Introduction au réseau

Par Baptiste Wicht

Date de publication : 2 mars 2007

Dernière mise à jour : 9 mars 2020

Avec cet article, vous allez apprendre les bases de la connaissance du réseau.

I - Avant-propos

Cet article va vous apprendre les bases de la connaissance du réseau. C'est-à-dire que vous allez découvrir quels sont les différents appareils qui opèrent dans un réseau et comment sont organisés les réseaux. Car il y a beaucoup de spécifications et de règles sur l'élaboration d'un réseau qu'il est très utile de connaître avant de se lancer dans le réseau.

II - Introduction

Avant de commencer à apprendre des notions purement réseau, nous allons nous attarder un moment sur les bases.

II-A - Les composants

Je vais maintenant vous présenter brièvement les principaux composants entrant dans la communication réseau.

II-A-1 - Le processeur

Le processeur est le cerveau de l'ordinateur, c'est lui qui gère toutes les opérations de base, il va s'occuper de rediriger les flux du clavier, de la souris et de tout autre périphérique d'entrée, vers les bons composants. C'est lui qui va envoyer les flux de sortie vers l'écran, les écouteurs…
Sa vitesse est mesurée en Hertz et d'elle, dépend la vitesse du PC en lui-même. Le processeur est installé sur la carte mère.

II-A-2 - La carte mère

La carte mère est un assemblage de circuits imprimés. Elle s'occupe de gérer les communications entre les différents composants et les périphériques. Tout vient se brancher sur elle. Elle héberge aussi la mémoire morte (ROM) et la mémoire vive (RAM). La RAM est employée pour mettre en mémoire les données des applications qui marchent, alors que la ROM contient des informations dont le système a besoin par exemple pour démarrer. C'est encore la carte mère qui va gérer les périphériques des stockages. Sur la carte mère, on va pouvoir brancher des cartes d'extension qui vont ajouter des fonctionnalités à notre système. On va pouvoir les brancher sur différents types de bus : AGP, PCI et ISA.

II-A-3 - La carte réseau

La carte réseau est employée pour faire communiquer le PC avec d'autres éléments, tels que des PC, des serveurs ou des imprimantes. Elle aussi vient s'intégrer sur la carte mère. Il faut prendre en compte certains éléments pour la sélection d'une carte.

- Type de réseau : 10, 100 ou 1000 Mbps, c'est-à-dire la vitesse de communication.
- Type de média : c'est en fait le type de câble qui va être utilisé pour relier la carte réseau à un autre élément réseau. Ce type peut être de la fibre optique, un câble à paire torsadée ou un réseau sans fil.
- Type de bus : c'est en fait le bus sur lequel on va brancher notre carte, cela peut être PCI ou ISA.

Une carte réseau communique de manière parallèle avec la carte mère et de manière sérielle avec le réseau.

II-B - Les formats de données

Un ordinateur peut comprendre une donnée seulement si celle-ci est binaire. Une donnée binaire est une donnée codée en base 2.
Un autre format de données aussi beaucoup utilisé est l'hexadécimal, il est codé en base 16.

II-B-1 - Les termes de mesure de données

- Bit(b) : c'est la plus petite unité de mesure possible, un bit peut être 1 ou 0, c'est le format binaire avec lequel travaille le CPU.
- Byte(B) ou Octet(o) : c'est un groupe de 8 bits.
- Kilo(k) : représente 1000 (1024). Exemple 2 kB = 2048 Bytes = 16384 bits
- Méga(M) : représente 1 000 000 (1 048 576).
- Giga(G) : Représente 1 000 000 000.
- Ps : par seconde, unité de mesure de vitesse d'un réseau par exemple : kbps.
- Hertzv (Hz) : c'est une unité de mesure de fréquence. C'est le nombre de cycles par secondes effectués. C'est avec cette mesure qu'on calcule la vitesse d'un processeur par exemple. Aussi très employée dans les ondes radio.

II-C - Terminologie de base de réseau

- Network Interface Card(NIC) : carte réseau.
- Média : c'est le type de câble.
- Protocol : c'est une série de règles qui définissent comment le PC va communiquer à travers le réseau, il existe beaucoup de types de protocoles, des protocoles de routage, des protocoles Internet…
- IOS (Internetwork Operation System) : c'est le logiciel qui est dans l'élément de réseau, en quelque sorte son OS.
- LAN (Local Area Network) : c'est un petit réseau, qui est confiné entre de petites barrières géographiques, cela peut être une chambre, un bâtiment, ou éventuellement plus grand.
- MAN (Metropolitan Area Network) : c'est un réseau plus grand que le LAN, il couvre environ une ville entière.
- WAN (Wide Area Network) : c'est un réseau gigantesque, qui peut s'étendre sur plusieurs pays. Internet en est un exemple.

II-D - Le modèle OSI (Open System Interconnexion)

Ce modèle a été créé par l'organisme ISO. C'est une norme internationale. Elle est implémentée dans presque tous les réseaux et la plupart des protocoles en sont dérivés. Les entreprises se sont rendu compte que si tout le monde se basait sur les mêmes spécifications, la communication entre réseaux serait énormément améliorée. Ce modèle est formé de sept couches ayant chacune des applications bien distinctes.

II-D-1 - Avantages d'OSI et de la division par couches

- Cela réduit la complexité, puisque cela subdivise la communication en plus petites couches.
- Cela standardise bien sûr les interfaces.
- Cela permet un meilleur développement et une meilleure évolution, car il suffit d'interagir sur la couche qui doit être modifiée.

II-D-2 - Les couches OSI

Je vais maintenant vous présenter les différentes couches qui forment la norme OSI.

II-D-2-a - La couche 7 : Application

La couche application est responsable de la communication entre le réseau et les applications. Elle offre le service réseau à l'application qui le demande. Elle est différente des autres couches, car elle n'offre pas de service aux autres couches.

II-D-2-b - La couche 6 : Présentation

Cette couche s'occupe surtout de traduire les données pour que les deux systèmes puissent communiquer entre eux et se comprendre. Par exemple si un envoie de l'ASCII et l'autre du DCB, la couche va s'occuper de traduire dans les deux sens.

II-D-2-c - La couche 5 : Session

Cette session établit, gère et termine les communications entre deux systèmes. Elle s'occupe aussi de synchroniser les dialogues entre les hosts. Elle assure la communication et la gestion des paquets entre deux stations.

II-D-2-d - La couche 4 : Transport

Cette couche divise les données de l'envoyeur, puis les rassemble chez le récepteur. La couche transport assure la fiabilité et la régulation du transfert de données. C'est la couche tampon en quelque sorte, car elle se trouve entre les couches purement réseau et les couches qui elles se réfèrent plus aux applications.

II-D-2-e - La couche 3 : Réseau

Cette couche gère la connectivité entre deux systèmes qui peuvent être localisés dans différents endroits géographiques et dans différents réseaux. La couche liaison de données assure un transit fiable des données sur une liaison physique. Elle se réfère aux adresses réseau donc IP

II-D-2-f - La couche 2 : Liaison de données

Cette couche définit comment les données sont formatées et comment on accède au réseau. Elle est responsable de « dire » comment un appareil correspond avec un autre alors qu'ils sont sur différents réseaux et médias. Elle se réfère à l'adressage physique donc aux adresses MAC.

II-D-2-g - La couche 1 : Physique

La couche physique est la couche de bas niveau, c'est la couche la plus basique du modèle, elle contient toutes les spécifications électriques, mécaniques pour l'activation, la maintenance entre le lien physique et le système. Par exemple, les distances de transmission, le voltage, les connecteurs physiques, le type de média.

II-E - La communication Peer-to-Peer

La communication Peer-to-Peer (P2P) est un modèle de réseau informatique dans lequel tous les éléments n'ont pas seulement un rôle (client ou serveur), mais peuvent fonctionner dans les deux rôles.

II-F - Le protocole TCP/IP

Le protocole TCP est basé sur les couches OSI, mais il n'en a lui-même que quatre.

Je vais maintenant vous présenter les couches du protocole TCP/IP. Vous ne serez néanmoins pas trop perturbés, car les couches ressemblent beaucoup à celles du modèle OSI.

II-F-1 - La couche 4 : Application

C'est la couche de haut niveau, elle correspond directement avec l'utilisateur, elle englobe les couches OSI d'application, de présentation et de session. Elle s'assure que les données soient correctement « empaquetées » pour qu'elles soient lisibles par la couche suivante.

II-F-2 - La couche 3 : Transport

Cette couche est sensiblement ressemblante à la couche transport du modèle OSI.

II-F-3 - La couche 2 : Internet

Cette couche doit s'assurer que les données envoyées arrivent correctement à destination.

II-F-4 - La couche 1 : Network Access

Cette couche est assez confuse. Elle inclut tous les protocoles LAN et WAN et tous les détails que les couches OSI liaisons de données et physiques fournissaient.

III - Généralités réseau

Dans un réseau, il faut différencier deux types d'utilisateurs, ceux qui travaillent directement depuis le bâtiment principal, donc qui auront un accès direct au réseau et ceux qui eux, travaillent depuis ailleurs ou alors sont mobiles. Les premiers auront accès directement au réseau, donc à une connexion haute vitesse. Par contre pour les suivants, soit ils travaillent dans des bureaux de l'entreprise, donc dans un sous-réseau du réseau et donc une connexion plus ou moins rapide ; soit avec les gens mobiles ou travaillant à la maison, on aura recours à une connexion en dialup (par modem, ex. : VPN) pour les connecter sur le réseau.

III-A - Le modèle réseau

Pour faciliter la compréhension d'un réseau, CISCO a mis au point un modèle hiérarchique en couches. Chaque couche a un but précis, et chacune des couches communique ensemble.

III-A-1 - La couche d'accès

Cette couche est le point d'accès dans le réseau, c'est par là qu'arrivent toutes les connexions. Elle est aussi appelée la couche bureau.

III-A-2 - La couche de distribution

Cette couche remplit les fonctions de routage, filtrage et gère les accès depuis le WAN. Elle s'occupe aussi de faire communiquer des réseaux dans différentes topologies. Elle va trouver le meilleur chemin pour la requête et ensuite va transmettre cette requête à la couche de « cœur ». Elle est aussi appelée la couche Workgroups.

III-A-3 - La couche « cœur »

Cette couche va s'occuper de switcher le trafic vers le bon service, de la manière la meilleure et la plus rapide qui soit. Ensuite il va répondre à la couche de distribution qui si c'est un accès WAN va directement rendre réponse, soit passer la main à la couche d'accès. On l'appelle aussi la couche backbone.

III-B - Les topologies

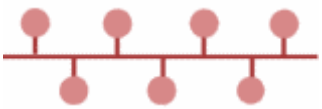
On peut différencier deux types de topologies.

- Topologie physique : c'est l'emplacement exact des appareils de réseau et comment ils sont interconnectés.
- Topologie logique : c'est comment chaque point du réseau et connecté à un autre point du réseau.

Les topologies logique et physique d'un réseau peuvent tout à fait être les mêmes. Mais cela peut aussi être tout à fait différent.
La topologie est définie dans la couche physique et la couche de liaisons de données du modèle OSI.

III-B-1 - La topologie en bus

Dans cette topologie, chaque élément est relié au même câble. Le câble se termine par un « bouchon », pour absorber le signal à la fin du parcours, pour ne pas causer d'erreurs dans le système. Cette structure est très vulnérable, car si un seul des hôtes tombe, tout le réseau tombe.



Topologie en bus

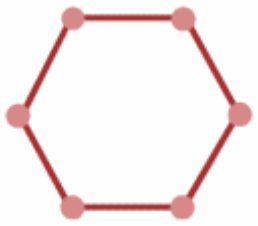
III-B-2 - La topologie en étoile

Ce type de réseau est très employé, car efficace et peu couteux. Tous les éléments sont reliés à un point central. Si un hôte tombe, seul celui-ci tombe, par contre si un élément central tombe, tout le réseau tombe.

Topologie en étoile

III-B-3 - La topologie en anneau

Une topologie en anneau ressemble assez à une topologie en bus, sauf qu'elle n'a pas de fin ni de début, elle forme une boucle. Quand un paquet est envoyé, il parcourt la boucle jusqu'à ce qu'il trouve le destinataire. Il existe soit la topologie en anneau simple soit la topologie en double boucle(FDDI), qui permet une redondance et qui comme son nom l'indique est formée de deux anneaux.



Topologie en anneau

Topologie en double anneau

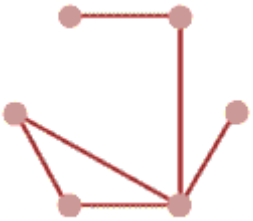
III-B-4 - La topologie point par point

Cette topologie consiste à relier chaque point l'un à l'autre, ce qui implique un coût extrêmement élevé. Cette topologie n'est pas utilisée en pratique, mais c'est sur une topologie pareille qu'est basé Internet. C'est la technologie la plus sûre.

Topologie point par point

III-B-5 - La topologie quelconque

Cette topologie est malheureusement souvent utilisée. Elle ne suit aucune règle précise et de ce fait n'est pas très fiable ni efficace… Elle apparaît souvent lorsque l'on connecte ensemble des sous-réseaux.



Topologie quelconque

III-C - Couche physique : détails

Cette couche définit le type de média, le type de connecteurs et le type de signal. Elle spécifie le voltage, la vitesse de transfert, la distance de transmission maximale et les connecteurs physiques.

III-C-1 - Spécifications IEEE 802.3

Type	10 base 2	10 base 5	10 base t	10 base fl	100 base tx	100 base fx
Media	Coaxial fin Thinet	Coaxial épais thicknet	UTP/STP	Mutlimode	UTP/STP	Multimode
Connecteurs	BNC	AUI	RJ45	ST	RJ45	SC
Longeur max.	185m	500m	100m	2000m	100m	2000m
Topologies	Bus	Bus	Etoile	Etoile	Etoile	Etoile
Bande passante	10 MBits/s	10 MBits/s	10 MBits/s	10 MBits/s	100 MBits/s	100 MBits/s

Type	1000 base sx	1000 base lx	1000 base zx	1000 base tx
Media	Multimode	Multi mono	Monomode	UTP/STP
Connecteurs	SC	SC	SC	RJ45
Longeur max.	550m	10000m	70000m	100m
Topologies	Etoile	Etoile	Etoile	Etoile
Bande passante	1000 MBits/s	1000 MBits/s	1000 MBits/s	1000 MBits/s

III-C-2 - Périphériques

Les périphériques de la couche 1 sont les appareils les plus basiques du réseau :

- Repeater : cet appareil permet d'étendre l'utilisation d'un média en régénérant le signal, et ainsi, lui permettre d'atteindre une plus longue distance ;
- Hub : il a la même fonction que le repeater, à la différence près qu'il possède plusieurs ports, donc il divise le signal en plusieurs parties, tout en le régénérant. Dès qu'il reçoit un paquet sur un port, il l'envoie automatiquement sur tous les autres ports. Il est déconseillé maintenant d'utiliser des hubs, il faut leur préférer les switchs, car avec un hub la bande passante est divisée par le nombre de machines connectées et en plus le domaine de collision est le même pour toutes les machines interconnectées.

III-D - Couche liaison de données : détails

Alors que la couche 1 ne gérait aucun adressage, cette couche gère l'adressage via les adresses physiques (MAC) des machines.

III-D-1 - L'adresse MAC

L'adresse mac est une adresse de 48 bits de 12 chiffres hexadécimaux. Cette adresse est un identifiant physique, stockée dans la mémoire de la carte réseau. Elle identifie donc l'interface réseau de la machine.

III-D-2 - Périphériques

Les périphériques de la couche 2 sont déjà moins basiques que ceux de la couche 1, ils permettent déjà de l'adressage et sont plus intelligents :

- Bridge : c'est une sorte de hub, mais en plus intelligent. Il crée plusieurs domaines de collisions, permet le passage de paquets entre plusieurs segments LAN, maintient à jour une table d'adresses MAC ;

- Switch : aussi dans la couche 2, car il emploie aussi les adresses MAC. En fait, il est formé de plusieurs hubs. Un switch peut avoir une adresse MAC, qui va servir au routeur pour le rediriger. Chaque port du switch a son propre domaine de collision. Il a aussi sa propre table d'adresses MAC.

Le but de cette couche est surtout de réduire les collisions.

III-E - Couche réseau : détails

Cette couche gère un adressage autre que l'adressage de la couche 2, c'est un adressage réseau et non plus physique, aussi appelées adresses logiques ; il s'agit des adresses IP.

III-E-1 - Adresse IP

L'adresse IP est une adresse de 32 bits, répartis en 4 fois 8 bits (octets). Cette adresse est un identifiant réseau. On peut ensuite la diviser en deux portions : la portion du réseau et la portion hôte. La première identifie le réseau sur lequel est la machine et la deuxième identifie la machine en elle-même. Pour identifier ces deux parties, chaque adresse est liée à un masque de sous-réseau. Ce qui permet de définir sur quel réseau elle se trouve.

III-E-2 - Périphériques

Le périphérique principal qui est sur cette couche est le routeur. Il est utilisé pour relier et faire communiquer ensemble des réseaux différents. Pour cela, il utilise une table de routage, dans laquelle il va stocker des informations importantes aidant au routage entre différents réseaux, sur quelle interface est ce réseau, à quelle distance (nombre de sauts) est ce réseau, sur quelle plage d'adresse est ce réseau. Il peut aussi s'occuper de router deux réseaux sur deux protocoles différents.

III-F - Couche Transport : détails

Cette couche gère les transmissions entre les protocoles de la couche réseau (IP, IPX) et les protocoles propres à la couche transport (TCP, SPX).

III-F-1 - Périphériques

Les seuls appareils qui appartiennent à cette couche sont les appareils multicouches, tels qu'un switch qui peut utiliser aussi les adresses IP.

IV - Types de réseau

IV-A - Lan : Détails

Le réseau Lan est le réseau le plus employé de nos jours. Depuis qu'Internet a été créé, c'est-à-dire depuis environ 20 ans, le LAN a beaucoup évolué pour correspondre aux nouvelles technologies. Il existe différentes technologies de LAN : Ethernet, Fast Ethernet et Gigabit Ethernet. Un Lan est confiné dans un petit endroit, il ne couvre pas de longues distances. Le Lan s'étend sur les couches Physique et liaison de données du modèle OSI.

IV-A-1 - Ethernet (IEEE 802.3)

C'est le type de Lan le plus employé. Ce standard, développé par IEEE, est basé sur un processus appelé « carrier sense multiple accès collision detect » (CSMA/CD). Ce standard est aujourd'hui tout simplement appelé Ethernet.

IEEE divise la couche de liaison de données en deux : LLC (couche du haut vers réseau) et MAC (couche du bas vers physique). Les signaux Ethernet sont transmis à chaque station en utilisant une série de règles pour savoir quelle station peut « parler » et quand.
Avant de transmettre un signal, le PC commence par écouter le réseau et ensuite, si le réseau est prêt, il envoie ses données. Ensuite il attend à nouveau un temps et continue à envoyer. Ainsi, aucun PC n'a de priorité sur les autres. Mais il est possible que deux PC écoutent en même temps et voient en même temps que le réseau est libre, donc envoient simultanément un paquet, ce qui crée une collision ; les données du paquet sont perdues et les PC doivent donc recommencer l'envoi. Quand une collision est détectée, un message JAM est envoyé à toutes les machines, comme ça les machines sont alertées et ne vont pas continuer d'envoyer en même temps les paquets, ce qui pourrait créer une boucle infinie et un arrêt complet du réseau, mais les JAM sont là pour éviter ça.
L'Ethernet a une vitesse de 10 Mbps.

IV-A-2 - Fast Ethernet (IEEE 802.3u)

Ce standard augmente la vitesse de transmission de 10 à 100 Mbps. Les changements sont minimaux, car il n'y a pas besoin de changement d'application ni de protocoles

IV-A-2-a - Spécifications

Protocole	Vitesse	Média
100 Base-T	100	Paire torsadée
100 Base-F	100	Mono ou Multimode fibre
100 Base-X	100	Fibre ou cuivre
100 Base-FX	100	Multimode fibre
100 Base-T4	100	Cuivre UTP 4 paires Category 3-5
100 Base-TX	100	2 Paires cuivre Category 5

IV-A-3 - Gigabit Ethernet (IEEE 802.3z)

Ce standard, quant à lui, permet une vitesse de transmission de 1000 Mbps. Il est utilisé avec des fibres ou des câbles à paires torsadées. C'est devenu un standard très utilisé pour les connexions haute vitesse, par exemple sur les backbones. Il est aussi utilisé pour la connexion de plusieurs endroits ensemble.

IV-A-3-a - Spécifications

Protocole	Vitesse	Média
1000Base-LX	1000	Mono ou Multimode fibre
1000Base-SX	1000	Multimode fibre
1000Base-CX	1000	2 paires Cuivres STP
1000Base-T	1000	Category 5 cuivre

IV-A-4 - 10 Gigabit Ethernet (IEEE 802.3ae)

Ce standard est le plus rapide, il permet une vitesse de transmission de 10 GBps. Il est utilisé soit avec de la fibre optique soit avec des câbles à paires torsadées. Ce standard est surtout utilisé pour des accès à des bases de données de gros volume ou moins souvent pour le backbone.

IV-B - Wan : Détails

Ce type de réseau couvre une région géographique plus ou moins grande. C'est une interconnexion de Lan d'habitude. Il emploie les trois premières couches du modèle OSI.

Les périphériques employés sur ce réseau sont les suivants :

- les routeurs qui font la liaison entre le LAN et le Wan ;
- les switchs WAN, qui redistribuent le réseau Wan ;
- les modems qui font une liaison entre deux Lan par le Wan, en passant par le réseau téléphonique…

Le principal désavantage du Wan est sa vitesse, car il ne s'agit pas de fibre optique ni de paire torsadée, mais il s'agit de passer sur le réseau public, donc par un provider pour relier deux Lan très éloignés. Ce type de réseau est de moins en moins employé, on préfère maintenant installer des lignes fibre optiques donc connexion Lan sans plus passer sur un réseau public. La meilleure des alternatives au Wan est le MAN.

IV-C - Man : Détails

Un Man est une sorte de Wan, sauf que c'est à haute vitesse et qu'il passe par les médias propres au réseau et non plus par un provider externe. C'est très employé pour la connexion de plusieurs lieux de travail d'une entreprise dans une même ville ou même plus loin qu'une ville, dans un même canton. Même s'il est sûr que c'est plus cher d'interconnecter soi-même que de passer par un provider, c'est beaucoup plus rapide et fiable et cela peut même se révéler rentable à plus long terme.

IV-D - Storage area network (SAN)

Un réseau San est utilisé pour transférer des données des serveurs jusqu'à des ressources de stockage. On utilise d'habitude de la fibre pour ces connexions, car on leur préfère leur grande rapidité. Ce réseau est isolé du reste du réseau, ce qui permet une meilleure configuration et sécurité de celui-ci. Le cout d'installation d'un San est très élevé justement à cause du fait de son isolation. Mais par contre on n'a plus besoin de se préoccuper de l'espace de stockage de chaque serveur, puisque l'espace de stockage forme un tout.

IV-E - Content Network (CN)

C'est un réseau qui s'occupe d'accélérer l'envoi de données entre les services réseau (Web, Streaming, applications, etc.). Il optimise l'envoi des informations vers les demandeurs. Il divise en plusieurs parties les technologies des services pour permettre une meilleure distribution de ceux-ci. Il va par exemple choisir le meilleur serveur pour telle ou telle ressource, il va aussi choisir le bon site pour le téléchargement d'une information et va s'occuper de garder « au frais » des ressources statiques ou en streaming pour qu'elles soient disponibles plus rapidement.

IV-F - Virtual private Network (VPN)

Un réseau VPN permet de créer un tunnel par exemple depuis votre maison jusqu'à l'entreprise via l'Internet. Par ce tunnel vous serez virtuellement dans le réseau de votre entreprise tout en étant physiquement chez vous.
Pour faire une liaison, il faut passer par le réseau public.

Il existe plusieurs types de VPN :

- Access VPN : c'est le VPN qui lie un travailleur mobile ou une personne travaillant chez elle jusqu'à au réseau de l'entreprise. La connexion se fait habituellement par modem, ISDN, dialup, DSL… ;
- Intranet VPN : c'est le réseau qui lie des bureaux régionaux jusqu'au réseau de l'entreprise. Il ne permet l'accès au réseau qu'aux membres de l'entreprise ;

- Extranet VPN : c'est le réseau utilisé pour lier les entreprises externes sur le réseau de l'entreprise. L'accès est permis pour un groupe de gens bien défini.

V - La couche physique

Un média est un support par lequel vont passer des données.

V-A - Câble à paire torsadée

Un câble à paire torsadée est un câble dans lequel passent des fils de cuivres. C'est le média le plus employé de nos jours. C'est un câble utilisé pour câbler des courtes distances. Ces câbles ne peuvent couvrir qu'au maximum 100 mètres.

Un câble à paire torsadée est composé de plusieurs éléments :

- des brins de cuivre entrelacés ;
- d'une enveloppe isolante autour.

Il en existe plusieurs catégories :

- Catégorie 1 : utilisé pour les communications téléphoniques, inutilisables pour le transfert de données ;
- Catégorie 2 : transmission de données à 4 Mbps ;
- Catégorie 3 : transmission de données à 10 Mbps ;
- Catégorie 4 : utilisé dans les réseaux Token Ring, transmission à 16 Mbps ;
- Catégorie 5 : transmission de données à 100 Mbps ;
- Catégorie 5e : transmission de données à 1 Gbps ;
- Catégorie 6 : consiste en 4 paires de 24 gauges de cuivre, 1 Gbps ;
- Catégorie 7 : transmission de données à 10 Gbps.

V-A-1 - UTP

C'est un câble à paire torsadée tout simple, sans aucun blindage. Il est fait de quatre paires de brins. Il est très utilisé pour les téléphones, car il est plus petit qu'un câble STP.

V-A-2 - STP

L'ensemble des paires torsadées est entouré d'un blindage. Il est plus utilisé dans les réseaux Ethernet que l'UTP, car il permet de réduire les effets électromagnétiques sur le câble grâce à son blindage. Il existe encore une autre variante, le SSTP, qui rajoute un blindage supplémentaire sur chaque paire.

Le blindage permet de réduire les interférences, donc le mélange de signaux électriques et il permet des transferts à des débits plus importants et sur des distances plus grandes.

V-B - Câble coaxial

Un câble coaxial consiste en un conducteur de cuivre isolé dans une insolation. Autour de cette isolation, il y a un bouclier en cuivre qui aide à réduire les interférences. Ce câble peut supporter des vitesses de 10 ou 100 Mbps et n'est pas très couteux, bien que plus cher que l'UTP. Par contre, il peut couvrir des distances plus longues que l'UTP, jusqu'à 500 mètres.

V-C - Câble fibre optique

Un câble fibre optique est fait de deux fibres, chacune est blindé et ensuite mises dans un « tube » en plastique qui vient ensuite se coller au tube de la deuxième fibre. Il existe une multitude de connecteurs pour la fibre optique, que vous choisirez surtout en fonction de leur taille, de leur robustesse et de leur prix. Ce média permet des liaisons longues, voire très longues distances à des débits élevés.

Il existe deux types de fibre optique :

- Monomode : utilisée pour les très longues distances, son prix est très élevé. Le laser circule tout droit ;
- Multimode : utilisée plutôt en local pour les connexions appareils réseaux - serveurs. Elle coute moins cher que de la Multimode, mais comme toute fibre, son prix reste élevé. Le laser circule à l'intérieur de la fibre en rebondissant sur les côtés.

La fibre optique est le type de câblage le plus avancé technologiquement. Un des plus gros avantages est le fait qu'il est insensible aux perturbations électromagnétiques, puisqu'il transporte de la lumière. De plus, il est aussi insensible aux écoutes clandestines puisque pour l'écouter, il faudrait se couper directement dessus, ce qui bien sûr, couperait la communication. Un câble optique peut négocier des transferts allant jusqu'à 200 Gigabit/s. Et là on parle de distances dépassant plusieurs kilomètres, ce qu'aucun câble de cuivre ne permet de faire. Aujourd'hui, c'est la meilleure solution pour des grandes distances et des gros transferts. Mais il faut quand même de gros moyens pour mettre en place une solution fibre optique.

V-D - Communications Wireless

La communication par Wireless utilise des fréquences radio ou infrarouges pour communiquer entre plusieurs appareils dans un LAN. Les signaux Wireless sont des signaux électromagnétiques qui peuvent conduire des données. Plus on augmente la fréquence des signaux, plus la distance sur laquelle l'onde est propagée diminue.
Les communications par Wireless ont pas mal d'avantages : l'accès à Internet par des natels, transfert de données entre deux périphériques sans fil, permet de diminuer le nombre de câbles, augmente la mobilité, permet la connexion de souris et clavier…

V-E - Tableau comparatif médias

Media	Longueur max	Vitesse	Coût	+	-
UTP	100	10-100	Le - cher	Facile à installer Facile à utiliser	Sensibles interférences Distance limitée
STP	100	10-10000	Un peu + cher	Peu sensible inter.	Distance limitée
Coaxial	500	10-100	Peu cher, mais + qu'UTP	Peu sensible inter.	Distance et bande passante limitées
Fibre optique	70'000	10-10000	Cher	Grande distance, très bonne bande passante et pas sensible aux interférences	Difficile d'utilisation et sensible
Wireless	50	1-540	Cher	Pas de média physique	Sensible aux conditions

					atmosphériques, difficile à sécuriser

V-F - Câblage Lan

Beaucoup de types de médias peuvent être employés dans un LAN, il vous appartient de faire le choix le plus approprié à vos besoins. Avant de monter un réseau LAN, vous devez définir quels seront les besoins des utilisateurs de ce réseau, la vitesse, la mobilité, la stabilité, la disponibilité… Vous devez aussi définir quel sera votre budget pour ce Lan. Vous devrez définir les vitesses du réseau à tel ou tel endroit, la façon dont vont se connecter les utilisateurs, depuis ou vont-ils pouvoir se connecter et quelle vitesse de connexion vous voulez leur accorder. Voulez-vous pencher vers un réseau très rapide, mais très couteux ou alors vers un réseau de vitesse normale, mais de cout plus réduit.

Dès que vous aurez défini ces choses, vous serez en mesure de choisir les médias dont vous aurez besoin, peut du STP pour connecter les PC et de la fibre pour la connexion des serveurs. Il vous faudra aussi bien sûr définir les connecteurs dont vous aurez besoin pour chaque média. Les connecteurs ne sont pas plus performants les uns que les autres, mais certains sont plus petits, d'autres plus stables, d'autres encore sont plus solides, d'autres sont faits pour telles ou telles applications et d'autres pas…

Il faut aussi penser à ce que vont connecter vos câbles, parce que pour l'interconnexion des éléments suivants, il faut des câbles croisés :

- Switch à switch ;
- Switch à hub ;
- Hub à hub ;
- Routeur à routeur ;
- PC à PC ;
- Routeur à PC.

Mais certains éléments réseau peuvent s'occuper de croiser eux-mêmes les pins si besoin est.

V-G - Câblage Wan

Les réseaux Wan sont de moins en moins employés au vu de leur vitesse réduite, c'est pourquoi nous n'allons pas consacrer beaucoup de temps à leur étude.

Pour les communications longues distances, le réseau WAN utilise une communication sérielle. Pour faire un réseau Wan, vous devrez surtout définir la vitesse à laquelle vous voudrez transférer des infos. Si vous voulez des grandes vitesses, il vous sera plus facile alors de louer des fibres optiques ou alors de faire poser vos propres fibres.

On distingue dans le WAN, deux types d'appareils :

- le DTE : c'est le périphérique qui relie le Lan jusqu'au DCE. C'est d'habitude un routeur ;
- le DCE : c'est le périphérique qui fait la liaison WAN. C'est des modems ou autres choses dans le genre.

Par exemple, on peut avoir un routeur avec d'un côté le Lan et de l'autre côté un port série qui va sur le modem(DCE). Et de l'autre côté de la ligne, le DCE va de nouveau aller en sérial sur un autre routeur qui va lui, faire la connexion avec le deuxième réseau LAN. Il existe aussi des appareils qui remplissent directement les deux fonctions.

La connexion est souvent une liaison DSL.

VI - La couche de liaison de données

Avec l'évolution et l'augmentation de la vitesse des machines, il devient impératif d'augmenter aussi la vitesse de connexion et la stabilité du réseau pour éviter que ces machines ne saturent le réseau.

VI-A - Segments Ethernet

Un segment est une connexion faite par un simple câble. La longueur maximale d'un segment est définie par la longueur possible du média. Par exemple on pourra faire un segment de 100 mètres avec un câble UTP et un segment de 10 km avec un câble fibre monomode. Il est possible d'augmenter la longueur d'un segment grâce à un hub ou à un repeater. Mais on ne peut le faire infiniment, car le signal se dégrade quand même peu à peu à chaque fois qu'il est répété. On peut retenir la règle suivante : il ne faut jamais mettre plus de quatre hubs entre deux PC.

Dans un Lan, chaque frame est reçue par chaque PC, il est donc nécessaire de savoir si la frame concerne ce PC, pour qu'il ne doive pas tout lire. C'est pour ça qu'il a trois possibilités de communication :

- Unicast : le message est envoyé seulement à une adresse de destination et seulement celui-ci pourra lire ce message. C'est bien entendu la forme la plus utilisée ;
- Multicast : un message est envoyé à un groupe de PC ;
- Broadcast : le message est envoyé à tout le monde. C'est une adresse broadcast qui permet ceci.

Une collision apparaît quand deux PC du même segment essayent d'envoyer un message en même temps. Un domaine de collision est un groupe d'appareils réseau directement connectés. Dans un domaine de collision, une seule machine peut envoyer un paquet et les autres doivent attendre. Il faut faire attention aux hubs, car ils étendent le domaine de collision.

Plus il y a de PC sur le même segment, plus la vitesse sur ce segment diminue.

VI-B - Switch et Bridge

Les bridges et les switchs sont des appareils de niveau 2 sur le modèle OSI, avec eux, on peut réduire la taille des domaines de collisions. Cela, en utilisant une table d'adresses et en envoyant le message seulement à l'adresse correcte et empêchant ainsi d'avoir plusieurs paquets passant en même temps.

La grande différence des switchs et des bridges est l'hardware, dans un switch, le code est optimisé. Donc un switch peut opérer à de plus grandes vitesses que le bridge et permet plus de choses, mais est plus cher. Voilà ce que permet le switch de plus que le bridge :

- des multiples communications simultanées ;
- des communications full-Duplex ;
- l'accès à la totalité de la bande passante par tous les appareils connectés ;
- possibilité d'associer une vitesse spécifique sur chaque port, ce qui permet de connecter des machines de différentes vitesses derrière le switch.

Le switch a une procédure bien définie pour la communication :

- le switch reçoit une frame sur un port ;
- le switch entre l'adresse MAC source et le port du switch qui a reçu la trame, dans la table MAC ;
- si l'adresse de destination est inconnue, le switch envoie la frame sur tous les ports, sinon il l'envoie sur le port correspondant à l'adresse de destination dans la table MAC ;
- le PC de destination répond ;
- là encore, le switch écrit dans la table MAC, l'adresse du répondeur et le numéro du port correspondant ;
- maintenant, si le destinataire ou l'envoyeur était inconnu, si le cas se représente où un message est envoyé à l'un des deux, le switch pourra l'envoyer directement sur le bon port.

Quand derrière un port d'un switch il y a un autre switch ou un appareil dans ce genre-là, il y a un risque que les paquets puissent tourner en boucle. Pour éviter cela, il existe le protocole « spanning tree protocol », qui permet justement d'éviter les boucles. Ce protocole permet de mettre en standby un port d'un switch pendant un moment pour éviter que celui-ci ne crée une boucle avec un autre.

VI-C - Vlan

Un Vlan se définit comme un groupe de segments Ethernet, qui ont différentes connexions physiques, mais qui communiquent comme s'ils étaient dans le même segment. Un Vlan divise le réseau en plusieurs domaines broadcast.

Un Vlan procure les avantages suivants :

- réduction du cout d'administration : par exemple si un ordinateur change de lieu physique, il suffira de le changer, mais plus besoin de reconfigurer puisqu'il sera toujours dans le même Vlan ;
- facilité d'application des policies : il est plus facile d'appliquer des policies puisqu'il suffit de les affecter au Vlan qui contient les PC sur lesquels on veut appliquer une nouvelle politique ;
- réduction du trafic : en confinant les domaines de broadcast dans un réseau, le trafic s'en voit réduit de manière significative.

Il y a deux manières d'assignement de Vlan :

- basée sur les ports : on met chaque port dans un Vlan, ce qui fait que le PC derrière ce port va se trouver dans le Vlan ;
- basée sur les Mac-Address : on fait correspondre chaque Mac- Address à un Vlan, ça donne un avantage sur la méthode 1, car ainsi si on déplace un PC, il reste de toute façon dans le bon Vlan. Mais cette méthode prend plus de temps à mettre en œuvre, mais ensuite est plus souple quand on veut changer un PC de place, puisqu'il ne faut plus rien faire.

VII - TCP-IP

VII-A - Protocoles Ip

VII-A-1 - Internet Protocol (IP)

Ce protocole utilise des paquets pour transporter des infos à travers le réseau. Chaque paquet contient l'adresse de l'envoyeur et du destinataire, mais le service IP n'assure pas que le paquet arrivera à destination, il peut être perdu ou mal dirigé. Ce protocole n'assure rien pour retrouver des paquets perdus ou rediriger des paquets mal dirigés. On pourrait faire une analogie avec le service postal, il n'assure pas que les lettres que vous envoyez passent toutes par le même endroit et n'assurent pas non plus qu'elles arrivent dans l'ordre ou vous les envoyez. C'est pareil avec le protocole IP. Comme une lettre, un paquet contient un header qui contient des infos importantes pour la distribution du paquet.

VII-A-1-a - IP Header

Nom du champ	Description	Nombre de bits
Version	Numéro de version	4
Header Length	Taille du header	4
Priority	Priorité du paquet	8
Total Length	Longueur du paquet, header + data	16
Identification	Valeur unique du paquet	16
Flags	Spécifie la fragmentation du paquet	3
Fragments offset	Fragmentation des paquets pour découper un gros message en plusieurs paquets.	13
TTL	Time To live, c'est-à-dire nombre de fois qu'il peut être lu avant d'être détruit	8
Protocole	Protocoles de destination du paquet, UDP, TCP, ICMP, IPv6…	8
Header Checksum	Intégrité du paquet	16
Source IP Adress	Adresse de la source	32
Destination IP adress	Adresse du destinataire	32
IP Options	Test, debug et autres	0 ou 32
Data	Les données du paquet	Variable

VII-A-1-b - Internet Control Message Protocol (ICMP)

Ce protocole est implémenté sur chaque hosts TCP/IP. Il dépend du protocole IP pour envoyer les paquets. Il définit un petit nombre de messages utilisés pour le diagnostic et le management. Le Ping est son utilisation la plus connue. Le message ICMP est encapsulé dans un paquet IP, il contient le type de messages, le code de l'erreur et la somme de contrôle.

Voici une petite liste non exhaustive des messages ICMP possibles :

- Destination Unreachable : la destination n'est pas pingable ;
- Time Exceeded :l e temps a été trop long ;
- Echo Reply : réponse à une demande, réponse à un Ping par exemple ;
- Echo : requête, Ping par exemple.

ICMP est employé pour compléter IP, car celui-ci ne permet rien en cas de problèmes c'est donc pour pallier ce problème qu'on emploie ICMP qui va nous « dire » s'il y a un problème.

VII-A-1-c - Adress Resolution Protocol (ARP)

Ce protocole permet la résolution des adresses MAC à partir de l'adresse IP.

VII-A-1-d - Reverse Adress Resolution Protocol (RARP)

Ce protocole permet la résolution des adresses IP à partir de l'adresse MAC.

VII-A-1-e - Dynamic Host Configuration Protocol (DHCP)

Ce protocole permet de configurer automatiquement les paramètres réseau d'une machine dès son entrée dans le réseau. Il attribue automatiquement l'adresse IP, le masque de sous-réseau, la passerelle et aussi le serveur DNS. Ce protocole passe par le protocole TCP/IP.

VII-A-2 - Couche transport

Cette couche est le cœur du protocole TCP/IP. C'est une couche très importante du protocole TCP/IP. Il y a deux protocoles qui œuvrent sur cette couche :

- UDP : ce protocole est plus rapide que le TCP, mais il n'exécute aucun contrôle quand au fait que le paquet soit arrivé à destination ou pas. C'est un protocole non orienté connexion.
- TCP : ce protocole est un plus lent, mais il va s'occuper de contrôler que le paquet arrive bel et bien à destination. Ce protocole est orienté connexion. À la suite, vous trouverez les caractéristiques du protocole TCP.

Caractéristiques du TCP-IP

- Orienté Connexion : le protocole crée une liaison entre les deux périphériques voulant se parler ;
- Full Duplex : on peut parler et écouter en même temps ;
- Contrôle des erreurs : il vérifie que les paquets ne sont pas corrompus ;
- Numérotation des paquets pour que la remise en ordre de ceux-ci soit plus aisée ;
- Contrôle de flux : Si l'envoyeur surcharge le buffer, il va lui dire d'arrêter l'envoi.

Voici quelques applications du TCP/IP :

- FTP : emploi du TCP pour envoyer des fichiers ;
- TFTP : emploi de l'UDP pour envoyer des fichiers, c'est un peu plus rapide que le FTP, et c'est donc employé dans les cas ou ce n'est pas trop grave de perdre un paquet ;
- Telnet : permet de se connecter à distance sur un autre périphérique ;
- SMTP : permet l'envoi de mail.

VII-A-2-a - TCP Header

Nom du champ	Description	Nombre de bits
Source port	Numéro du port sortant	16
Destination port	Numéro du port entrant	16
Sequence Number	Numéro utilisé pour remettre les paquets dans le bon ordre	32
Acknowledgments Number	Prochain octet	32
Header Length	Taille du header	4
Reserved	Réservé pour un usage futur, doit être 0	6
Code bits	Fonctions pour terminer ou commencer une session	6
Window	Nombre d'octets que le périphérique peut accepter	16
Checksum	Somme du header et des champs de données	16
Urgent		16
IP Options	Longueur maximale du segment TCP	Variable
Padding	Ce champ est utilisé pour être sûr que le header se termine dans un multiple de 32 bits.	Variable
Data	Les données du paquet	Variable

VII-A-2-b - UDP Header

Nom du champ	Description	Nombre de bits
Source port	Numéro du port sortant	16
Destination port	Numéro du port entrant	16
Length	Longueur du header et des données	16
Checksum	Somme du header et des champs de données	16
Data	Les données du paquet	Variable

Le header UDP est plus simple puisque l'UDP assure moins de choses que le TCP.

VIII - Adressage IP et routage IP

VIII-A - IP Addresses

Une adresse IP est une adresse de 32 bits, séparées en groupe de quatre octets par des points. Chaque octet peut donc aller de 0 à 255. On l'écrit d'habitude en décimal, mais il est toujours codé en binaire. Chaque adresse IP est formée d'une partie réseau et d'une partie hôte.

VIII-B - Classes IP

Pour différencier différentes tailles de réseau et permettre de mieux identifier des adresses, on a séparé les adresses IP en cinq classes.

VIII-B-1 - Classe A

Cette classe est faite pour les très grands réseaux. Seul le premier octet est utilisé pour la partie réseau, ce qui laisse donc trois octets pour la partie hôte. Ce premier octet est compris entre 1 et 126. Cette classe peut accueillir plusieurs millions d'hôtes.

VIII-B-2 - Classe B

Cette classe est faite pour les moyens et grands réseaux. Les deux premiers octets sont utilisés pour la partie réseau et les deux suivants pour la partie hôte. Le premier octet est compris entre 128 et 191. Cette classe peut accueillir plusieurs dizaines de milliers d'hôtes.

VIII-B-3 - Classe C

Cette classe est faite pour les petits réseaux puisqu'elle ne peut accueillir que 254 hôtes. Les trois premiers octets étant employés pour la partie réseau, il n'en reste qu'un seul pour la partie hôte. Le premier octet est compris entre 192 et 223.

VIII-B-4 - Classe D

C'est une classe utilisée pour le multicasting. Le premier octet de cette classe est compris entre 224 et 239.

VIII-B-5 - Classe E

Cette classe a été définie comme étant une classe pour les ordinateurs de recherche. Le premier octet de cette classe est compris entre 240 et 255.

VIII-C - Adresse réseau et Broadcast

Certaines adresses sont réservées et ne peuvent être utilisées pour les hôtes. C'est le cas de l'adresse de Broadcast et de l'adresse réseau.

VIII-C-1 - Adresse réseau

Cette adresse sert à identifier le réseau, chaque bit de la partie hôte de l'adresse est fait de 0. Par exemple pour une classe A, l'adresse réseau serait XXX.0.0.0 et pour une classe C ce serait XXX.XXX.XXX.0. On ne peut pas employer cette adresse pour un hôte, c'est donc une adresse de perdue.

VIII-C-2 - Adresse Broadcast

Cette adresse est utilisée pour envoyer un message à toutes les machines d'un réseau. Chaque bit de la partie hôte de l'adresse est fait de 1. Par exemple pour une classe A, l'adresse réseau serait XXX.255.255.255 et pour une classe C ce serait XXX.XXX.XXX.255. On ne peut pas employer cette adresse pour un hôte, c'est donc une autre adresse de perdue. Le routeur quand il va recevoir une adresse de Broadcast, va envoyer le message dans tous les périphériques du réseau concerné. On peut aussi utiliser l'adresse de Broadcast « générale », c'est-à-dire envoyé un message à tous les périphériques de tous les réseaux connectés sur le même réseau que nous ; pour cela, il suffit d'employer l'adresse 255.255.255.255.

VIII-D - Calcul sur adresse IP

N => Nombres de bits après la partie réseau de la classe (donc 2 pour 255.255.192.0 si classe B)
n => Nombres de bits dans la portion hôte

2^N -2 = nombre de sous-réseaux

2^n -2 = nombre d'hôtes par sous-réseau

VIII-E - 1.7.5 Adresses privées et publiques

Il existe des adresses privées, dans chaque classe :

- A --> 10.0.0.0 à 10.255.255.255
- B --> 172.16.0.0 à 172.31.255.255
- C --> 192.168.0.0 à 192.168.255.255

Une adresse IP privée n'est pas visible sur Internet, au contraire d'une IP publique. On emploie les adresses privées à l'intérieur du réseau et les adresses publiques sont des adresses Internet. En interne, il y aura donc un routeur qui va dire où aller pour rejoindre une adresse publique. On peut accéder à une adresse publique depuis n'importe où dans le monde alors qu'on ne pourra jamais arriver sur une adresse privée sans être dans le même réseau qu'elle ou à moins de réussir à pirater le réseau.

VIII-F - Épuisement des adresses IP

Au départ de l'Internet, on ne prévoyait pas autant de monde sur Internet en même temps. On a donc commencé avec de l'IPv4, mais ce protocole commence à ne plus suffire. Une alternative est donc l'IPv6. Ce protocole permet bien plus de hôtes que l'IPv4, car il est codé sur 128 bits et supporte 3.4 * 10^38 adresses, alors que l'Ipv4 permet « seulement » environ 4.3 milliards d'hôtes.

VIII-G - Le subnetting

On peut encore subdiviser un réseau, pour cela, on a recours à des sous-réseaux (subnet), c'est le subnetting, qui permet d'étendre le nombre de réseaux. Chaque adresse qui est subnettée a obligatoirement un masque de sous-réseau. C'est lui qui permet d'identifier le sous-réseau d'où vient l'adresse.
Le masque de sous-réseaux est formé seulement d'une suite de 1 suivie d'une suite de 0. Il ne peut pas y avoir de 1 suivi de 0 puis un recommencement avec des 1. Il n'est donc formé que des nombres suivants : 0, 128, 192, 224, 240, 248, 252, 254, 255. Ce masque sert aux routeurs et autres appareils à trouver de quel réseau ou sous-réseau fait partie l'adresse.

VIII-H - Calcul sous-réseaux (identification des adresses)

Pour calculer le sous-réseau d'une adresse et les adresses de ce réseau, il faut commencer par prendre le masque de sous-réseau et de trouver en quelle position se trouve le dernier 1. Ensuite, il faut prendre l'adresse IP et la couper à la position que l'on a trouvée. On aura donc une adresse incomplète, il suffira de remplir par des 0 les trous pour trouver le sous-réseau, par des 1 pour trouver le broadcast, par des 0 suivi d'un 1 pour trouver la première adresse utilisable du réseau et par des 1 suivi d'un 0 pour trouver la dernière adresse utilisable de ce réseau.

VIII-H-1 - Exemple 1

Adresse IP : 172.16.2.10
Masque de sous -réseau : 255.255.255.0

10101100.00010000.00000010.//00001010 IP
11111111.11111111.11111111.//00000000 Masque
10101100.00010000.00000010.//00000000 Subnet ==> 172.16.2.0
10101100.00010000.00000010.//11111111 Broadcast ==> 172.16.2.255
10101100.00010000.00000010.000000001 First ==> 172.16.2.1
10101100.00010000.00000010.111111110 Last ==> 172.16.2.254

Subnet ==> 172.16.2.0

VIII-H-2 - Exemple 2

Adresse IP : 201.222.10.60
Masque de sous-réseau : 255.255.255.248

11001001.11011110.00001010.00111//100 IP
11111111.11111111.11111111.11111//000 Masque
11001001.11011110.00001010.00111//000 Subnet ==> 201.222.10.56
11001001.11011110.00001010.00111//111 Broadcast ==> 201.222.10.63
11001001.11011110.00001010.00111//001 First ==> 201.222.10.1
11001001.11011110.00001010.00111//110 Last ==> 201.222.10.62

Subnet ==> 201.222.10.56

VIII-I - Tableau des sous-réseaux

VIII-I-1 - Classe B

Nombre de bits	Masque	Nombres de sous-réseaux	Nombres d'hôtes
2	255.255.192.0	2	16382
3	255.255.224.0	6	8190
4	255.255.240.0	14	4094
5	255.255.248.0	30	2046
6	255.255.252.0	62	1022
7	255.255.254.0	126	510
8	255.255.255.0	254	254
9	255.255.255.128	510	126
10	255.255.255.192	1022	62
11	255.255.255.224	2046	30
12	255.255.255.240	4094	14
13	255.255.255.248	8190	6
14	255.255.255.252	16382	2

VIII-I-2 - Classe C

Nombre de bits	Masque	Nombres de sous-réseaux	Nombres d'hôtes
2	255.255.255.192	2	62
3	255.255.255.224	6	30
4	255.255.255.240	14	14
5	255.255.255.248	30	6
6	255.255.255.252	62	2

VIII-J - Routage

Le routage est la fonction qui s'occupe de diriger les données réseau à travers différents segments. Il va diriger jusqu'au prochain point de route. Cette fonction emploie des algorithmes de routages et des tables de routage (carte routière en quelque sorte). Le principal périphérique de routage est le routeur. Il utilise les adresses IP pour diriger correctement les paquets d'un réseau ou segment à un autre. Il doit maintenir sa table de routage à jour et connaître les changements effectués sur les autres appareils par lequel il pourrait faire transiter le paquet.
Pour remplir et mettre à jour la table de routage, il y a deux manières de faire, on peut le faire soit manuellement soit de manière dynamique en employant des processus tournant sur le réseau.

VIII-J-1 - Routes statiques

Le routeur apprend ces routes quand l'administrateur les entre manuellement. Cela peut prendre un temps considérable si l'entreprise possède beaucoup de routeurs et en cas de modification d'un réseau, il va falloir passer sur tous les routeurs pour faire la modification.

VIII-J-2 - Routes dynamiques

Le routeur apprend ces routes de manière automatique. Pour cela, on utilise un protocole de routage, qui va s'occuper de remplir la table de routage selon ses propres critères. Dès qu'il y a un changement sur le réseau, le routeur va l'apprendre automatiquement et il n'y aura pas besoin d'une intervention manuelle sur le routeur pour changer quelque chose puisque le protocole va s'en charger. Il faut bien entendu plusieurs routeurs pour que cela serve à quelque chose.

VIII-J-3 - Types de protocoles de routage

Chaque protocole de routage maintient une table de routage à jour avec les informations suivantes : la destination et la « priorité » de celle-ci. Pour que deux routeurs se partagent ensemble leur table de routage, il faut bien entendu que ceux-ci soient configurés sur le même protocole de routage. Un protocole de routage sert à améliorer la vitesse de routage, à gagner du temps en évitant de devoir configurer manuellement toutes les routes sur chaque routeur, à améliorer la stabilité du réseau en choisissant chaque fois la meilleure route.

VIII-J-3-a - Distance Vector Protocol

Ce type de méthode compte le nombre de sauts qu'il y a entre deux endroits. Et c'est en fonction de ce nombre de sauts qu'il va choisir le chemin le plus correct. Tous les tant de temps (temps très court, d'habitude dans les 30 secondes), il envoie sa table de routage complète à tous les routeurs voisins pour que tous soient toujours à jour. À chaque fois qu'il reçoit une table d'un voisin, il va l'analyser pour contrôler que rien n'a changé depuis la dernière fois et si besoin est, il va effectuer des modifications dans sa propre table.
Les protocoles basés là-dessus sont RIP et IGRP

VIII-J-3-b - Link-State Routing Protocol

Ce type de méthode se base sur l'état de la route, c'est-à-dire l'état des routeurs sur lesquels il doit passer. Il va donc choisir un chemin sur lequel il est sûr que tout marche pour rediriger le paquet. Dès qu'un lien change d'état, le périphérique qui a détecté le changement envoie un paquet avec les données de ce changement à tous les routeurs. Chaque routeur met donc à jour sa table avec les données du paquet. Ce protocole est moins « lourd » que le DVP, car il envoie beaucoup moins de paquets que lui et ne risque donc pas de surcharger le réseau.
Le principal protocole basé là-dessus est l'OSPF.

VIII-J-3-c - Hybrid Routing Protocol

Ce type de méthode est quant à lui, un mélange des deux techniques que nous voyons de voir. Il possède donc beaucoup d'avantages.
Un protocole basé là-dessus est l'EIGRP.

VIII-J-4 - Protocoles de routage

VIII-J-4-a - RIP

Ce protocole utilise Distance Vector Protocol. S'il y a plusieurs chemins possibles pour un paquet, il va choisir le chemin le plus court en nombre de sauts. RIP a besoin de souvent se mettre à jour, pour cela, un paquet va être envoyé toutes les 30 secondes environ, ce qui peut causer pas mal de trafic. Un autre problème est le fait qu'il ne peut gérer que 15 sauts. Donc si un PC se trouve éloigné d'un autre de plus de 15 routeurs, il n'y aura aucune communication entre eux. RIPv1 ne supporte pas différents masques de sous-réseaux.

VIII-J-4-b - IGRP

Ce protocole utilise Distance Vector Protocol. Il n'y a pas de limites de taille de réseau avec IGRP. Par contre il ne supporte pas différents masques de sous-réseaux. Il est actualisé toutes les 90 secondes. Il a plus de critères que le protocole RIP, il peut aussi prendre en compte, la bande passante, le délai, la charge réseau. On peut même donner manuellement une priorité à chacune de ses conditions.

VIII-J-4-c - EIGRP

Ce protocole est une amélioration d'IGRP. Il cumule les avantages du Vector Distance Protocol et du Link State Protocol. Il n'est pas limité en sauts. Comme IGRP, il se base aussi sur des critères auxquels on peut donner des pondérations, mais y ajoute l'état des liens. Avec le protocole DUAL, il garde des chemins de secours en cas de problèmes pour permettre une convergence rapide. Il prend en compte les masques de sous-réseaux et les différents subnets.

VIII-J-4-d - OSPF

La convergence en cas de problèmes est plus rapide qu'avec RIP. Le nombre de sauts n'est aucunement limité. L'envoi de la table ne se fait pas de manière régulière donc une meilleure utilisation de la bande passante. En plus de se baser sur l'état des liens, il se base aussi sur le cout de tel ou tel chemin. Il est calculé en fonction de la bande passante, plus la bande passante, plus le cout est faible. Si deux chemins ont le même cout, il se basera sur le nombre de sauts.

VIII-J-4-e - BGP

Ce protocole est seulement utilisé pour faire la liaison entre deux systèmes autonomes, donc deux réseaux bien distincts. C'est le seul protocole qui utilise le protocole TCP pour le transfert de ses paquets.

IX - Utilisation des technologies WAN

IX-A - Technologies basiques Wan

Nous n'allons pas trop nous étendre sur cette technologie, car elle n'est aujourd'hui plus très utilisée.

Il existe plusieurs différentes technologies pour un Wan. Un Wan est un réseau de données qui couvre une très grande surface et qui passe par les transmissions données soit par un provider, soit par le téléphone ou alors par un câble de la compagnie.

IX-A-1 - Circuit Switching

La ligne n'est pas que pour nous, elle est publique. On fait une demande quand on va avoir besoin de passer dessus et ensuite la ligne nous est temporairement accordée. On peut citer en exemple le réseau téléphonique public ou alors l'ISDN.

IX-A-2 - Packet Switching

Avec cette technologie, les users partagent ensemble des ressources pour la transmission de données. Dans un environnement comme celui-ci, chaque client partage le réseau avec beaucoup d'autres clients.

IX-A-3 - Point to point

Il s'agit d'une ligne louée. Le client a donc cette fois une ligne pour lui tout seul ce qui augmente naturellement la vitesse de transfert. La vitesse est fixée des le départ et n'est variable qu'en fonction de ce que l'on met dessus (nos appareils). Les prix d'une telle technologie sont basés sur la bande passante de la ligne et aussi sur la distance de la ligne. Avec cette technologie, il vous faudra bien sûr un routeur de chaque côté et ensuite aussi si vous employez des connexions sérielles, il vous faudra un CSU d'un côté et un DSU, ce sont des modems qui vont transformer les signaux.

La bande passante sur un tel système peut aller de 64 kbps à 4 Mbps.

IX-B - Technologies d'accès Wan

Quand un Wan est branché, il faut définir la technologie qui va acheminer les données d'un bout à l'autre du Wan, chacune de ces technologies a un différent but et donne un différent type de transmission de données.

IX-B-1 - PPP (Point to point protocol)

Protocole de connexion d'un ordinateur au réseau TCP/IP via un modem et une ligne téléphonique. C'est un nouveau standard qui a remplacé le protocole SLIP. En clair, cela permet à une personne avec une ligne téléphonique et un modem, de se connecter sur l'Internet.

IX-B-2 - HDLC

Le but de ce protocole est de définir un mécanisme pour délimiter des packets de différents types, en ajoutant un contrôle d'erreur.

IX-B-3 - ISDN (Integrated service digital network)

ISDN est un protocole qui marche sur circuit switching. Il permet au réseau téléphone de transporter des données, de la voix, des graphiques, de la musique, de la vidéo… Une liaison ISDN a plusieurs lignes, des lignes pour les données et des lignes pour la communication téléphonique.

IX-B-4 - DSL (Digital Subscriber Line)

Ce protocole permet d'obtenir des vitesses très bonnes sur des lignes téléphoniques simples. Les technologies ADSL ET HS-DSL sont basées là-dessus. Cela permet aussi de pouvoir faire transiter et de la voix et des données en même temps à différentes fréquences. Le mot d'ordre de cette technologie est d'exploiter l'entier du spectre de fréquences de la ligne téléphonique et non pas se limiter à la petite partie employée par la voix.

IX-B-5 - Frame Relay

Ce protocole multiplexe la ligne. Il permet des vitesses de transfert plus ou moins importantes. Il ne gére pas de contrôle de flux ni d'erreur.

IX-B-6 - ATM

Ce protocole peut être utilisé sur plusieurs médias différents, fibre, cuivre…
Il envoie des paquets de tailles fixes (53 Bytes), appelés cellules. Il peut aller à des vitesses très élevées. Il divise la bande passante, chacun envoie un paquet tour à tour. Il permet l'envoi simultané de plusieurs types de données. Il emploie le multiplexage sur les lignes se basant un peu sur le modèle du frame Relay.

IX-B-7 - SONET

Ce protocole est utilisé pour les transferts de données sur de la fibre optique à très haut débit.

IX-C - Modems

Pour établir une connexion Wan, il faut employer un modem pour convertir les signaux digitaux en signaux analogiques. Le modem est donc une sorte de traducteur.

IX-C-1 - Modem analogique

Un modem analogique est employé pour transférer des données à travers une ligne téléphonique.

IX-C-2 - Modem câble

Un modem câble est employé pour transférer des données à travers le câble de télévision. Comme le modem analogique, il module et démodule le signal pour permettre la transmission. Il permet de bien meilleures bandes passantes qu'avec l'emploi de la transmission par le câble téléphonique.