Les réseaux informatiques

1- Définitions

Un réseau est un outil permettant de partager des informations (vidéo, son etc.), des ressources (imprimante, serveur etc.) et des services (stockage, mise à jour etc.). Les réseaux sont classifiés en fonction de leur taille et de leur structure selon 3 types principaux : les réseaux locaux ou LAN *Local Area Network,* de quelques kilomètres de portée, les réseaux métropolitains ou MAN *Metropolitan Area Network,* de quelques dizaines de kilomètres de portée et les réseaux étendus ou WAN, *Wide Area Network*

2- Classement des réseaux

2.1- Les PAN : (Personal Area Network) : sont des réseaux limités au niveau de l'utilisateur comme les oreillettes et les téléphones portables ou au niveau de son habitation comme les PC, imprimantes.

2.2- Les LAN : ils ne dépassent pas l'étendue d'un bâtiment ou d'une entreprise, le support peut varier sur le réseau : câble a paire torsadée, fibre optique ou Wi-Fi, mais la technologie de transmission est souvent Ethernet.

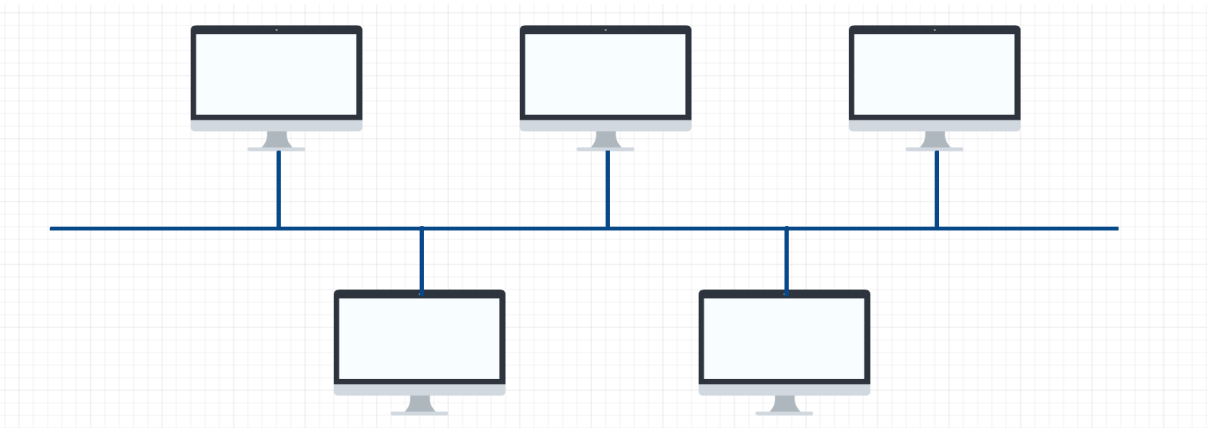
2.3- Les MAN : c'est le cas d'un regroupement d'un petit nombre de réseaux locaux au niveau d'une ville ou une région. Ils peuvent être privés ou loués chez un opérateur.

2.4- Les WAN ou les réseaux étendus : sont des réseaux qui connectent des réseaux en fournissant des liens distants et rapides.

3- Topologies de réseaux

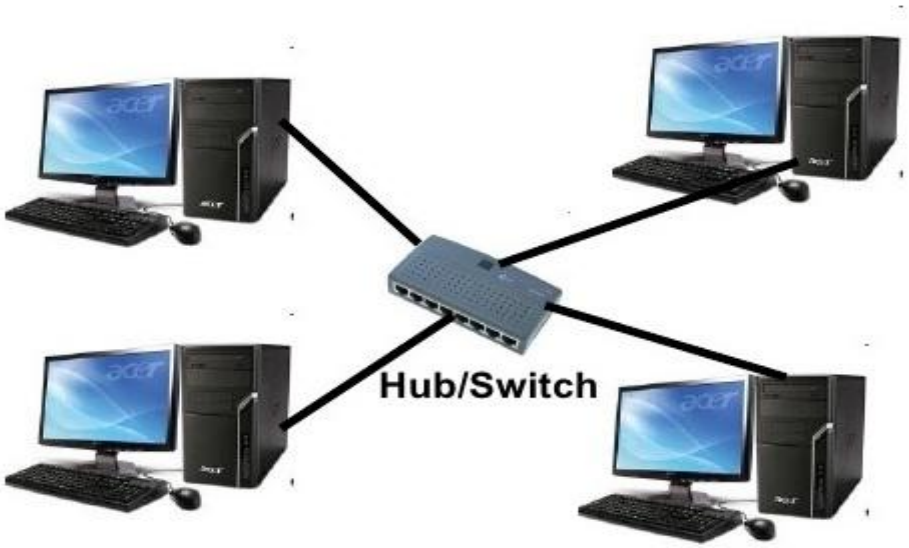
On appelle topologie d'un réseau la façon dont ses éléments sont connectés les uns des autres.

3.1- Topologie en bus



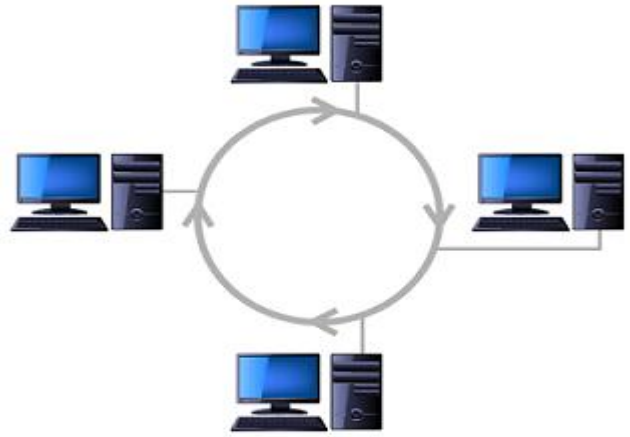
Tous les éléments sont connectés à un même bus et se partagent le support de transmission. Cette topologie a quelques avantage comme l'absence de matériel supplémentaire, la simplicité puisqu'un seul câble permet toutes les communications ou la facilité d'ajouter des postes. Par contre elle présente plusieurs inconvénients comme l'obligation de rajouter des terminaisons aux extrémités du bus pour éviter les phénomènes de réflexion dus à l'écho du signal. Un défaut de liaison à un seul endroit rend tout le réseau inopérant. La bande passante est partagée entre tous les éléments d'où la diminution de début de transmission dès que des postes sont rajoutés.

3.2- Topologie en étoile



Elle est basée sur un équipement central, tel qu'un commutateur, les commutateurs étant des éléments actifs, cette topologie nécessite une alimentation. De plus, le nombre de ports d'un commutateur étant limité, rajouter des éléments est plus difficile. Et enfin, les commutateurs représentent un cout supplémentaire. L'avantage est qu'une liaison en panne n'empêche pas les autres liassions de fonctionner, la bande passante globale dépend du commutateur et non du nombre de postes et qu'on peut augmenter la taille du réseau sans dégrader les performances. La confidentialité est assurée avec des commutateurs, les concentrateurs, eux, relaient les trames sur tous les ports.

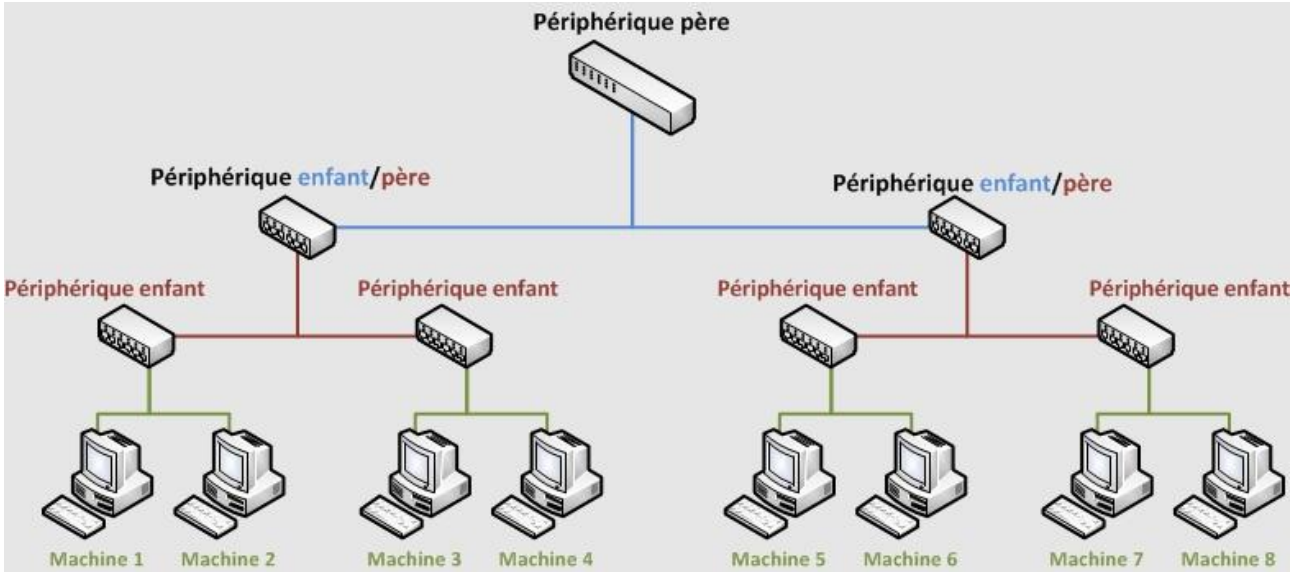
3.3- Topologie en anneau



Cette topologie repose sur une boucle fermée qui relie tous les éléments. Toutes les données transitent par chaque élément qui se comporte comme un répéteur. La plupart des réseaux en anneau utilisent en réalité un concentrateur actif qui joue le rôle de l'anneau appelé *Multistation Access Unit (MAU)*

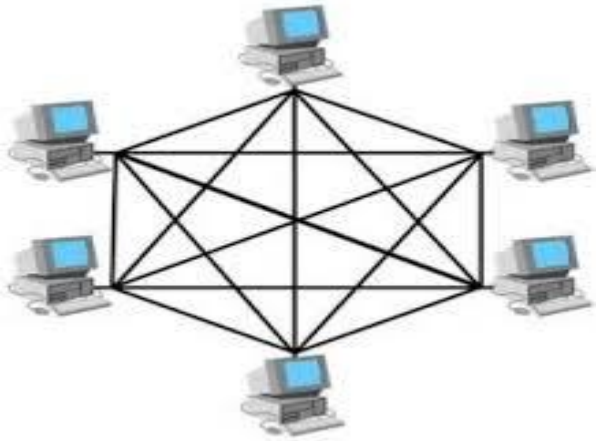
Chaque nœud dispose de sa bande de passante propre. L'augmentation de la taille du réseau ne diminue pas la performance et la circulation des données est unidirectionnelle et s'adapte bien au support fibre optique. Comme inconvénients, il y a le cout de concentrateur de type MAU qui est relativement élevé. Les opérations de maintenance nécessite l'arrêter totalement le réseau. Le débit est fixe contrairement aux réseaux en étoile qui acceptent des débits différents sur chaque port d'un commutateur.

3.4- Topologie en arbre ou hiérarchique



Il s'agit en réalité d'une mise en cascade de réseaux en étoile

3.5- Topologie maillée



Cette topologie est utile pour lutter contre les ruptures de communication. Chaque hôte possède ses propres connexions à tous les autres hôtes. Ceci est le cas de la conception de l'Internet, qui possède de nombreux chemins vers un emplacement.

3.6- Conclusion

En réalité les topologies en anneau et en bus sont moins en moins utilisées au profit des topologies en étoile et en arbre. Dans les réseaux locaux domestiques on trouve en générale des topologies en étoile, alors que dans les grands réseaux d'entreprises on rencontre souvent des topologies en arbre. La topologie maillée est celle utilisée sur l'internet. Il existe de nombreuses topologies réseaux, elles ont toutes des avantages et des inconvénients et convient de trouver le bon équilibre en fonction de plusieurs critères :

Le cout, Le risque accepté, Le niveau de service attendu, La taille de l'infrastructure.

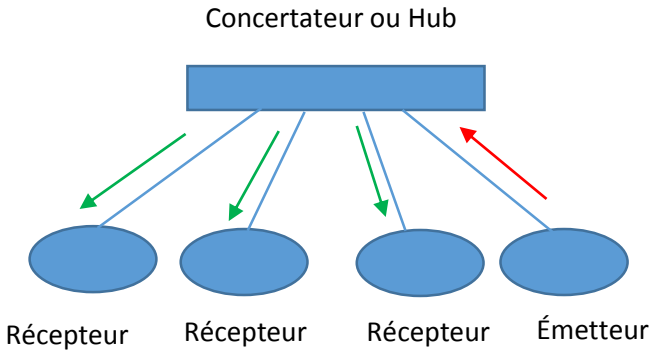
4- Les éléments d'un réseau

La mise en réseau de machines, PC, imprimantes, scanners, caméra, etc. nécessite l'usage d'équipements divers qui agissent chacun a un niveau du modèle OSI pour assurer une bonne communication.

4.1- Le répéteur, niveau 1 ou physique

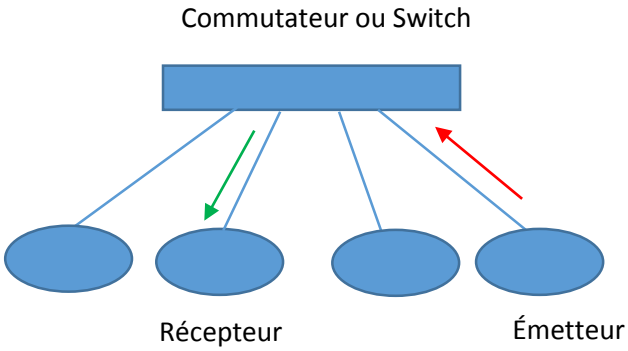
Généralement, la longue distance entre deux appareils affaiblit le signal, pour aller au-delà un équipement est nécessaire c'est le répéteur qui permet de régénérer le signal en l'amplifiant. Il traille uniquement dans la couche physique c'est-à-dire qu'il ne sait pas interpréter les trames de niveau 2 ni les paquets de niveau 3.

4.2- Le concertateur ou Hub, niveau 1 ou physique



C'est un équipement permettant de connecter plusieurs hôtes ensemble pour accéder au réseau. Il dispose pour cela d'un certain nombre de ports 8, 16, ou 32. Le concentrateur ne fait que récupérer les données qui arrivent sur un de ses ports pour les diffuser sur tous les autres ports.

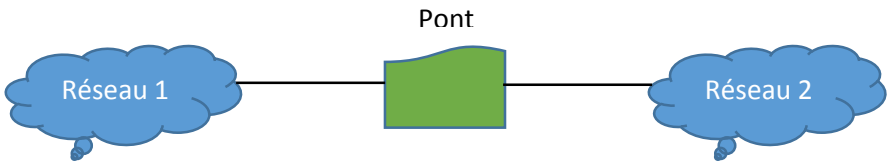
4.3- Le commutateur ou Switch, niveau 2 ou liaison



C'est équipement multiports comme le hub, mais il agit au niveau de la couche 2. Il analyse les trames arrivant sur un port pour les retransmettre seulement aux ports destinataire : c'est la commutation de données ou filtrage. Un switch maintient une table dans laquelle il mémorise les adresses sources détectées sur chaque port. C'est l'apprentissage d'adresse.

Quand il ne trouve pas l'adresse de destination dans sa table il envoie les données sur tous les ses ports. On dit qu'il fait du flooding. Si un port est occupé, la trame est mémorisée en attendant qu'il se libre.

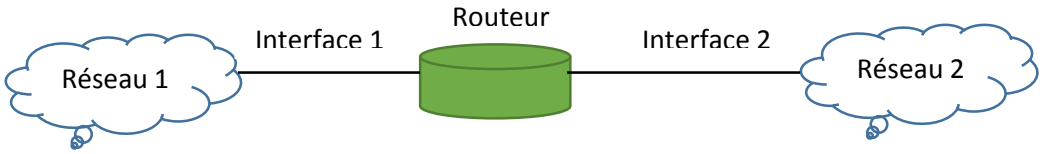
4.4- Le pont ou bridge, niveau 2 ou liaison



C'est un équipement à deux ports qui relie des réseaux travaillant avec le même protocole, même s'ils ont des supports physique différents comme un réseau filaire et un réseau sans fil. Contrairement au répéteur qui travaille uniquement au niveau physique, le pont travaille aussi au niveau liaison. Il est capable de filtrer les trames sur l'un de ses ports et ne laisser

passer sur l'autre port que les trames dont l'adresse correspond à une machine située de l'autre côté du pont. Le rôle principal du pont est segmenter un réseau : une trame arrivant sur un port n'est transmise sur l'autre port que si elle est destinée aux autres réseaux.

4.5- Le routeur ou router, niveau 3 ou réseau



Les routeurs sont des équipements essentiels d'internet, car ce sont eux qui assurent le routage, c'est-à-dire le choix, en fonction de l'adresse IP, du chemin qu'un message va emprunter. Il contient un CPU, de la mémoire et un système d'exploitation. Il agit au niveau de la couche réseau et en plus du routage, il assure l'interconnexion de plusieurs réseaux hétérogènes et la segmentation des grands réseaux. Chaque port représente donc un sous-réseau IP différent ou subnet et forme un domaine de broadcast à part

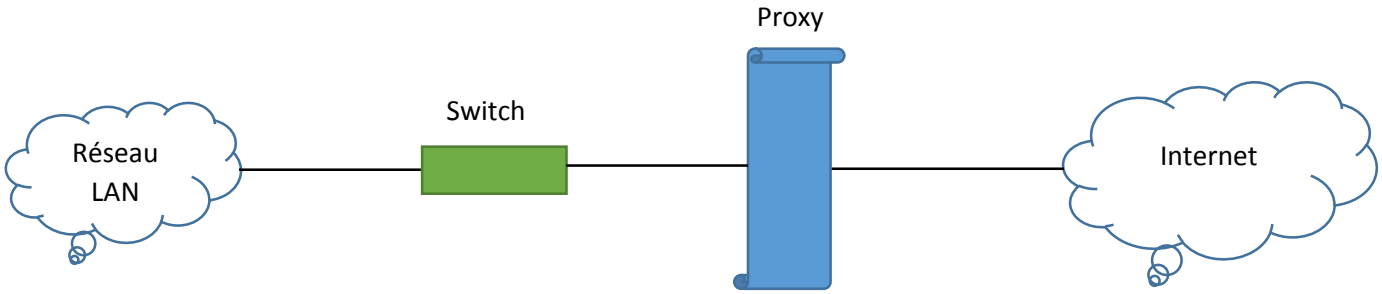
4.6- La passerelle ou Gateway, niveau 7 ou application

La passerelle est un ensemble matériel et logiciel, souvent un PC avec un logiciel spécifique, qui fait l'interface entre des protocoles haut niveau différents.

3.7- L'interface réseau ou NIC, niveau 1 et 2

C'est l'élément de base permettant à un équipement de se connecter à un réseau. Cette interface est souvent appelée NIC, *Network Interface Controller*. Elle peut être intégrée a l'équipement lui-même comme dans une carte mère d'un PC ou exister comme périphérique autonome.

3.8- Le proxy, niveau 7 ou application



Le proxy ou mandataire est un équipement qui se charge d'une tache pour le compte d'un ou plusieurs autres équipements. Il peut assurer par exemple l'accès à internet et mémoriser les pages web pour le compte d'autres postes. L'avantage est de centraliser l'accès au web en un seul point et donc d'en faciliter le contrôle.

5- Le modèle OSI

Introduction

Les ordinateurs d'un réseau n'ont pas à être identiques : les différences de systèmes d'exploitation, de logiciels utilisés pour naviguer sur le net, et les autres différences du genre ne doivent pas avoir le moindre impact sur la communication entre deux machines. Par exemple, on peut parfaitement connecter des ordinateurs sous Windows avec des ordinateurs sous Linux. Pour cela, il a fallu inventer un certain nombre de standards réseau, appelés protocoles réseaux. Des organismes publics supranationaux s'occupent d'établir et de normaliser ces protocoles : ils consultent les grandes entreprises du web (Microsoft, Apple, et ainsi de suite), et les négociations sur ce qui doit être mis dans les protocoles sont souvent longues. Un cours sur le réseau ne peut décemment pas passer sous silence le fonctionnement des protocoles les plus connus. Peut-être en avez-vous déjà entendu parler : les protocoles IP ou TCP sont de loin les plus connus, sans compter les protocoles UDP ou MAC.

UDP (User Datagram Protocol) est un protocole de communication de substitution à Transmission Control Protocol (TCP). Il est surtout utilisé pour établir des connexions à faible latence et à tolérance de perte entre applications sur Internet. UDP et TCP s'exécutent sur le protocole IP (Internet Protocol) et sont donc parfois appelés respectivement UDP/IP et TCP/IP. Les deux protocoles envoient les données par petits paquets, ou datagrammes.

UDP assure deux services non fournis par la couche IP. Il fournit des numéros de port pour distinguer des demandes utilisateur différentes et, en option, une fonctionnalité de contrôle (checksum) pour vérifier que les données sont arrivées intactes.

L'ISO (International Organisation for Standardisation) à développer un modèle de référence OSI (Open System Interconnexion). Ce modèle a pour but d'aider les fournisseurs à créer des réseaux informatiques compatibles entre eux.

Le modèle OSI est constitué d'un ensemble de 7 couches de protocoles. Chaque couche n'agit qu'avec ses voisines immédiates.

Cartes d'identité des couches du modèle OSI

Les couches basses, aussi appelées couches matérielles, s'occupent de tout ce qui a trait au bas-niveau, au matériel. Elles permettent d'envoyer un paquet de données sur un réseau et garantir que celui-ci arrive à destination. Elle est généralement prise en charge par le matériel et le système d'exploitation, mais pas du tout par les logiciels réseaux. Les couches basses sont donc des couches assez bas-niveau, peu abstraites. Les couches basses sont au nombre de trois. Pour résumer, ces trois couches s'occupent respectivement de la liaison point à point (entre deux ordinateurs/équipements réseaux), des réseaux locaux, et des réseaux Internet.

La couche 1 ou couche physique :

Nom : physique.

Rôle : offrir un support de transmission pour la communication.

Rôle secondaire : RAS.

Matériel associé : le hub, ou concentrateur en français.

S’occupe de la transmission physique des bits entre deux équipements réseaux. Elle s'occupe de la transmission des bits, leur encodage, la synchronisation entre deux cartes réseau, etc. Elle définit les standards des câbles réseaux, des fils de cuivre, du WIFI, de la fibre optique, ou de tout autre support électronique de transmission.

Est l’équivalent des camions, des trains et des avions transportant le courrier. En termes de réseau, cette couche n’en traite que les aspects physiques- les cartes, les câbles et les hubs véhiculant les paquets de données. Elle spécifie ce que sont les aspects physiques, ce qu’ils sont capables de réaliser correctement, et comment ils s’y prennent. Cette couche regroupe donc les spécifications des câbles et des connecteurs.

La couche 2 ou couche liaison :

Nom : liaison de données.

Rôle : connecter les machines entre elles sur un réseau local.

Rôle secondaire : détecter les erreurs de transmission.

Matériel associé : le switch, ou commutateur.

S’occupe de la transmission d'un flux de bits entre deux ordinateurs, par l'intermédiaire d'une liaison point à point ou d'un bus. Pour simplifier, elle s'occupe de la gestion du réseau local. Elle prend notamment en charge les protocoles MAC, ARP, et quelques autres.

Elle n’est pas physique au sens strict, contrairement à ce que l’on pourrait croire ? Il s’agit d’un ensemble de règles logicielles gravées dans les circuits mémoire des équipements (concentrateurs, cartes réseau, routeurs, etc.) qui stipulent comment le courrier doit être acheminé et distribué. C’est à cet endroit que sont stockées les règles de fonctionnement d’Ethernet, de Token Ring, de FDDI et d’ATM. Elle s’applique à trouver un chemin pour que la couche 1 puisse dialoguer avec la couche 3. C’est l’endroit où les adresses des cartes réseau (adresses MAC) deviennent importantes. La couche 2 se charge en outre de reconditionner les paquets dans des cadres (frames), qui correspondent au format de transmission des données par les équipements matériels opérant aux niveaux inférieurs à la couche 3.

La couche 3 ou couche réseau :

Nom : réseau.

Rôle : interconnecter les réseaux entre eux.

Rôle secondaire : fragmenter les paquets.

Matériel associé : le routeur.

S’occupe de tout ce qui a trait à internet : l'identification des différents réseaux à interconnecter, la spécification des transferts de données entre réseaux, leur synchronisation, etc. C'est notamment cette couche qui s'occupe du routage, à savoir la découverte d'un chemin de transmission entre récepteur et émetteur, chemin qui passe par une série de machines ou de routeurs qui transmettent l'information de proche en proche. Le protocole principal de cette couche est le protocole IP.

Les couches hautes, aussi appelées couches logicielles, contiennent des protocoles pour simplifier la programmation logicielle. Elles requièrent généralement que deux programmes communiquent entre eux sur le réseau. Elles sont implémentées par des bibliothèques logicielles ou directement dans divers logiciels. Le système d'exploitation ne doit pas, en général, implémenter les protocoles des couches hautes. Elles sont au nombre de quatre :

La couche 4 ou couche transport :

Nom : transport.

Rôle : gérer les connexions applicatives.

Rôle secondaire : garantir la connexion.

Matériel associé : RAS.

Permet de gérer la communication entre deux programmes, deux processus. Les deux protocoles de cette couche sont les protocoles TCP et UDP.

Elle s'assure que le courrier est bien remis à son destinataire. Si un paquet n'atteint pas sa destination, elle gère le processus consistant à prévenir l'expéditeur et à solliciter l'émission d'un autre exemplaire. En fait, elle s'assure que les trois couches situées au-dessous d'elle (c'est-à-dire les couches 1.2.3) font leur travail correctement. A défaut, le logiciel de la couche 4 peut intervenir et gérer la correction des erreurs en renvoyant les paquets altérés ou manquants (les paquets altérés sont écartés, dropped). C'est à ce niveau qu'opère la partie TCP (Transmission Control Protocol) de TCP/IP.

La couche 5 ou couche session : on s'en fiche !

Gère les connexions courantes entre systèmes. Elle tient compte de l'ordre des paquets de données et des communications bidirectionnelles. Dans la métaphore postale, elle aurait pour équivalent la division d'un gros document en parties plus petites, leur mise sous plis et leur affranchissement dans l'ordre où les enveloppes devront être ouvertes pour reconstituer l'ensemble. C'est à cet endroit que les flux de données sont transformés en paquets.

La couche 6 (présentation)

Concerne la façon dont les systèmes différents représentent les données. Par exemple, elle définit ce qui se passe lorsqu'on essaie d'afficher des données provenant d'Unix sur un écran MS-DOS.

Cette couche n'a pas d'équivalent réel dans le monde postal mais, si elle devait en avoir un, ce serait la réécriture de a lettre de façon que tout le monde puisse la lire. La meilleure analogie est sans doute celle d'un traducteur : supposez que votre lettre doive être envoyée à Mexico ; un traducteur (l'équivalent d'un logiciel de couche de présentation) peut convertir les données contenues dans votre enveloppe en espagnol. Comme la lettre de cet exemple, les données sont changeantes et peuvent être réorganisées pour se conformer au type d'ordinateur sur lequel elles sont utilisées.

La couche 7 ou couche application :

Nom : application.

Rôle : RAS.

Rôle secondaire : RAS.

Matériel associé : le proxy.

Concerne les applications, comme l'accès aux fichiers et le transfert de fichiers. Si vous avez déjà utilisé des applications telles que FTP ou Telnet, vous avez travaillé avec un exemple de couche 7. Dans le modèle postal, cette couche peut s'assimiler à l'écriture de la lettre. C'est à ce niveau qu'opèrent les applications (traitement de texte, tableur, etc.).

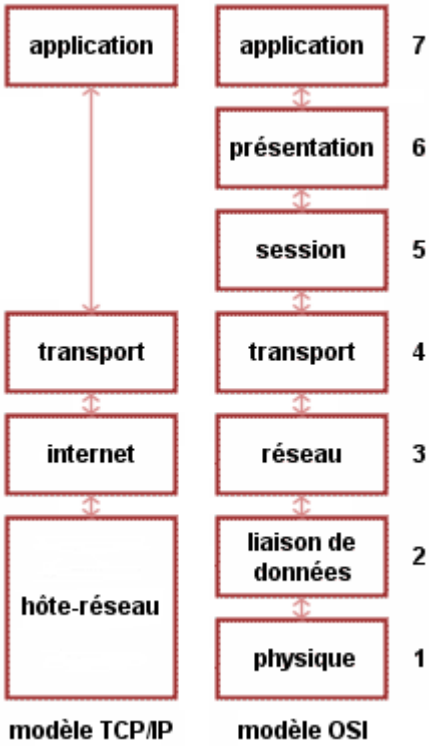
6- MODÈLE TCP/IP

TCP/IP désigne communément une architecture réseau, mais cet acronyme désigne en fait 2 protocoles étroitement liés : un protocole de transport, TCP (Transmission Control Protocol) qu'on utilise « par-dessus » un protocole réseau, IP (Internet Protocol). Ce qu'on entend par « modèle TCPIP », c'est en fait une architecture réseau en 4 couches dans laquelle les protocoles TCP et IP jouent un rôle prédominant, car ils en constituent l'implémentation la plus courante. Par abus de langage, TCP/IP peut donc désigner deux choses : le modèle TCP/IP et la suite de deux protocoles TCP et IP.

Le modèle TCP/IP, comme nous le verrons plus bas, s'est progressivement imposé comme modèle de référence en lieu et place du modèle OSI. Cela tient tout simplement à son histoire. En effet, contrairement au modèle OSI, le modèle TCP/IP est né d'une implémentation ; la normalisation est venue ensuite. Cet historique fait toute la particularité de ce modèle, ses avantages et ses inconvénients.

L'origine du modèle TCPIP remonte au réseau ARPANET. ARPANET est un réseau de télécommunication conçu par l'ARPA (Advanced Research Projects Agency), l'agence de recherche du ministère américain de la défense (le DOD : Department of Defense). Outre la possibilité de connecter des réseaux hétérogènes, ce réseau devait résister à une éventuelle guerre nucléaire, contrairement au réseau téléphonique habituellement utilisé pour les télécommunications mais considéré trop vulnérable. Il a alors été convenu qu'ARPANET utiliserait la technologie de commutation par paquet (mode datagramme), une technologie émergeante promettante. C'est donc dans cet objectif et ce choix technique que les protocoles TCP et IP furent inventés en 1974. L'ARPA signa alors plusieurs contrats avec les constructeurs (BBN principalement) et l'université de Berkeley qui développait un Unix pour imposer ce standard, ce qui fut fait.

6.1 Description des couches



6.1.1 La couche d'accès réseau

Elle est dotée des protocoles pour transmettre et livrer des trames de données ainsi que ceux nécessaires pour déterminer comment sont passées les trames au réseau physique même. Cette couche s'appuie sur les adresses physiques des cartes réseau (adresses

MAC). Cette couche répond à la question : Comment transmettre des paquets de données

La couche hôte-réseau, intégrant les services des couches physique et liaison du modèle OSI, a en charge la communication avec l'interface physique afin de transmettre ou de récupérer les paquets de données qui lui sont transmis de la couche supérieure. Le protocole utilisé pour assurer cet interfaçage n'est pas explicitement définit puisqu'il dépend du réseau utilisé ainsi que du nœud (Ethernet en LAN, X25 en WAN).

Cette couche répond à la question : Comment transmettre des paquets de données ?

6.1.2 La couche Internet

Elle a un rôle similaire à la couche réseau du modèle OSI, elle s'appuie sur un protocole Universel : le protocole IP. Cette couche réalise l'interconnexion des réseaux (hétérogènes) distants sans connexion. Son rôle est de permettre l'injection de paquets dans n'importe quel réseau et l'acheminement de ces paquets indépendamment les uns des autres jusqu'à destination. Comme aucune connexion n'est établie au préalable, les paquets peuvent arriver dans le désordre ; le contrôle de l'ordre de remise est éventuellement la tâche des couches supérieures. Du fait du rôle imminent de cette couche dans l'acheminement des paquets, le point critique de cette couche est le routage.

La couche internet possède une implémentation officielle : le protocole IP (Internet Protocol). Remarquons que le nom de la couche (« internet ») est écrit avec un i minuscule, pour la simple et bonne raison que le mot internet est pris ici au sens large (littéralement, « interconnexion de réseaux »), même si l'Internet (avec un grand I) utilise cette couche.

Les trames crées par cette couche portent le nom de trames IP, elles sont entièrement indépendantes de l'environnement matériel.

Cette couche répond à la question : Comment acheminer les trames sur le réseau ?

6.1.3 La couche Transport

Cette couche doit garantir la fiabilité de la livraison des données de bout en bout. Elle doit aider les ordinateurs en communication à établir une connexion. Elle fournit aux ordinateurs un chemin défini, sur lequel vont transiter les données.

Officiellement, cette couche n'a que deux implémentations : le protocole TCP (Transmission Control Protocol) et le protocole UDP (User Datagram Protocol). TCP est un protocole fiable, orienté connexion, qui permet l'acheminement sans erreur de paquets issus d'une machine d'un internet à une autre machine du même internet. Son rôle est de fragmenter le message à transmettre de manière à pouvoir le faire passer sur la couche internet. A l'inverse, sur la machine destination, TCP replace dans l'ordre les fragments transmis sur la couche internet pour reconstruire le message initial. TCP s'occupe également du contrôle de flux de la connexion.

Le rôle de protocole UDP est de permettre la transmission de données (sous forme de datagrammes) de manière très simple entre deux entités, chacune étant définie par une adresse IP et un numéro de port. Aucune communication préalable n'est requise pour établir la connexion, au contraire de TCP (qui utilise le procédé de handshaking). UDP utilise un mode de transmission sans connexion.

Cette couche répond à la question : Comment envoyer un message à un destinataire ?

6.1.4 La couche Application

Cette couche est assimilable aux couches application et présentation du modèle OSI.

Elle renferme les nombreux protocoles fournissant aux applications les accès au réseau et à ses services. Un grand nombre de protocoles divers de haut niveau permettent d'assurer les services de cette couche :

- Telnet : ouverture de session à distance ;
- FTP (File Transfer Protocol) : protocole de transfert de fichier
- HTTP (HyperText Transfer Protocol) : protocole de transfert de l'hypertexte
- SMTP (Simple Mail Transfer Protocol) : protocole simple de transfert de courrier
- DNS (Domain Name system) : system de nom de domaine

Cette couche répond à la question : Comment constituer des applications réseaux ?

Le modèle TCP/IP correspond donc à une suite de protocoles de différents niveaux participant à la réalisation d'une communication via un réseau informatique. Beaucoup de ces protocoles sont régulièrement utilisés pas tous du fait de l'essor d'internet

7- L’adressage IP et routage

7.1 L’adresse IP

Sur Internet, les ordinateurs et les équipements réseaux communiquent entre eux grâce au protocole IP, Internet Protocol, qui utilise des adresses numériques, appelées adresses IP et constituées d’une suite de 32 bits. On divise souvent une adresse IP en 4 de manière à former 4 octets et on la note alors sous la forme de quatre nombres décimaux séparer par des points

xxx.xxx.xxx.xxx

Chaque notation appelée notation décimale pointée. 194.153.205.26, par exemple, est une adresse IP. Chaque interface réseau possède une adresse IP unique sur son réseau. L’ICANN, Internet Corporation for Assigned Names and Numbres, remplaçant l’IANA, Internet Assigned Numbres Agency, depuis 1998, est chargée d’attribuer les adresses IP publiques, celles des machines directement connectées sur le réseau public internet.

L’ICANN définit les procédures d’attribution et de résolution de conflits d’adresse et délègue la gestion de ces ressources a des instances régionales puis locales dans chaque région appelées RIR ou Régional Internet Registres. Il existe cinq RIR : APNIC pour la région Asie pacifique, ARIN pour l’Amérique, AFRINIC pour l’Afrique, LACNIC pour l’Amérique Latine et RIPE NCC pour l’Europe, Réseaux IP Européen Network Coordination Centre. Les adresses IP sont allouées à l’utilisateur final par un LIR, local Internet Registry, qui souvent est le fournisseur d’accès internet, FAI.

7.1.1 Identifiant réseau et identifiant hôte

Dans la suite des 32 bits qui forment un adresse IP, on distingue une partie à gauche pour désigner le réseau, appelée ID de réseau ou netID qu’on note Idr et une partie à droite pour désigner l’ordinateur lui-même ou hôte dans ce réseau et appelée ID d’hote ou hostID qu’on note Idh.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Idr **Idh**

Dans l’adresse 150.123.10.1, par exemple, l’Idr comprend les 16 premiers bits, soit les 2 premiers octets : 150.123. et l’Idh les bits restent, soit les 2 derniers octets : 10.1.

7.1.2 Adresse réseau

Lorsque, dans une adresse IP, tous les bits de l’identifiant hôte contiennent des zéros on obtient ce que l’on appelle l’adresse réseau. Cette adresse sert par exemple aux routeurs pour trouver le chemin vers un réseau sans avoir besoin de connaitre une machine particulière. Cette adresse ne peut donc être attribuée a aucune des machines du réseau. Dans l’exemple ci-dessus de l’adresse IP 150.123.10.1, l’adresse réseau est 150.123.0.0.

7.1.3 Adresse hôte

Lorsque, dans une adresse IP, tous les bits de l’identifiant réseau sont des zéros, on obtient l’adresse hôte ou machine par défaut. Cette adresse identifie une machine sur la réception seau courant. Elle est utilisée quand on ne connait pas l’adresse réseau. Dans l’exemple ci-dessus, l’adresse machine sur le réseau courant est 0.0.10.1.

7.1.4 Adresse de diffusion ou de broadcast

Lorsque, dans une adresse IP, tous les bits de l'identifiant hôte sont à 1, l'adresse obtenue est appelée adresse de diffusion ou de broadcast. C'est une adresse spécifique, permettant d'envoyer un message à toutes les machines du même réseau. Dans l'exemple ci-dessus, l'adresse de broadcast de 150.123.10.1 est 150.123.255.255. Tout comme l'adresse réseau, cette adresse ne peut être attribuée à aucune machines du réseau.

7.1.5 Masque de réseau

En informatique on crée un masque d'un mot binaire en mettant des 1 en face des bits que l'on désire conserver, et des 0 en face des autres. Ensuite, il suffit de faire un ET logique entre le mot binaire et le masque afin de garder la partie souhaitée et annuler le reste. Si par exemple, dans le mot binaire 10110010, on veut garder le 4 premier bits (les plus gauches), on utilise alors le masque suivant 11110000 et on fait un ET logique. Les 4 premiers bits du résultat sont les même que ceux du mot binaire et les autres sont devenue des 0. Ils ont été masques.

1 0 1 1 0 0 1 0
&
1 1 1 1 0 0 0 0
= 1 0 1 1 0 0 0 0

Ainsi, un masque de réseau ou netmask, est une suite de 32 bits, comme une adresse IP, qui comprend des zéro au niveau des bits de l'Idh est des 1 au niveau des ceux de l'Idr. Le masque de réseau pour l'adresse 150.123.10.1 par exemple 255.255.0.0.

L'intérêt principal d'un masque de réseau est de permettre d'identifier simplement le réseau associé à une adresse IP. A retenir : le masque ne sert pas à déterminer la classe.

Pour connaitre, par exemple, l'adresse réseau de l'adresse IP 34.56.123.12, connaissant son masque 255.0.0.0, il suffit de faire un ET logique entre l'adresse IP et le masque.

0 0 1 0 0 0 1 0 . 1 1 0 1 0 0 0 0 . 0 1 1 1 1 0 1 1 . 0 0 0 0 1 1 0 0 adresse IP en binaire
&
1 1 1 1 1 1 1 1 . 0 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0 masque en binaire
=
0 0 1 0 0 0 1 0 . 0 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0 adresse réseau en binaire

L'adresse du réseau est donc 34.0.0.0

7.2 Les classes de réseaux

Les adresses IP étaient à l'origine, réparties en classes, selon le nombre d'octets qui représentent l'identifiant réseau et l'identifiant hôte et la valeur des premiers bits de l'adresse.

7.2.1 Classe A

Une adresse IP est de classe A si son bit de poids fort est 0, en classe A, le premier octet représentent l'identifiant réseau, le masque de réseau de la classe A est donc 255.0.0.0. Il y a 2^7 =128 réseaux possibles. Toutefois, la valeur 0 est réservée pour les réseaux par défaut et 127 est réservée pour désigner la machine locale. Les réseaux disponibles en classe A sont donc les réseaux allant de 1.0.0.0 à 126.0.0.0. Les trois octets de droite représentent l'identifiant hôte. Le réseau peut donc contenir un nombre de machines égale à 2^{24}-2=16777214 machines. On enlève 2 pour les adresses ou tous les bits de l'Idh sont tous à 0 ou tous 1 qui correspondent

respectivement à l'adresse réseau et à celle de broadcast. Une adresse IP de classe A, a le format suivant :

0xxxxxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx
Réseau	**Hôtes**		

7.2.2 Classe B

Une adresse IP est de classe B si ses deux bits de poids fort sont 10. En classe B, les deux premiers octets représentent l'identifiant réseaux, le masque de réseau de la classe B est donc 255.255.0.0. Il y a 2^{14}=16384 réseaux possibles. 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 machines du réseau. Le réseau peut donc contenir un nombre de machines égale à 2^{16}-2= 65 534 machines. Une adresse IP de classe B a le format suivant :

10xxxxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx
Réseau		**Hôtes**	

7.2.3 Classe C

Une adresse IP est de classe C si ses trois bits de poids fort sont 110. En classe C, les trois premiers octets représentent le réseau, le masque de réseau de la classe B est donc 255.255.255.0. Il y a 2^{21}=2 097 152 réseaux possibles. 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 représentent les machines du réseau, qui peut donc contenir 2^{8}-2=254 machines. Une adresse IP de classe C a le format suivant :

110xxxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx
Réseau			**Hôtes**

7.2.4 Classe D et E

Les premiers bits de la classe D sont 1110 et ceux de la classe E sont 1111. Les classes D et E ont une utilisation particulière. La classe D est utilisée pour le multicast, c'est-à-dire l'émission vers un groupe donné de machines. Par exemple, 224.0.0.2 est une adresse de classe D qui sert à émettre vers tous les routeurs du réseau courant. La classe E est réservée pour une utilisation future. Elles n'ont pas de masque ni de division en identifiant réseau et identifiant hôte. Une adresse IP de classe D ou E a le format suivant :

D	1110xxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx
E	1111xxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx

7.3 Résumé

Les réseaux de la classe A sont moins nombreux mais contiennent beaucoup de machines. Ils sont utilisés par les grandes entreprises et les organismes étatiques. Les réseaux de classe C sont les plus nombreux et contiennent peu de machines. Ils sont utilisés par les petites entités. La classe B est utilisé par les entreprises moyennes.

Classe	Format d'adresse	Masque par défaut	Nombre de réseaux	1er réseaux	Dernier réseau	Nombre de machines
A	0xxxxxx…	255.0.0.0	126	1.0.0.0	126.0.0.0	16777214
B	10xxxxx…	255.255.0.0	16384	128.0.0.0	191.255.0.0	65534
C	110xxx…	255.255.255.0	2097152	192.0.0.0	223.255.225.0	254
D	1110xxx…	Utilisée en multicast : émission multi destinataires, dans les routeurs, etc.				
E	1111xxx…	Réservée pour un usage futur				

Les classes D et E n'ont pas de masque et forment chacune un seul réseau dont les adresse limites sont :

Classe	1er adresse hôte	Dernière adresse hôte
D	224.0.0.1	239.255.255.254
E	240.0.0.1	255.255.255.254

La division de l'adresse IP en trois classes A, B, et C facilite la recherche d'un ordinateur sur le réseau, lors du routage par exemple. En effet, avec cette notation il est possible de rechercher d'abord le réseau à atteindre puis de rechercher une machine sur celui-ci. Les masques des classes A, B, et C sont appelés des masques par défaut.

7.4 Adresse IP Privées

Il arrive souvent dans une entreprise ou une organisation qu'un seul ordinateur appelé proxy ou passerelle soit relié à internet et sert de lien pour tous les autres ordinateur du réseau. Dans ce cas, seul cet ordinateur relié à internet a besoin de réserver une adresse IP auprès de l'ICANN. Toutefois, les autres ordinateurs ont besoin d'une adresse IP pour pouvoir communiquer entre eux en interne. Ainsi, l'ICANN a réservé une plage d'adresses dans chaque classe pour permettre d'affecter une IP aux machines d'un réseau local relié à internet sans risquer de créer des conflits d'adresses IP sur ce réseau et sans avoir besoin d'autorisation préalable. Les adresses IP privées de classe A vont de 10.0.0.1 à 10.255.255.254, ce qui correspond à une classe A. Les adresses IP privées de classe B vont de 172.16.0.1 à 172.31.255.254, ce qui correspond à 16 classe B qui suivent 172.16.0.0 à 172.31.0.0. Les adresses IP privées de classe C vont de 192.168.0.1 à 192.168.255.254, ce qui correspond à 256 classes de C qui suivent 192.168.0.0 à 192.168.255.0.

Les adresses privées ne sont pas routées au niveau de réseau internet. Un paquet à destination d'une telle adresse serait tout simplement rejeté. Ces adresses sont tout de même routées localement.

7.5 Adresse IP réservées

Certaines adresses sont réservées à des usages particuliers ne peuvent pas être affectées à un hôte.

a- L'adresse réseau désigne le réseau, par exemple 192.168.10.0.
b- L'adresse de broadcast sert pour la diffusion sur le réseau, par exemple 192.168.10.225.
c- L'adresse 0.0.0.0 est utilisée comme adresse par défaut par les équipements réseaux.
d- L'adresse 255.255.255.255 est utilisée pour des diffusions par exemple par le DHCP.
e- L'adresse 127.0.0.1, appelée adresse de rebouclage ou loopback, désigne la machine locale ou localhost. Toute adresse de la forme 127.x.x.x est considérée comme adresse de rebouclage.
f- Les adresses 169.254.0.0 à 169.254.255.255 forment une plage utilisée par les machines qui ne trouve pas un serveur DHCP.

7.6 Le routage

7.6.1 Routeur

Les routeurs sont les dispositifs permettant de choisir le chemin emprunté par les datagrammes pour arriver à destination. Ce sont des machines ayant plusieurs interfaces réseau, reliée chacune a un réseau différent. Ces interfaces sont aussi appelées ports.

7.6.2 Routage

Le routage est l'action d'acheminer un paquet à travers les routeurs du réseau. Pour chaque paquet arrivant sur un port d'entrée ou interface, les routeurs choisissent de manière déterministe et optimisée une interface de sortie. Le routage est une opération de la couche réseau du modèle OSI. Pour trouver le chemin, les routeurs utilisent des algorithmes et des tables de routage enregistrées dans leur mémoire interne et contenant les informations nécessaires au routage ou aux algorithmes. Le routage est dit direct si la destination est sur le routeur et indirect si la destination se trouve sur un autre routeur. Il est dit statique ou non adaptif si la table de routage est construite préalablement et est introduite manuellement dans les routeurs par l'administrateur. Ceci est valable pour les petits réseaux, mais devient assez lourd

pour les grands. Le routage est dit dynamique ou adaptif si la table est construite et est mise à jour automatiquement par le routeur.

7.6.3 Table de routage

Le routeur extrait l'adresse IP de destination de chaque paquet IP qu'il reçoit et il utilise la table de routage pour trouver le chemin du paquet vers cette destination. La table de routage peut contenir plus ou moins de colonnes en fonction de l'algorithme de routage.

Adresse du réseau de destination	masque du réseau de destination	Adresse de la passerelle	Interface à emprunter	métrique
192.168.1.0 …	255.255.255.0 …	192.168.10.254 …	192.168.10.1 …	1 …

- Adresse du réseau de destination : cette colonne comporte les adresses des réseaux accessibles à partir de ce routeur.
- Masque : c'est le masque à appliquer à l'adresse de destination pour déterminer à quel réseau destination de la colonne précédente appartient-elle.
- Passerelle : elle peut être celle d'une interface du routeur lui-même si le routage est direct ou celle du prochain routeur à emprunter par le paquet.
- Interface : c'est l'adresse IP du port du routeur que doit emprunter le paquet pour être acheminer vers la passerelle.
- Métrique : la métrique est le paramètre qualifiant l'accessibilité d'une destination. Son calcul prend en compte des paramètres tels que les suivantes :
    a- Le nombre sauts : c'est le nombre de routeurs par lesquels un paquet doit passer avant d'arriver à destination.
    b- Le débit de la liaison : une liaison Ethernet de 100Mbps est par exemple préférable à une ligne à 10Mbps
    c- La fiabilité : mesure du taux d'erreurs de chaque liaison de réseau.
    d- La charge : c'est la quantité de trafic sur un équipement tel qu'un routeur.

7.6.4 Construire de table de routage

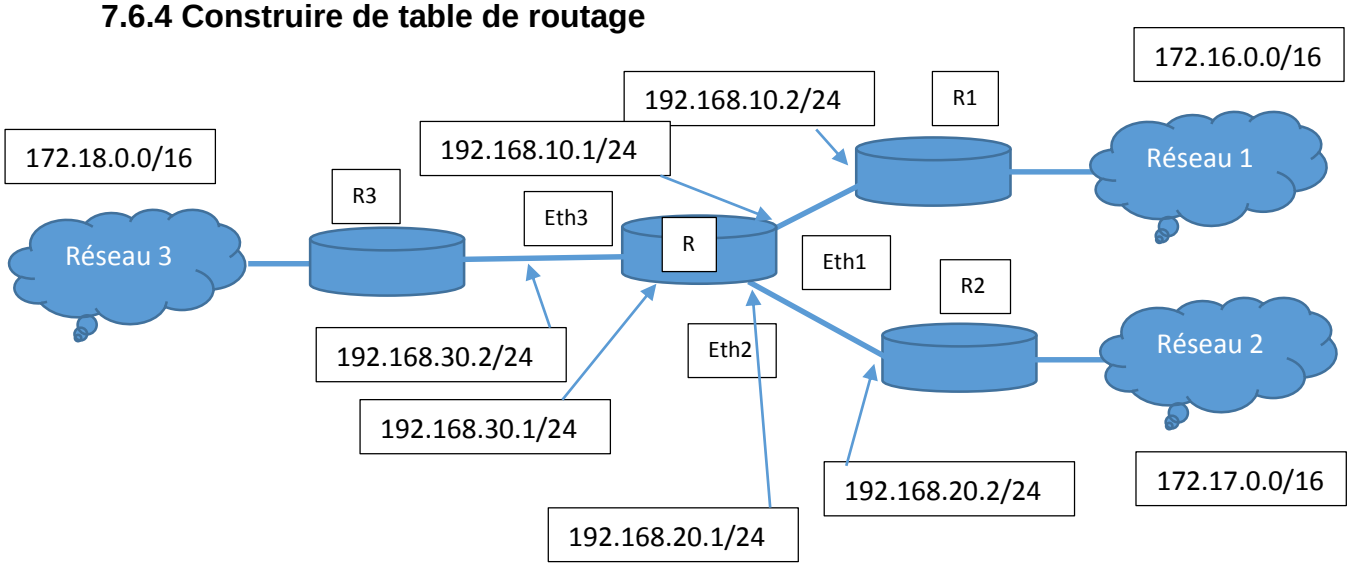


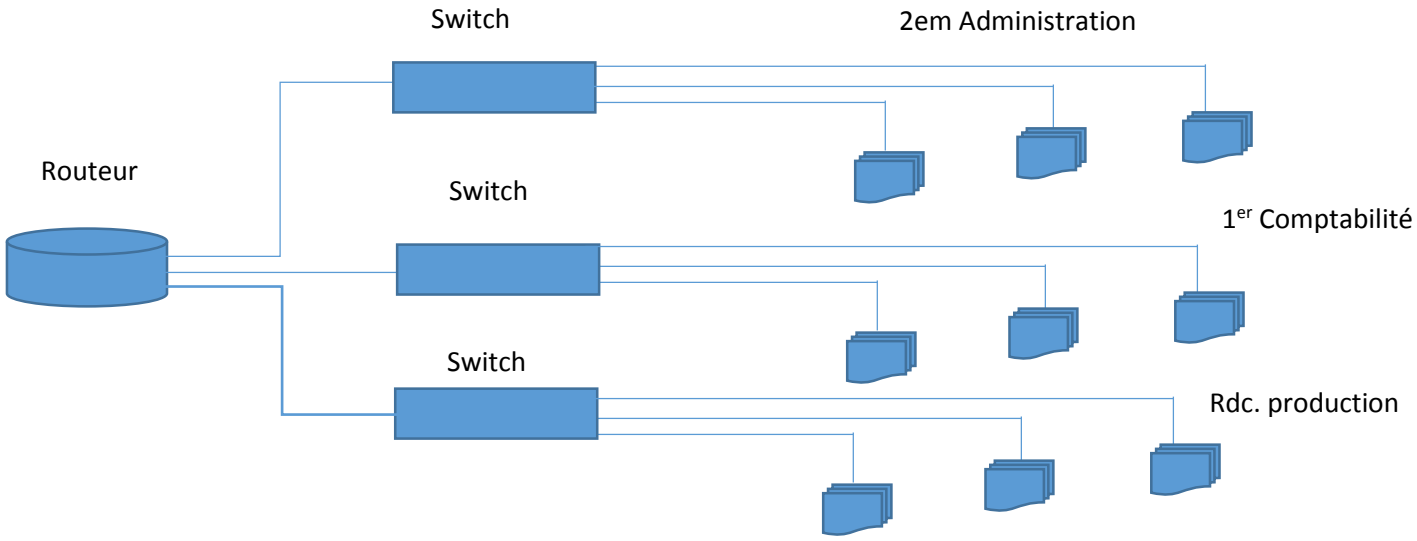
Table de routage du routeur R

Réseau de destination	masque	interface	passerelle
172.16.0.0	255.255.0.0	Eth1	192.168.10.2
172.17.0.0	255.255.0.0	Eth2	192.168.20.2
172.18.0.0	255.255.0.0	Eth3	192.168.30.2

1- Tout paquet à destination du réseau 172.16.0.0, reconnu grâce au masque 255.255.0.0, sera envoyé vers la passerelle 192.168.10.2, via l'interface eth1.
2- Tout paquet à destination du réseau 172.17.0.0, reconnu grâce au masque 255.255.0.0, sera envoyé vers la passerelle 192.168.20.2, via l'interface eth2.
3- Tout paquet à destination du réseau 172.18.0.0, reconnu grâce au masque 255.255.0.0, sera envoyé vers la passerelle 192.168.30.2, via l'interface eth3.

8 Les réseaux locaux virtuels

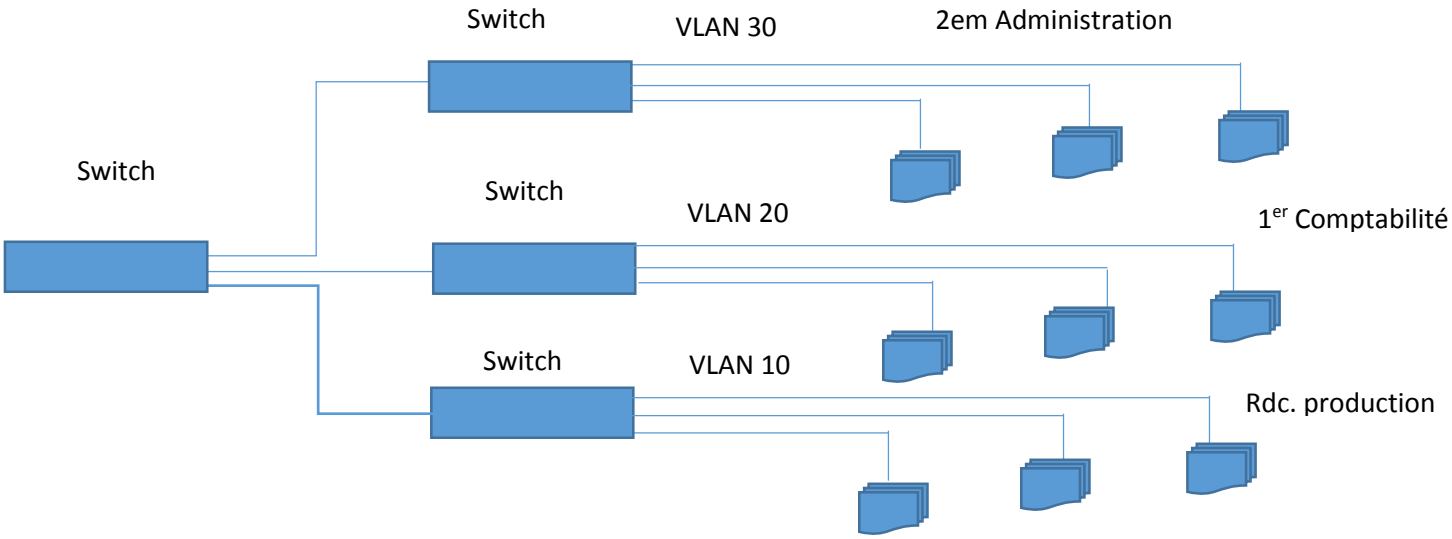
Pour assurer de meilleurs performances et une meilleure confidentialité un réseau doit être segmenté. Avant les vlan, segmenter un réseau obligeait souvent d'utiliser un routeur.



Ceci comporte des inconvénients. On peut citer le surcout du au prix du routeur mais aussi le manque de souplesse au niveau des switches. En effet on ne peut ajouter un poste à un étage s'il manque des ports sur les switches concernés et ceci même si les switches des autres étages ont des ports libres. La création d'un nouveau sous-réseau pour un nouveau service par exemple, nécessite un port libre sur le routeur. La délocalisation d'un membre d'un service dans une autre zone service, par manque de bureaux par exemple, pose un problème de câblage, car il doit rester connecté au même port du routeur afin de rester dans le même sous-réseau.

8.1 La solution VLAN

Le concept de vlan permet de réaliser des réseaux de façon indépendante du système de câblage. Ces réseaux définissent des domaines de diffusion restreints. Cela signifie qu'un message émis par une station d'un vlan ne pourra être reçu que par les stations de ce même vlan. Un vlan est donc un regroupement logique, et non physique, de plusieurs stations. Pour réaliser ce regroupement, on intervient directement, par voie logicielle, sur les commutateurs pour configurer les ports dans vlan donné.



8.2 Les avantages d'un vlan

Le vlan rend l'appartenance à un groupe, indépendante de sa position géographique. Un utilisateur d'un étage, par exemple, peut déménager à un autre étage en restant rattaché à son réseau et sans modification du câblage. Le vlan optimise aussi la bande passante, en réalisant des réseaux disjoints, donc en réduisant les domaines de collision et de diffusion. Il simplifie l'administration en utilisant des commandes centralisées pour gérer un réseau plutôt que des inconvénients dans les armoires de brassage. Il améliore la sécurité, en créant des règles de filtrage du trafic échangé entre les vlan.

8.3 Les différents types de VLAN

Pour réaliser des vlan, il faut utiliser des commutateurs administrables qui supportent le VLAN et qui permettent l'affectation des ports a un VLAN depuis une console centrale. Il existe plusieurs types de VLAN qui peuvent être associés à une couche du modèle OSI. On distingue le VLAN de niveau 1, associé à la couche physique, le VLAN de niveau 2, associé à la couche liaison, et le VLAN de niveau 3, associé à la couche réseau.

8.3.1 VLAN de niveau 1 ou VLAN par port

Ce VLAN correspond à une configuration physique du réseau. Il s'agit d'associer chaque port du switch à un VLAN. C'est donc le port qui détermine le VLAN auquel appartiennent les stations associées. En plus de la table de correspondance port/adresse MAC le commutateur maintient une correspondance Port/VLAN.

port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
VLAN	20	20	20	20	1	10	30	10	1	30	10	10	10	30	30	30

Table port/VLAN du switch

8.3.2 VLAN de niveau 2

Dans ce type de VLAN, c'est l'adresse MAC de la carte réseau de la station, qui détermine le VLAN de la station quel que soit le port utilisé. Ainsi, on peut avoir des stations sur un même port du switch et appartenant à des VLAN différents. C'est au moment où la station envoie un message que le switch saura que le port 8 est en VLAN 30.

Le VLAN de niveau 2 consiste en fait l'affectation dynamique des ports du switch à chacun des VLAN en fonction de l'adresse MAC de l'hôte qui émet sur ce port et de l'association MAC/VLAN.

8.3.3 VLAN de niveau 3

C'est l'adresse IP qui détermine le VLAN de la station, en associant un vlan à une plage d'adresse IP. Il n'y a donc plus besoin de configuration matérielle de ports ou d'adresses MAC. Des stations sur un même port de switch peuvent appartenir à des VLAN différents. Il est aussi possible de définir des VLAN par type de protocole de niveau 3. Le VLAN de niveau 3 agit en fait par l'affectation dynamique des ports des switches aux VLAN à partir de l'association adresse IP/VLAN.