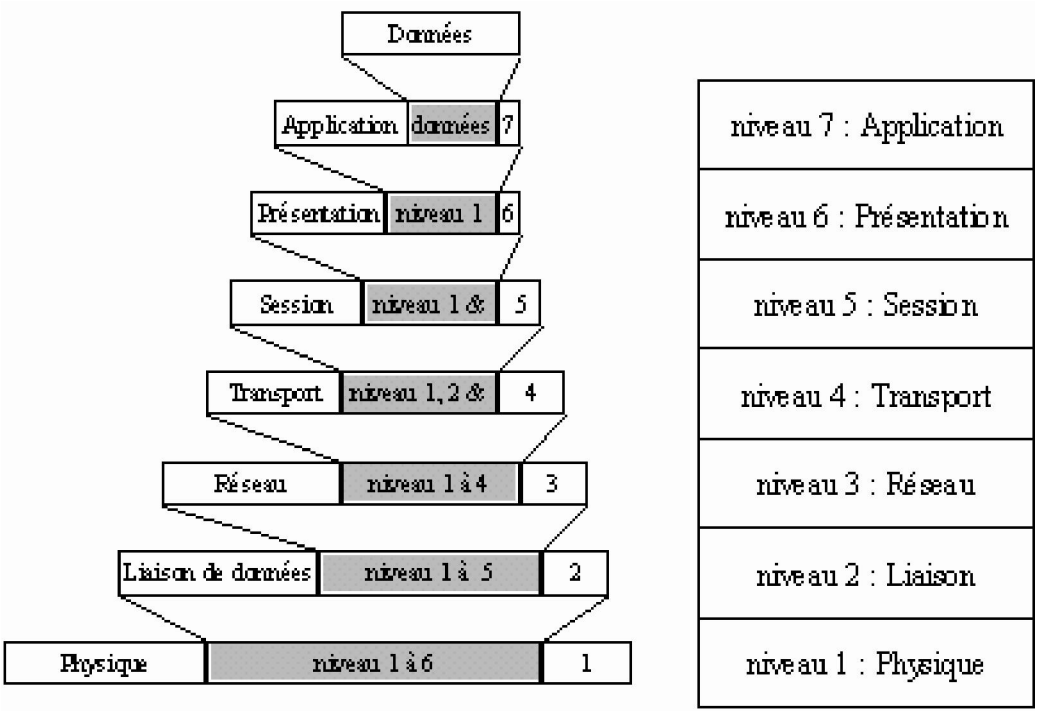
Pour faire circuler l'information sur un réseau, on fragmente l'information en petits morceaux (*paquets*), chaque paquet est envoyé séparément sur le réseau, les paquets sont ensuite réassemblés sur la machine destinataire, on parle réseau à *commutations de paquets.*

Le modèle OSI est un modèle à 7 couches qui décrit le fonctionnement d'un réseau à commutations de paquets. Chacune des couches de ce modèle représente une catégorie de problème que l'on rencontre dans un réseau.

Découper les problèmes en couche présente des avantages. Lorsque l'on met en place un réseau, il suffit de trouver une solution pour chacune des couches.

L'utilisation de couches permet également de changer de solution technique pour une couche sans pour autant être obligé de tout repenser.

Chaque couche garantit à la couche qui lui est supérieur que le travail qui lui a été confié a été réalisé sans erreur.



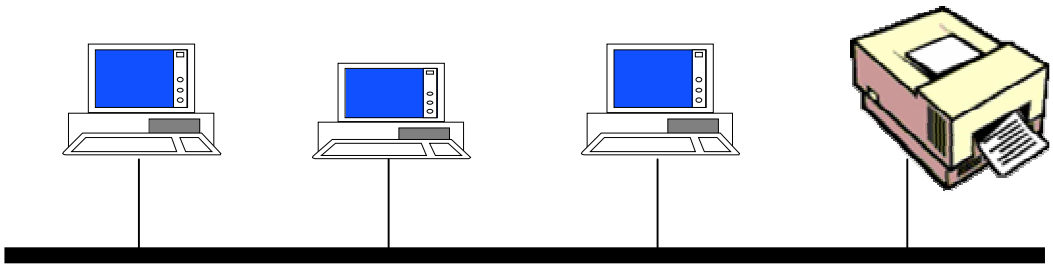
- **Niveau 7 (application)**: gère le format des données entre logiciels.
- **Niveau 6 (présentation)**: met les données en forme, éventuellement de l'encryptage et de la compression, par exemple mise en forme des textes, images et vidéo.
- **Niveau 5 (session)**: gère l'établissement, la gestion et coordination des communications
- **Niveau 4 (transport)**: s'occupe de la gestion des erreurs, notamment avec les protocoles UDP et TCP/IP
- **Niveau 3 (réseau)**: sélectionne les routes de transport (routage) et s'occupe du traitement et du transfert des messages: gère par exemple les protocoles IP (adresse et le masque de sous réseau) et ICMP. Utilisé par les routeurs et les switchers manageables.
- **Niveau 2 (liaison de données)**: utilise les **adresses MAC**. Le message Ethernet à ce stade est la trame, il est constitué d'un en-tête et des informations. L'en-tête reprend l'adresse MAC de départ, celle d'arrivée + une indication du protocole supérieur.

Mrad Brahim

- **Niveau 1 (physique)**: gère les connections matérielles et la transmission, définit la façon dont les données sont converties en signaux numériques: ça peut-être un câble coaxial, paires sur RJ45, onde radio, fibre optique, ...

Topologies réseaux

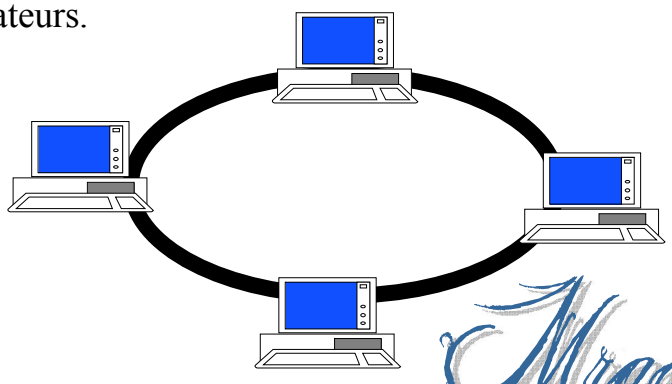
Câblage en bus



Les ordinateurs sont connectés les uns à la suite des autres le long d'un seul câble appelé segment. Un message émis par un ordinateur est diffusé sur le câble ; C'est au destinataire de reconnaître le message qui le concerne.
Cette topologie a pour avantage d'être facile à mettre en oeuvre et de posséder un fonctionnement simple. En revanche, elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, l'ensemble du réseau en est affecté.

Câblage en anneau

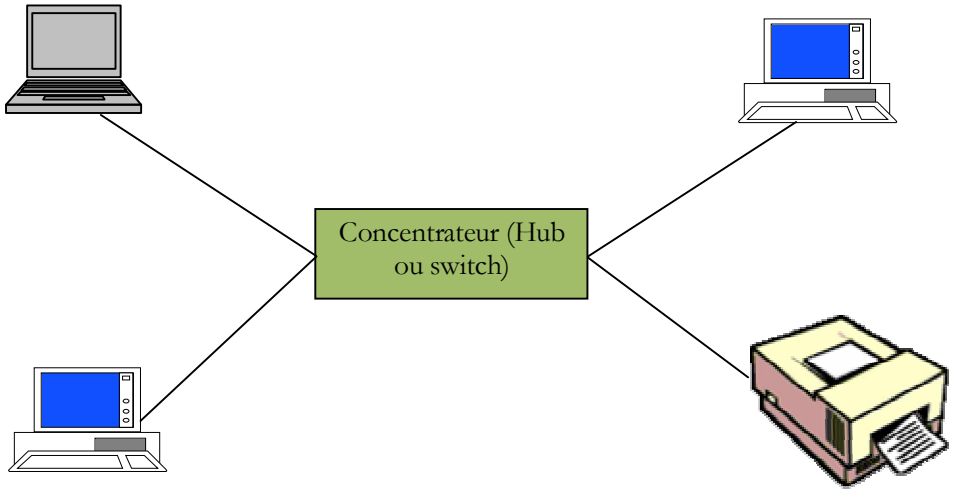
Dans cette architecture, les ordinateurs sont reliés sur une seule boucle de câble ; Les signaux se déplacent le long de la boucle dans une direction et passe par chacun des ordinateurs.



Mrad Brahim

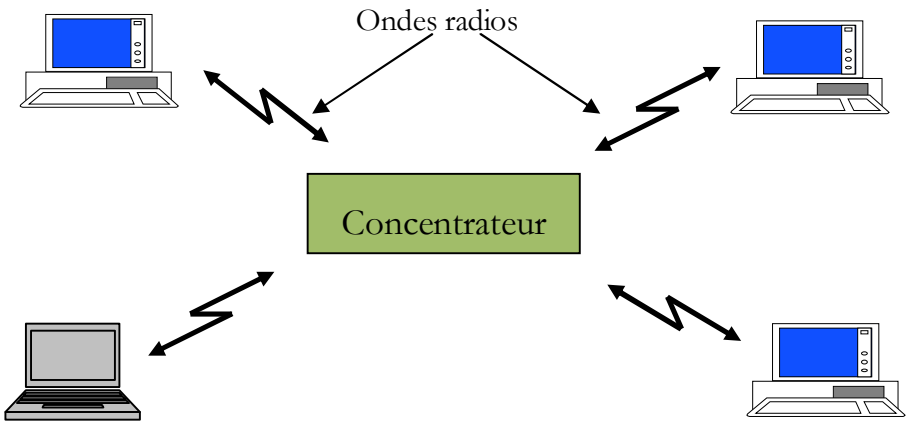
En réalité, dans une topologie anneau, les ordinateurs ne sont pas reliés en boucle, mais sont reliés à un **répartiteur** (appelé *MAU*, *Multi station Access Unit*) qui va gérer la communication entre les ordinateurs qui lui sont reliés en impartissant à chacun d'entre-eux un temps de parole.

Câblage en étoile



Dans une topologie en étoile, les ordinateurs sont connectés par des segments de câble à un composant central, appelé concentrateur (Hub ou switch).

Remarque : WIFI (Wireless Fidelity)



Dans cette architecture, les machines communiquent par des ondes radio à l'aide du composant central (Routeur ou switch). En fait, le WIFI est une topologie en étoile, mais sans fils.

Contrairement aux réseaux construits sur une topologie en bus, les réseaux suivant une topologie en étoile sont beaucoup moins vulnérables car une des connexions peut être débranchée sans paralyser le reste du réseau. Le point névralgique de ce réseau est le concentrateur, car sans lui plus aucune communication entre les ordinateurs du réseau n'est possible.

En revanche, un réseau à topologie en étoile est plus onéreux qu'un réseau à topologie en bus car un matériel supplémentaire est nécessaire (le hub ou switch)

Avantages et inconvénients de chaque topologie

Sur un réseau en bus, deux machines peuvent monopoliser le câble. L'architecture en anneau avec un protocole à base de jeton, peut servir dans un environnement temps réel car le délai maximum pour transmettre une information entre 2 machines peut être calculé. Le câblage en anneau nécessite plus de câble puisqu'il faut reboucler la dernière machine sur la première. Le câblage en anneau peut être perturbé par la panne d'une seule machine.
Dans l'architecture en étoile, le point faible est le centre de l'étoile, si cet élément tombe en panne, alors tout le réseau est paralysé.
Le Wifi permet une plus grande liberté (le réseau reste fonctionnel, même en déplaçant les machines), En plus, la portée radio du Wi-Fi est capable de traverser des murs en béton armé ou des étages sans avoir à refaire un câblage mais dans ces conditions, le débit est ralenti.

Le standard Ethernet

C'est une couche physique permettant le partage du médium sur bus. Débit original 10 Mb/s aujourd'hui FastEthernet (sous standard), permet un transfert à 100 Mb/s (norme IEEE802.12) et plus... Sur un même tronçon toutes les cartes doivent avoir le même débit.

Chapitre II- Le matériel

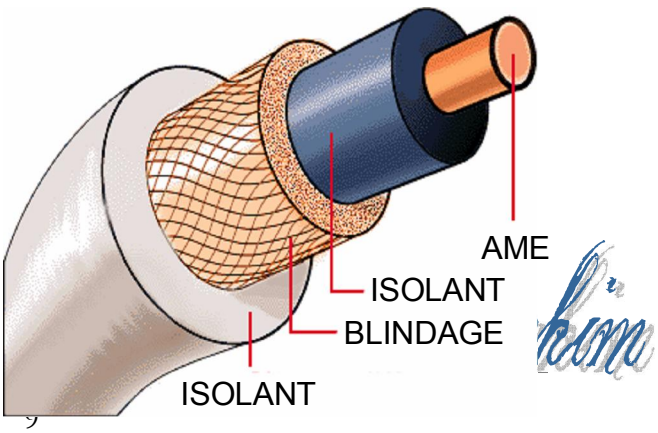
Les Câbles

Définition : câble destiné exclusivement au transport de données numériques (donc à des courants faibles).
Les principaux véhicules de l'information entre machines reliées en réseau local appartiennent à trois grandes familles de câbles :

1. Coaxial
2. Paires torsadées
3. Fibres optiques

Câbles blindés coaxiaux

Les câbles électriques (cuivre) blindés coaxiaux ressemblent aux câbles TV, ils sont dits BNC.



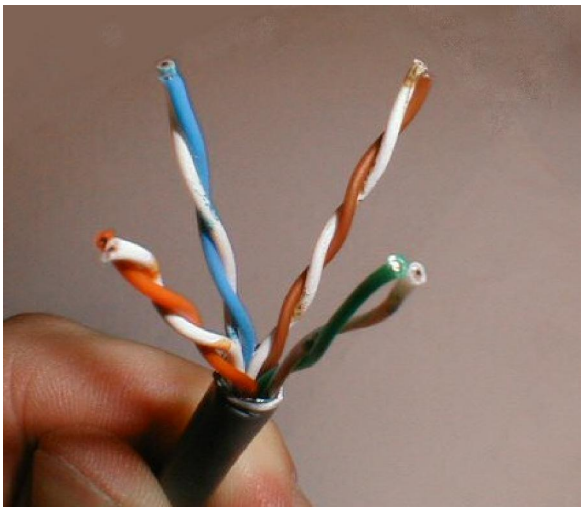
Malgré de bonnes qualités intrinsèques (notamment leur faible sensibilité aux perturbations électromagnétiques ou parasites), ils sont de moins en moins utilisés et laissent de plus en plus la main aux paires torsadées.

Connecteur en T pour l'interconnexion entre les différents cables réseau

Terminaison

N.B : La norme la plus utilisée pour ce type de câble est : 10 Base 2 (10 Mbits/s, 185 m par segment, 30 noeuds max)

Câbles paires torsadées



Les câbles électriques (cuivre) à paires torsadées ressemblent très fortement aux câbles téléphoniques.

On notera que les torsades diminuent la sensibilité aux perturbations et l'atténuation du signal tout au long du câble.

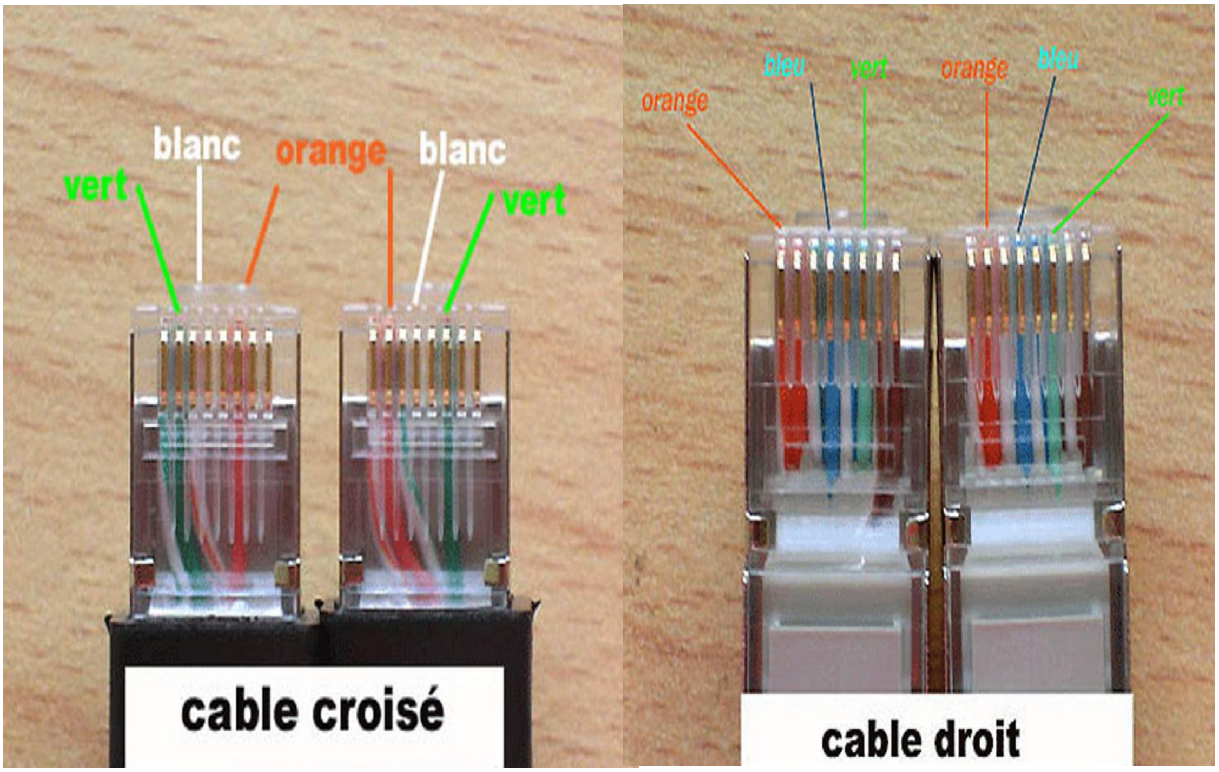
Il existe des versions blindées (STP) et non blindées (UTP).Les câbles à paires torsadées sont actuellement, et de loin, les plus employés, en raison de leur prix raisonnable, mais surtout parce que celles-ci

Mrad Brahim

s'adaptant nettement mieux aux câblages de groupes de travail et au pré câblages d'immeubles de bureaux.

Les connecteurs utilisés pour ce type de câble ont la référence RJ45. Ils sont cousins de RJ12 utilisées aux USA en téléphonie. Ils supportent « huit fils » (**quatre paires**)

RJ45



- le câble **croisé** : pour relier deux ordinateurs.
- le câble **droit** : pour relier plus de 2 ordinateurs. Chaque ordinateur est relié à un switch, ou à un routeur, ou modem routeur, LiveBox, FreeBox, etc.

N.B : Les normes les plus utilisées actuellement pour ce type de câble sont :

- 100 Base-TX : (100 Mbits/s, 100 m entre machine et Hub ainsi qu'inter Hubs)
- 1000 Base-t: permet un débit d'un Gigabit par seconde.

Mead Brahim

Câble fibres optiques

Une fibre optique est un fil en verre ou en plastique très fin qui a la propriété de conduire la lumière et sert dans les transmissions terrestres et océaniques de données. Elle offre un débit d'informations nettement supérieur à celui des câbles coaxiaux et supporte un réseau « large bande » par lequel peuvent transiter aussi bien la télévision, le téléphone, la visioconférence ou les données informatiques.
Le principe de la fibre optique a été développé dans les années 1970 dans les laboratoires de l'entreprise américaine Corning Glass Works (actuelle Corning Incorporated).
Entourée d'une gaine protectrice, la fibre optique peut être utilisée pour conduire de la lumière entre deux lieux distants de plusieurs centaines, voire milliers, de kilomètres. Le signal lumineux codé par une variation d'intensité est capable de transmettre une grande quantité d'informations. En permettant les communications à très longue distance et à des débits jusqu'alors impossibles, les fibres optiques ont constitué l'un des éléments clef de la révolution des télécommunications optiques. Ses propriétés sont également exploitées dans le domaine des capteurs (température, pression, etc.), dans l'imagerie et dans l'éclairage.
Un nouveau type de fibres optiques, fibres à cristaux photoniques, a également été mis au point ces dernières années, permettant des gains significatifs de performances dans le domaine du traitement optique de l'information par des techniques non linéaires, dans l'amplification optique ou bien encore dans la génération de supercontinuums utilisables par exemple dans le diagnostic médical.
Dans les réseaux informatiques du type Ethernet, pour la relier à d'autres équipements, on peut utiliser un émetteur-récepteur.

Lorsque le trafic devient important les liaisons cuivre sont insuffisantes et il faut passer à la fibre optique. Citons les liaisons :

- entre les étages ou les services
- entre les commutateurs
- vers les serveurs
- entre les bâtiments

Le tableau ci-dessous donne un panorama des types de liaisons Ethernet disponibles :

	100 m	1 km	5 km	50 km
10 Gb/s	10 GBase-SX *multimode*	10 Gbase-Lx *multimode*	10 GBase-LX *monomode*	10 GBase-EX *monomode*
1 Gb/s	1 GBase-T *cuivre*	1 GBase-SX *multimode*	1 GBase-LX *monomode*	
100 Mb/s	100 Base-Tx *cuivre*	100 Base-FX *multimode*		
10 Mb/s	10 Base-T *cuivre*	10 Base-F *multimode*		

Norme Ethernet et type de conducteur suivant les distances et les débits requis
doc. Yalta

Les cartes réseaux

Ce sont les supports de transmissions des données, de plus en plus de machines ont une carte réseau intégrée à la carte mère, ce qui facilite la mise en place de réseaux pour ces machines.

Les cartes les plus utilisées actuellement sont les cartes supportant la paire torsadée avec une entrée RJ45 (8fils, 4 paires).

Parmi les marques les plus connus on trouve : 3 com, D-Link, Intel, IBM, Realtek, …)

Les éléments actifs

HUB

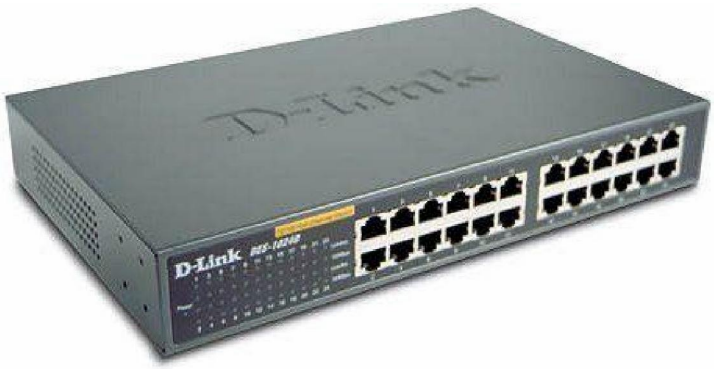
Les entrées ou « ports » d'un concentrateur ou « HUB » sont reliés individuellement aux machines, la topologie logique est normalement la topologie en étoile.

Cependant, le HUB simule intérieurement le « bus ». Les trames envoyées à destination d'une machine sont en fait reçues par toutes les machines même si elles sont seulement traitées par la machine à qui elles sont destinées (principe du BUS).

De plus la bande passante théorique de 10 Mbits/s ou de 100 Mb/s n'est disponible pour chaque machine mais partagée entre toutes les autres, puisqu'une seule machine à la fois peut normalement émettre et recevoir sur le réseau.

Si le Hub du réseau ne possède plus de port disponible, il est possible alors de connecter un nouveau Hub avec l'ancien (chaînage de Hub ou Interlink). En norme Ethernet, un maximum de 4 Hubs peut être installé.

SWITCH



Avec les concentrateurs commutateurs, que l'on appelle le plus souvent Switched Hubs ou même tout simplement Switchs, les trames envoyées à une machine particulière sont directement aiguillées vers la machine destinatrice, en supprimant toute collision, la topologie logique n'est donc plus le bus mais l'étoile.

Le Switch crée des liens privilégiés entre chaque élément connecté. Grâce à la fonction d'auto apprentissage des adresses MAC (adresses physiques des cartes réseaux), l'information envoyée à travers le Switch est directement dirigée vers la machine de destination.

De plus, chaque machine connectée à un port du Switch dispose d'une bande passante dédiée. Les machines connectées à un Switch peuvent travailler en full duplex, c'est-à-dire qu'elles peuvent émettre et recevoir en même temps.

Routeur

Un **routeur** est un élément intermédiaire dans un réseau informatique assurant le routage des paquets. Son rôle est de faire transiter des paquets d'une interface réseau vers une autre, selon un ensemble de règles formant la table de routage. C'est un équipement de couche 3 du modèle OSI.

Il ne doit pas être confondu avec un commutateur (couche 2) ou une passerelle (couche 3 et supérieures).

Mrad Brahim

Chapitre III : Les normes logicielles

Architectures réseaux

Réseaux poste à poste (peer to peer)

Dans un réseau à serveurs non dédiés, « poste à poste » ou encore « égal à égal », toute machine est potentiellement aussi bien un serveur pour les autres machines qu'une « station cliente ».
Ce type de réseau est parfaitement adapté aux petits groupes de travail et aux professions libérales en raison de son bas prix et de sa simplicité d'utilisation.
Principaux avantages des réseaux poste à poste

• Les machines continuent de fonctionner comme avant, sans grande modification, sous leur système d'exploitation originel. On n'a pas besoin de prévoir des machines « gonflées » ou des configurations spéciales.
• La plupart du temps (selon le réseau choisi) un technicien spécialiste est inutile.
• Le coût de base est faible et les évolutions sont faciles et économiques.
Réseaux à serveurs dédiés

Dans un réseau à serveurs dédiés, on distingue les « serveurs » et les « stations clientes ». Hormis leur connectivité réseau, ces dernières restent des machines classiques, comme celles que l'on aurait utilisées en absence de réseau ou dans un réseau à serveur non dédié dit « poste à poste ».
Aucun utilisateur classique n'est physiquement installé sur les serveurs sinon ces derniers ne seraient plus « dédiés » ! Les serveurs ont alors seule fonction de servir les autres machines.

Ces serveurs ne sont pas des machines ordinaires que l'on aurait simplement « gonflés », ils doivent être optimisés pour ce type de travail : on soigne particulièrement les « entrée/sortie » (E/S ; In/Out, I/O en anglais) ce qui nécessite des bus et des périphériques rapides et un OS multitâche comme Windows NT, Linux, Unix, Netware,…

Ce type de réseau, qui rapproche la « micro-informatique » de la « mini » ou des « grands systèmes » en « centralisant l'information », est très performant et parfaitement adapté aux activités critiques, exigeantes en sécurités de toute nature et à celles qui sont génératrices de transferts de données intensifs (trafic important, car nombreux utilisateurs) ou importants (gros fichiers) à travers le réseau.

En raison de sa complexité et de son coût global (sans oublier les coûts cachés) nettement plus élevés à tous points de vue, il est le plus souvent inadapté (sauf activités lourdes) aux toutes petites structures de deux ou trois machines ; c'est le type même de réseau que l'on utilisera pour gérer l'ensemble du système d'information global de l'entreprise. Dans certains cas, il est possible d'y rattacher des groupes de travail en réseaux poste à poste.

De nombreux réseaux, petits ou moyens, ont un unique « serveur dédié » il fait alors simultanément fonction, comme pour les réseaux « poste à poste », de serveur de fichiers, de serveur d'impression et de serveur de messagerie et/ou de Fax.

Dès que le nombre de machines connectées est élevé et que l'on prévoit un trafic réseau important, il est préférable de spécialiser des serveurs, tant pour éviter les goulots d'étranglement que les blocages intempestifs du système (une impression ou une émission de télécopie qui pose problème pourra totalement bloquer certains serveurs).

On dit souvent que ces réseaux travaillent en mode « client-serveur » ; en vérité, si les applications sont bien situées sur le serveur, elles sont le plus souvent

Mrad Brahim

exécutées (à distance) par les stations clientes : on travaille alors en mode « serveur de fichiers ».

On peut véritablement parler de « client-serveur » lorsque les applications, le plus souvent des bases de données haut de gamme comme Sybase, Oracle, SQL server, Access sont exécutées par le serveur lui-même, donc développées spécialement pour son système d'exploitation propre et présentes dans sa mémoire (qui doit être étendue en conséquence). On comprend bien la différence de rapidité qui peut en résulter pour les « requête » effectuées par les utilisateurs.

Dans la pratique, on combine le mode « client-serveur » pur et dur et le mode « serveur de fichiers ».

Principaux avantages des réseaux à « serveurs dédiés »

• Les performances globales sont très supérieures à celle des réseaux « poste à poste ». Le goulot d'étranglement est nettement moins marqué qu'avec les serveurs des réseaux « poste à poste ».

• Sécurités d'accès et de fonctionnement centralisées, pouvant être absolues.

• Possibilité de spécialiser les serveurs, afin d'améliorer les performances et la fiabilité.

• Possibilité de mettre en oeuvre des imprimantes spéciales réseau. Elles recevront et traiteront les données beaucoup plus rapidement qu'à partir d'un port parallèle ou série et pourront être installées n'importe où (au plus près des utilisateurs), grâce à leur connexion directe sur le câble réseau.

• On n'a pas besoin de se préoccuper de maintenir sous tension toutes les machines qui contiennent les données utiles ou qui alimentent telle ou telle imprimante, comme avec les réseaux « poste à poste ». Puisque les données sont toujours situées uniquement sur le disque dur de chaque station cliente ou sur les serveurs, il suffit que ces derniers soient alimentés (dans la plupart des cas, ils sont sous tension 24h/24h).

Les protocoles :

Protocole : Description formelle de règles et de conventions régissant la manière dont les stations d'un réseau échange des informations.
Le protocole est un élément déterminant. Il est couramment lié aux couches 3 et 4 du modèle OSI (transport et réseau). Il segmente les données en « paquets » qu'il place dans le champ « données » des trames créées par les couches physiques. Il établit les relations entre adresses logiques et physiques (MAC) de tous les destinataires, choisit l'itinéraire le plus approprié pour assurer leur acheminement (« routage ») et corrige les erreurs de transmission.
Les principaux protocoles LAN les plus utilisés en micro-informatique actuellement sont :

- NetBEUI
- IPX/SPX
- AppleTalk
- TCP/IP

NetBEUI

Il a été conçu et optimisé pour les réseaux purement locaux (LAN) et il est mal adapté aux réseaux WAN. Il est essentiellement supporté par IBM et Microsoft qui le proposent traditionnellement par défaut sur leurs NOS pour réseaux locaux
IPX/SPX

IPX/SPX a été proposé en 1983 par la société Novell pour NetWare, son système d'exploitation de réseau (NOS) ;
IPX/SPX est d'une mise en oeuvre assez simple (il se configure et se règle tout seul). Il sait ce qu'est une adresse logique ou réseau (il est dit « routable »), ce qui

Mrad Brahim

facilite l'interconnexion inter réseau. Il est plus performant en fonctionnement local LAN que TCP/IP et occupe très peu de place en mémoire, notamment sur les stations clientes utilisant MS-DOS.
Il est essentiellement utilisé par les produits Net Ware et compatibles qui ne proposent pas NetBEUI.

AppleTalk

AppleTalk est un protocole réseau spécifique et intrinsèque aux machines Apple. Conçu originellement pour fonctionner exclusivement sur le réseau physique LocalTalk d'Apple (réseau propriétaire intégré à toute machine Macintosh, comme AppleTalk, très simple à mettre en oeuvre mais limité à 230 Kb/s et à 32 noeuds physiques), il a été adapté sur les bases physiques Ethernet (avec pour nom EtherTalk).
On notera qu'il est aussi possible d'ajouter TCP/IP, récemment fourni en standard par Apple, aux machines Macintosh.

TCP/IP

TCP/IP est un **protocole**, c'est à dire des **règles de communication**.
IP signifie Internet Protocol : littéralement "le protocole d'Internet". Il permet principalement d'identifier les machines à l'aide d'adresses.

Le rôle du protocole IP de découper l'information à transmettre en paquets, de les adresser, de les transporter indépendamment les uns des autres et de recomposer le message initial à l'arrivée, sans aucune perte ou changement sur le plan de leur intégrité. Ce protocole est dit de commutation de paquets. Il permet donc aux ordinateurs reliés à Internet de dialoguer entre eux.

Il existe des adresses IP de version 4 et de version 6. La version 4 est actuellement la plus utilisée : elle est généralement écrite en notation décimale avec quatre nombres compris entre 0 et 254, séparés par des points ; exemple : `212.85.150.134`.

Une partie des nombres à gauche désigne le réseau est appelée **ID de réseau** (en anglais *netID*),

Les nombres de droite désignent les ordinateurs de ce réseau est appelée **ID d'hôte** (en anglais *host-ID*)

IPV6

La façon dont nous utilisons les adresses IP est bientôt révolue. Le protocole IP actuel, dans sa version 4, présente un problème de taille : il n'y a bientôt plus d'adresses disponibles ! En effet, avec un maximum de 256x256x256x256 soit 4,3 milliards d'IP, les experts du monde entier s'accordent à dire qu'elles seront toutes utilisées à court terme. Ils annonçaient déjà la saturation en 2005, qui n'a pas eu lieu semble-t-il, mais il se pourrait bien que nous ne puissions pas aller plus loin qu'en 2008 dans le meilleur des cas ! Heureusement, des ingénieurs développent depuis quelques années le remplaçant d'IPv4, c'est IPv6. Ce dernier, déjà utilisé par quelques réseaux, permet un maximum de 3,4x1038 (34 suivi de 38 « 0 » !) d'adresses, un nombre inimaginable en somme. Alors que les IP actuelles sont des suites de 4 nombres 8 bits, les IPv6 seront 8 nombres notés en hexadécimal !
Par exemple,
4000.6200.00a0.0bc0.9999.8888.a25b.cd16.

Cela ne changera pas grand-chose pour les Internautes et la configuration des réseaux locaux ne deviendra pas un calvaire pour autant. La transition a déjà commencé, tout doucement. D'ici 2010, il ne devrait plus y avoir que quelques

Mrad Brahim

traces d'IPv4. Bien que la fonction ne soit pas activée, Windows 2000 et XP sont déjà compatibles IPv6, et il se pourrait bien que Windows Vista et Windows 7 gères IPv6 en standard.

Les classes des réseaux

On avait à cette époque 3 classes pour les adresses unicast, une classe pour les adresses multi destinataires (multicast), la classe D et une classe E non utilisée.

Classe A

Les réseaux disponibles en classe A sont les réseaux allant de 1.0.0.0 à 126.0.0.0 (les derniers octets sont des zéros ce qui indique qu'il s'agit bien de réseaux et non d'ordinateurs !)

Les trois octets de droite représentent les ordinateurs du réseaux, le réseau peut donc contenir un nombre d'ordinateur égal à :
$2^{24}-2^{1}$ = 16777214 ordinateurs.

Une adresse IP de classe A, en binaire, ressemble à ceci :

xxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx

Réseau Ordinateurs

Classe B

Dans une adresse IP de classe B, les deux premiers octets représentent le réseau.

Les réseaux disponibles en classe B sont donc les réseaux allant de 128.0.0.0 à 191.255.0.0

Les deux octets de droite représentent les ordinateurs du réseau. Le réseau peut donc contenir un nombre d'ordinateurs égal à :

$2^{16}-2^{1} = 65534$ *ordinateurs.*

Une adresse IP de classe B, en binaire, ressemble à ceci :

xxxxxx xxxxxxxx xxxxxxxx xxxxxxxx

Réseau Ordinateurs

Classe C

Dans une adresse IP de classe C, les trois premiers octets représentent le réseau. Les réseaux disponibles en classe C sont donc les réseaux allant de 192.0.0.0 à 223.255.255.0

L'octet de droite représente les ordinateurs du réseau, le réseau peut donc contenir:

$2^{8}-2^{1}$ = 254 ordinateurs.

Une adresse IP de classe C, en binaire, ressemble à ceci :

xxxxx xxxxxxxx xxxxxxxx xxxxxxxx

Réseau Ordinateurs

Le but de la division des adresses IP en trois classes A, B et C est de faciliter la recherche d'un ordinateur sur le réseau. En effet avec cette notation il est possible de rechercher dans un premier temps le réseau que l'on désire atteindre puis de chercher un ordinateur sur celui-ci. Ainsi, l'attribution des adresses IP se fait selon la taille du réseau.

Classe	Nombre de réseaux possibles	Nombre d'ordinateurs maxi sur chacun
A	126	16777214
B	16384	65534
C	2097152	254

Le masque sous réseaux

Un masque de sous réseau (désigné par subnet mask, netmask ou address mask en anglais) est un masque indiquant le nombre de bits d'une adresse IPv4 utilisés pour identifier le sous réseau, et le nombre de bits caractérisant les hôtes (ce qui indique aussi le nombre d'hôtes possibles dans ce sous-réseau).
L'adresse du sous-réseau est obtenue en appliquant l'opérateur ET binaire entre l'adresse IPv4 et le masque de sous-réseau. L'adresse de l'hôte à l'intérieur du

Mrad Brahim

sous réseau est quant à elle obtenue en appliquant l'opérateur ET entre l'adresse IPv4 et le complément à un du masque

Les masques de sous réseau utilisent la même représentation que celles des adresses IPv4. En IPv4, une adresse IP est codée sur 4 octets, soit 32 bits (représentés en notation décimale à point). Un masque de sous réseau possède lui aussi 4 octets. Bien que la norme IPv4 n'interdise pas que la partie significative du masque contienne des bits à 0, on utilise en pratique des masques constitués (sous leur forme binaire) d'une suite de 1 suivis d'une suite de 0, il y a donc 32 masques réseau possibles.

Exemple

Adresse 192.168.1.2 et masque 255.255.255.0

192.168.1.2 & 255.255.255.0 = 192.168.1.0

192.168.1.2 & 0.0.0.255 = 0.0.0.2

Soit en binaire :

11000000.10101000.00000001.00000010

11000000.10101000.00000001.00000010

&

11111111.11111111.11111111.00000000 &

00000000.00000000.00000000.11111111

= 11000000.10101000.00000001.00000000 =

00000000.00000000.00000000.00000010

Autrement dit, il suffit pour obtenir l'adresse du sous réseau de conserver les bits de l'adresse IPv4 là où les bits du masque sont à 1 (un certain nombre de bits en partant de la gauche de l'adresse). La partie numéro d'hôte est, elle, contenue dans les bits qui restent (les plus à droite).

Une forme plus courte est connue sous le nom de « notation CIDR » (Classless Inter-Domain Routing). Elle donne le numéro du réseau suivi par une barre oblique (ou slash, « / ») et le nombre de bits à 1 dans la notation binaire du masque de sous réseau. Le masque 255.255.224.0, équivalent en binaire à 11111111.11111111.11100000.00000000, sera donc représenté par /19 (19 bits à la valeur 1, suivis de 13 bits 0).
La notation 91.198.174.2/19 désigne donc l'adresse IP 91.198.174.2 avec le masque 255.255.224.0, et signifie que les 19 premiers bits de l'adresse sont dédiés à l'adresse du sous réseau, et le reste à l'adresse de l'ordinateur hôte à l'intérieur du sous réseau.
Deux adresses IP appartiennent à un même sous réseau si elles ont en commun les bits du masque de sous réseau.
À partir de la connaissance de l'adresse IPv4 et du masque de sous réseau il est possible de calculer le nombre d'interfaces que l'on peut numéroter à l'intérieur d'un sous réseau. Le nombre de sous réseaux possibles est donné par 2r-n, où n représente le nombre de bits à 1 dans le masque réseau et r le nombre de bits du masque de sous réseau. Le nombre d'hôtes est 232-n-2, deux adresses de ce sous réseau étant réservées au sous réseau lui-même et au broadcast et ne peuvent pas être utilisées pour numéroter une interface.
/32 désigne un réseau qui ne comporte qu'une seule adresse IP, c'est-à-dire une adresse IP individuelle.

Le masque /31 était autrefois considéré comme inutilisable, car ce réseau comporte que deux adresses, dont l'adresse du sous réseau et l'adresse de broadcast. Pour numéroter des adresses de liens point à point, on utilisait donc des /30, soit quatre adresses dont deux utilisables pour adresser des interfaces.
Le RFC 3021 permet cependant d'utiliser plus efficacement l'espace d'adressage en permettant le /31 (il n'y a dans ce cas pas d'adresse de broadcast et l'adresse du sous réseau est utilisée pour numéroter une interface).

Liste des masques de sous réseaux

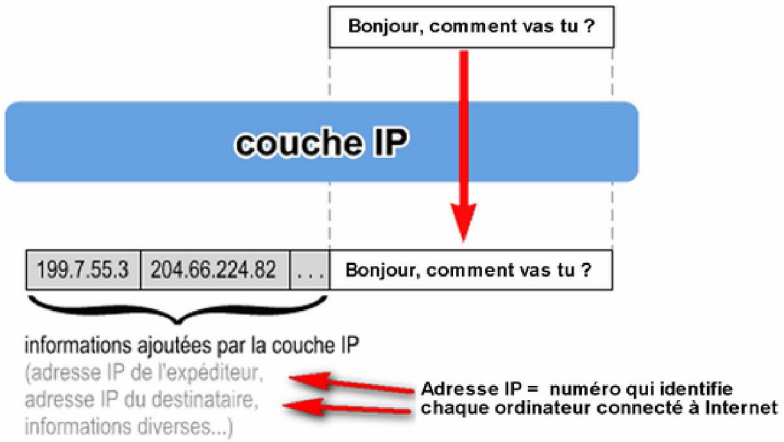
bits disponibles	Masque de sous réseau	Nombre d'hôtes par sous réseau
31	128.0.0.0	2^{31}-2 = 2147483646
30	192.0.0.0	2^{30}-2 = 1073741822
29	224.0.0.0	2^{29}-2 = 536870910
28	240.0.0.0	2^{28}-2 = 268435454
27	248.0.0.0	2^{27}-2 = 134217726
26	252.0.0.0	2^{26}-2 = 67108862
25	254.0.0.0	2^{25}-2 = 33554430
24	255.0.0.0	2^{24}-2 = 16777214
23	255.128.0.0	2^{23}-2 = 8388606
22	255.192.0.0	2^{22}-2 = 4194302
21	255.224.0.0	2^{21}-2 = 2097150
20	255.240.0.0	2^{20}-2 = 1048574
19	255.248.0.0	2^{19}-2 = 524286
18	255.252.0.0	2^{18}-2 = 262142
17	255.254.0.0	2^{17}-2 = 131070
16	255.255.0.0	2^{16}-2 = 65534
15	255.255.128.0	2^{15}-2 = 32766
14	255.255.192.0	2^{14}-2 = 16382
13	255.255.224.0	2^{13}-2 = 8190
12	255.255.240.0	2^{12}-2 = 4094
11	255.255.248.0	2^{11}-2 = 2046
10	255.255.252.0	2^{10}-2 = 1022
9	255.255.254.0	2^{9}-2 = 510
8	255.255.255.0	2^{8}-2 = 254
7	255.255.255.128	2^{7}-2 = 126
6	255.255.255.192	2^{6}-2 = 62
5	255.255.255.224	2^{5}-2 = 30
4	255.255.255.240	2^{4}-2 = 14
3	255.255.255.248	2^{3}-2 = 6
2	255.255.255.252	2^{2}-2 = 2
1	255.255.255.254	2^{1}
0	255.255.255.255	2^{0}

Comment fonctionne une adresse IP ?

La fonction de IP est fonction, adressage, data gramme.

C'est le principal protocole utilisé sur Internet.

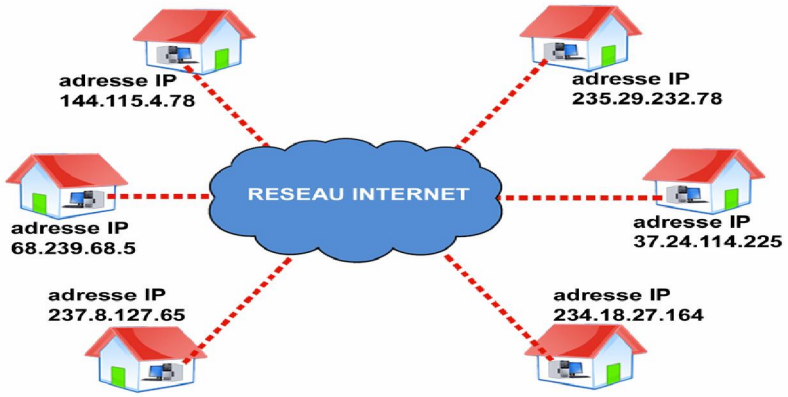
L'adresse IP se présente le plus souvent sous forme de 4 nombres (entre 0 et 255) séparés par des points.



Chaque message (chaque petit paquet de données) est enveloppé par IP qui y ajoute différentes informations:

- l'adresse de l'expéditeur (votre adresse IP)
- l'adresse IP du destinataire
- différentes données supplémentaires (qui permettent de bien contrôler l'acheminement du message)

L'adresse IP est une adresse unique attribuée à chaque ordinateur sur Internet (c'est-à-dire qu'il n'existe pas sur Internet deux ordinateurs ayant la même adresse IP). De même, l'adresse postale (nom, prénom, rue, numéro, code postal et ville) permet d'identifier de



manière unique un destinataire.

L'adresse IP est souvent une adresse temporaire, donnée par votre fournisseur d'accès à Internet (FAI). Votre FAI conserve normalement l'historique de vos adresses IP temporaires pendant un an !

Les ordinateurs hôtes qui hébergent des ressources (serveur web, serveur ftp, ...) ont une adresse IP fixe.

Le rôle du protocole TCP : TCP veut dire Transmission Control Protocol sa fonction est le transport et le contrôle de la transmission des données.

Il désigne communément une architecture réseau. Le protocole TCP est basé en couche 4 :

1-Application

2-Transport

3-internet

4-Hôte-Réseau

Le protocole TCP/IP permet donc à des logiciels situés sur des ordinateurs différents de communiquer de façon fiable il contrôle La gestion des flux et des erreurs. Le protocole TCP est un protocole Internet qui complète le protocole IP pour assurer le transport des données sur Internet

Il se charge de la communication entre les applications, c'est-à-dire entre les logiciels utilisés par les ordinateurs. Il vérifie que le destinataire est prêt à recevoir les données.

Il fractionne les messages en paquets plus petits (car les paquets IP ont une taille limitée) et numérote les paquets.

A la réception, il vérifie que tous les paquets sont bien arrivés et peut redemander les paquets manquants.

Il ré-assemble les paquets avant de les transmettre aux logiciels.

Il envoie des accusés de réception pour prévenir l'expéditeur que les données sont bien arrivées.

TCP fournit un service sécurisé de remise des paquets. Si un incident de réseau empêche les données d'arriver, le protocole le détecte et signale une erreur à l'application. TCP garantit donc l'ordre et la remise des paquets, il vérifie l'intégrité de l'en-tête des paquets et des données qu'ils contiennent. TCP est responsable de la retransmission des paquets altérés ou perdus par le réseau lors de leur transmission.

Le protocole TCP permet d'assurer le transfert des données de façon fiable, bien qu'il utilise le protocole IP, qui n'intègre aucun contrôle de livraison de datagrammes.

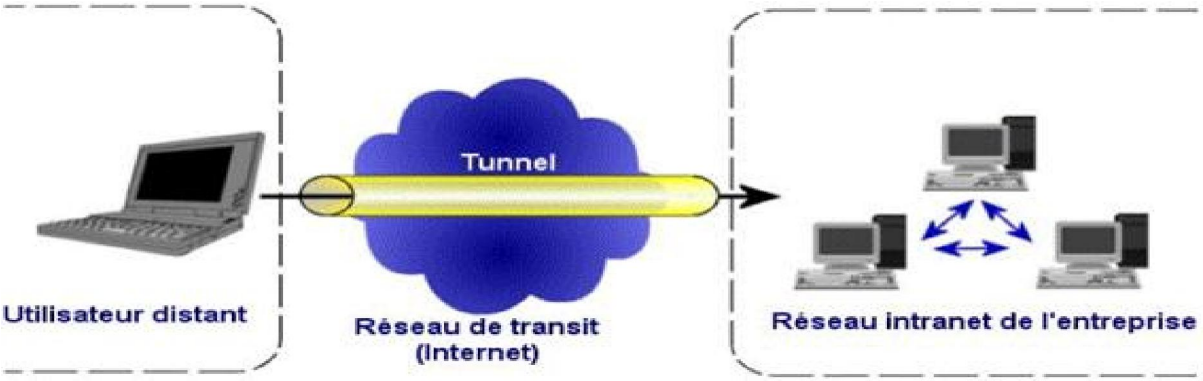
Les caractéristiques principales du protocole TCP sont les suivantes :

- TCP permet de remettre en ordre les datagrammes en provenance du protocole IP
- TCP permet de vérifier le flot de données afin d'éviter une saturation du réseau

- TCP permet de formater les données en segments de longueur variable afin de les "remettre" au protocole IP
- TCP permet de multiplexer les données, c'est-à-dire de faire circuler simultanément des informations provenant de sources (applications par exemple) distinctes sur une même ligne
- TCP permet enfin l'initialisation et la fin d'une communication de manière courtoise

VPN

Un VPN repose sur un protocole, appelé protocole de tunnelisation, c'est-à-dire un protocole permettant aux données passant d'une extrémité à l'autre du VPN d'être sécurisées par des algorithmes de cryptographie.



La mise en place d'un réseau privé virtuel permet de connecter de façon sécurisée des ordinateurs distants au travers d'une liaison non fiable (Internet), comme s'ils étaient sur le même réseau local.
Ce procédé est utilisé par de nombreuses entreprises afin de permettre à leurs utilisateurs de se connecter au réseau d'entreprise hors de leur lieu de travail. On peut facilement imaginer un grand nombre d'applications possibles :

- Accès au réseau local (d'entreprise) à distance et de façon sécurisée pour les travailleurs nomades

Mrad Brahim

- Partage de fichiers sécurisés
- Jeu en réseau local avec des machines distantes

Conclusion

Le réseau informatique a était flou pour moi avant de commencer cette année de formation mais grâce a mes formateurs qui m'ont donné toujours des réponses à mes questions j'ai arrivé à faire une mémoire en réseau avec confiance de mes informations à propos de ce sujet.
Cette mémoire est une occasion de dire que le réseau informatique c'est le futur de la terre car il relie tout le monde ce qui rend le partage de données et des ressources quelque chose de très facile avec des débit très élevées.
Le réseau informatique s'évalue rapidement de nos jours ce qui nous oblige a y être a jour afin de suivre et comprendre son fonctionnement et le bien utiliser dans tous les domaines.