Chapitre 2. Réseaux et Communication

1. Qu'est-ce qu'un réseau ?

Le terme générique « **réseau** » définit un ensemble d'entités (objets, personnes, etc.) interconnectées les unes avec les autres. Un réseau permet ainsi de faire circuler des éléments matériels ou immatériels entre chacune de ces entités selon des règles bien définies.

Selon le type d'entité concernée, le terme utilisé sera ainsi différent :

- **réseau de transport**: ensemble d'infrastructures et de dispositions permettant de transporter des personnes et des biens entre plusieurs zones géographiques.
- **réseau téléphonique**: infrastructure permettant de faire circuler la voix entre plusieurs postes téléphoniques.
- **réseau informatique**: ensemble d'ordinateurs et de périphériques reliés entre eux grâce à des lignes physiques et échangeant des informations sous forme de données numériques (formées de 0 et de 1).

Le présent chapitre s'intéresse bien évidemment aux réseaux informatiques.
Il n'existe pas un seul type de réseau, car historiquement il existe des types d'ordinateurs différents, communiquant selon des langages divers et variés. Par ailleurs ceci est également dû à l'hétérogénéité des supports physiques de transmission les reliant, que ce soit au niveau du transfert de données (circulation de données sous forme d'impulsions électriques, de lumière ou d'ondes électromagnétiques) ou bien au niveau du type de support (câble coaxial, paires torsadées, fibre optique, etc.).

2. Intérêt d'un réseau

Un ordinateur est une machine permettant de manipuler des informations. L'homme, en tant qu'être communiquant, a rapidement compris l'intérêt qu'il pouvait y avoir à relier ces ordinateurs entre eux afin de pouvoir échanger des informations.
Un réseau informatique peut servir plusieurs buts distincts :

- Le partage de ressources (fichiers, applications ou matériels, connexion à internet, etc.)
- La communication entre personnes (courrier électronique, discussion en direct, visioconférences, etc.)
- La communication entre processus (entre des ordinateurs industriels par exemple)
- L'accès partagé à l'information (bases de données en réseau)
- La collaboration dans la réalisation de différentes tâches à l'aide de groupwares (l'édition de texte par exemple)
- Le jeu vidéo multijoueurs.

3. Les deux catégories de réseau

On distingue généralement les deux catégories de réseaux suivants :

- Les réseaux poste à poste (peer to peer / égal à égal)
- Les réseaux organisés autour de serveurs (Client/Serveur)

Ces deux types de réseau ont des capacités différentes. Le type de réseau à installer dépend généralement des critères suivants :

- Taille de l'entreprise
- Niveau de sécurité nécessaire
- Type d'activité
- Niveau de compétence d'administration disponible
- Volume du trafic sur le réseau
- Besoins des utilisateurs du réseau
- Budget alloué au fonctionnement du réseau (pas seulement l'achat mais aussi l'entretien et la maintenance)

3. Topologie des réseaux

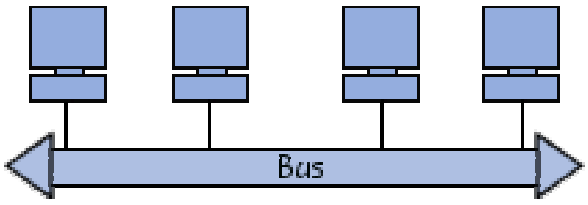
Un réseau informatique est constitué d'ordinateurs reliés entre eux grâce à des lignes de communication (câbles réseaux, ondes radio, etc.) et des éléments matériels (cartes réseau, ainsi que d'autres équipements permettant d'assurer la bonne circulation des données). L'arrangement physique, c'est-à-dire la configuration spatiale du réseau est appelé **topologie physique**. On distingue généralement les topologies suivantes :

1. Topologie en bus
2. Topologie en étoile
3. Topologie en anneau
4. Topologie en arbre
5. Topologie maillée

La **topologie logique**, par opposition à la topologie physique, représente la façon dont les données transitent dans les lignes de communication. Les topologies logiques les plus courantes sont Ethernet, Token Ring et FDDI.

3.1. Topologie en bus

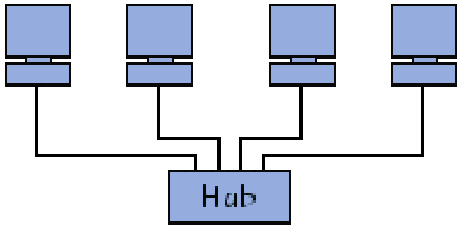
Une **topologie en bus** est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot « bus » désigne la ligne physique qui relie les machines du réseau.



Cette topologie a pour avantage d'être facile à mettre en oeuvre et de posséder un fonctionnement simple. En revanche, elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, l'ensemble du réseau en est affecté.

3.2. Topologie en étoile

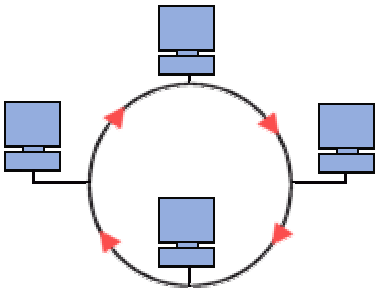
Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel central appelé concentrateur (en anglais hub). Il s'agit d'une boîte comprenant un certain nombre de jonctions auxquelles il est possible de raccorder les câbles réseau en provenance des ordinateurs. Celui-ci a pour rôle d'assurer la communication entre les différentes jonctions.



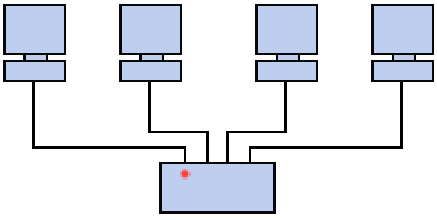
Contrairement aux réseaux construits sur une topologie en bus, les réseaux suivant une topologie en étoile sont beaucoup moins vulnérables car une des connexions peut être débranchée sans paralyser le reste du réseau. Le point névralgique de ce réseau est le concentrateur, car sans lui plus aucune communication entre les ordinateurs du réseau n'est possible.
En revanche, un réseau à topologie en étoile est plus onéreux qu'un réseau à topologie en bus car un matériel supplémentaire est nécessaire (le hub).

3.3. Topologie en anneau

Dans un réseau possédant une topologie en anneau, les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour.



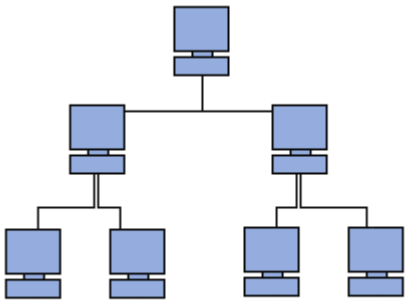
En réalité, dans une topologie anneau, les ordinateurs ne sont pas reliés en boucle, mais sont reliés à un **répartiteur** (appelé *MAU*, *Multistation Access Unit*) qui va gérer la communication entre les ordinateurs qui lui sont reliés en impartissant à chacun d'entre-eux un temps de parole.



Les deux principales topologies logiques utilisant cette topologie physique sont Token ring (anneau à jeton) et FDDI.

3.4. Topologie en arbre

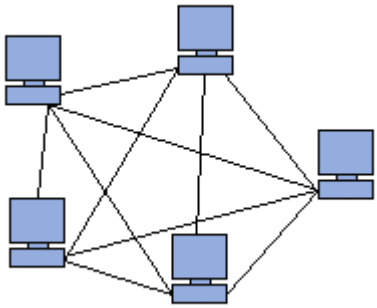
Aussi connu sous le nom de topologie hiérarchique, le réseau est divisé en niveaux. Le sommet, le haut niveau, est connectée à plusieurs nœuds de niveau inférieur, dans la hiérarchie. Ces nœuds peuvent être eux-mêmes connectés à plusieurs nœuds de niveau inférieur. Le tout dessine alors un arbre, ou une arborescence.



3.5. Topologie maillée

Une topologie maillée, est une évolution de la topologie en étoile, elle correspond à plusieurs liaisons point à point. Une unité réseau peut avoir (1,N) connexions point à point vers plusieurs autres unités. Chaque terminal est relié à tous les autres. L'inconvénient est le nombre de liaisons nécessaires qui devient très élevé.

Cette topologie se rencontre dans les grands réseaux de distribution (Exemple : Internet). L'information peut parcourir le réseau suivant des itinéraires divers, sous le contrôle de puissants superviseurs de réseau, ou grâce à des méthodes de routage réparties. L'armée utilise également cette topologie, ainsi, en cas de rupture d'un lien, l'information peut quand même être acheminée.
Elle existe aussi dans le cas de couverture Wi-Fi. On parle alors bien souvent de topologie mesh mais ne concerne que les routeurs WiFi.



4. Différents types de réseaux

On distingue différents types de réseaux (privés) selon leur taille (en terme de nombre de machines), leur vitesse de transfert des données ainsi que leur étendue. Les réseaux privés sont des réseaux appartenant à une même organisation. On fait généralement trois catégories de réseaux :

- LAN (local area network)
- MAN (metropolitan area network)
- WAN (wide area network)

4.1. Les LAN : réseaux locaux

LAN signifie *Local Area Network* (en français *Réseau Local*). Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie (la plus répandue étant Ethernet). Un réseau local est donc un réseau sous sa forme la plus simple. La vitesse de transfert de données d'un réseau local peut s'échelonner entre 10 Mbps (pour un réseau Ethernet par exemple) et 1 Gbps (en FDDI ou Gigabit Ethernet par exemple). La taille d'un réseau local peut atteindre jusqu'à 100 voire 1000 utilisateurs.
En élargissant le contexte de la définition aux services qu'apportent le réseau local, il est possible de distinguer deux modes de fonctionnement :

- dans un environnement d'"égal à égal" (en anglais *peer to peer*), dans lequel il n'y a pas d'ordinateur central et chaque ordinateur a un rôle similaire
- dans un environnement "client/serveur", dans lequel un ordinateur central fournit des services réseau aux utilisateurs.

4.2. Les MAN : réseaux métropolitains

Les **MAN** (*Metropolitan Area Network*) interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants. Ainsi un MAN permet à deux noeuds distants de communiquer comme si ils faisaient partie d'un même réseau local. Un MAN est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique).

4.3. Les WAN : réseaux étendus

Un **WAN** (*Wide Area Network* ou réseau étendu) interconnecte plusieurs LANs à travers de grandes distances géographiques. Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance) et peuvent être faibles.
Les WAN fonctionnent grâce à des routeurs qui permettent de "choisir" le trajet le plus approprié pour atteindre un noeud du réseau. Le plus connu des WAN est Internet.

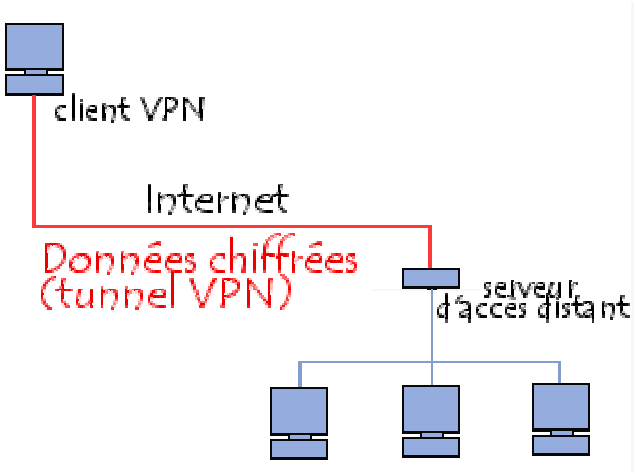
5. Le concept de réseau privé virtuel (RPV/VPN)

Les réseaux locaux d'entreprise (LAN ou RLE) sont des réseaux internes à une organisation, c'est-à-dire que les liaisons entre machines appartiennent à l'organisation. Ces réseaux sont de plus en plus souvent reliés à Internet par l'intermédiaire d'équipements d'interconnexion. Il arrive ainsi souvent que des entreprises éprouvent le besoin de communiquer avec des filiales, des clients ou même du personnel géographiquement éloignées via internet.
Pour autant, les données transmises sur Internet sont beaucoup plus vulnérables que lorsqu'elles circulent sur un réseau interne à une organisation car le chemin emprunté n'est pas défini à l'avance, ce qui signifie que les données empruntent une infrastructure réseau publique appartenant à différents opérateurs. Ainsi il n'est pas impossible que sur le chemin parcouru, le réseau soit écouté par un utilisateur indiscret ou même détourné. Il n'est donc pas concevable de transmettre dans de telles conditions des informations sensibles pour l'organisation ou l'entreprise.
La première solution pour répondre à ce besoin de communication sécurisé consiste à relier les réseaux distants à l'aide de liaisons spécialisées. Toutefois la plupart des entreprises ne

peuvent pas se permettre de relier deux réseaux locaux distants par une ligne spécialisée, il est parfois nécessaire d'utiliser Internet comme support de transmission.
Un bon compromis consiste à utiliser Internet comme support de transmission en utilisant un protocole d' "encapsulation" (en anglais *tunneling*, d'où l'utilisation impropre parfois du terme "tunnelisation"), c'est-à-dire encapsulant les données à transmettre de façon chiffrée. On parle alors de **réseau privé virtuel** (noté *RPV* ou **VPN**, acronyme de *Virtual Private Network*) pour désigner le réseau ainsi artificiellement créé.
Ce réseau est dit *virtuel* car il relie deux réseaux "physiques" (réseaux locaux) par une liaison non fiable (Internet), et *privé* car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent "voir" les données.
Le système de *VPN* permet donc d'obtenir une liaison sécurisée à moindre coût, si ce n'est la mise en oeuvre des équipements terminaux. En contrepartie il ne permet pas d'assurer une qualité de service comparable à une ligne louée dans la mesure où le réseau physique est public et donc non garanti.

Fonctionnement d'un VPN :

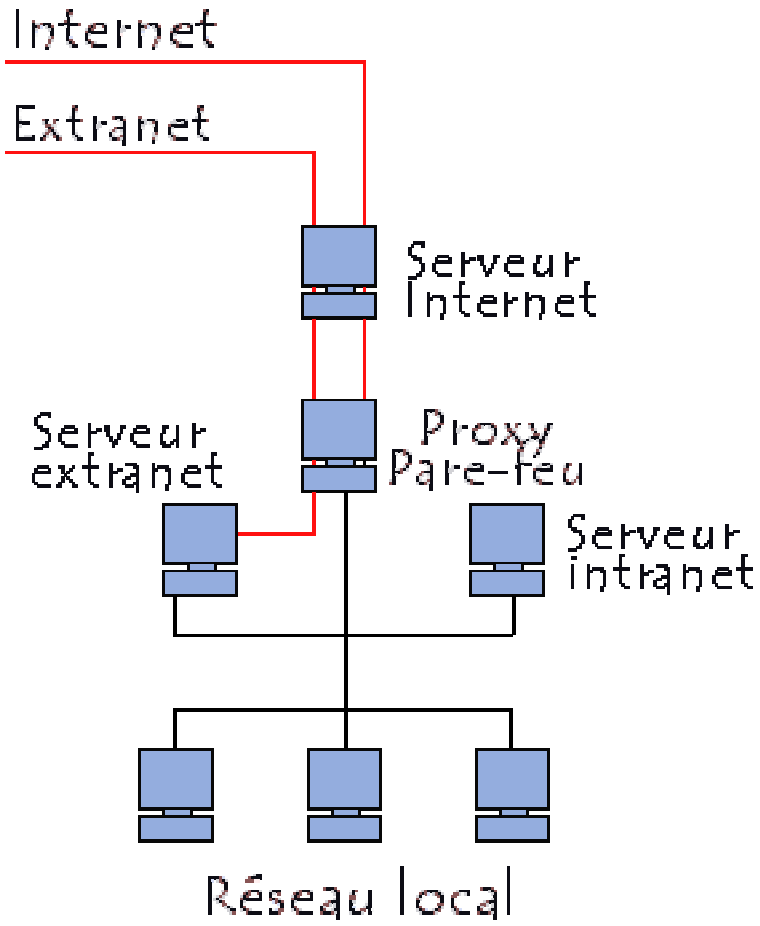
Un réseau privé virtuel repose sur un protocole, appelé **protocole de tunnelisation** (*tunneling*), c'est-à-dire un protocole permettant aux données passant d'une extrémité du VPN à l'autre d'être sécurisées par des algorithmes de cryptographie.



Le terme de "tunnel" est utilisé pour symboliser le fait qu'entre l'entrée et la sortie du VPN les données sont chiffrées (cryptées) et donc incompréhensible pour toute personne située entre les deux extrémités du VPN, comme si les données passaient dans un tunnel. Dans le cas d'un *VPN* établi entre deux machines, on appelle *client VPN* l'élément permettant de chiffrer et de déchiffrer les données du côté utilisateur (client) et *serveur VPN* (ou plus généralement **serveur d'accès distant**) l'élément chiffrant et déchiffrant les données du côté de l'organisation.
De cette façon, lorsqu'un utilisateur nécessite d'accéder au réseau privé virtuel, sa requête va être transmise en clair au système passerelle, qui va se connecter au réseau distant par l'intermédiaire d'une infrastructure de réseau public, puis va transmettre la requête de façon chiffrée. L'ordinateur distant va alors fournir les données au serveur VPN de son réseau local qui va transmettre la réponse de façon chiffrée. A réception sur le client VPN de l'utilisateur, les données seront déchiffrées, puis transmises à l'utilisateur.

6. Le concept d'Intranet

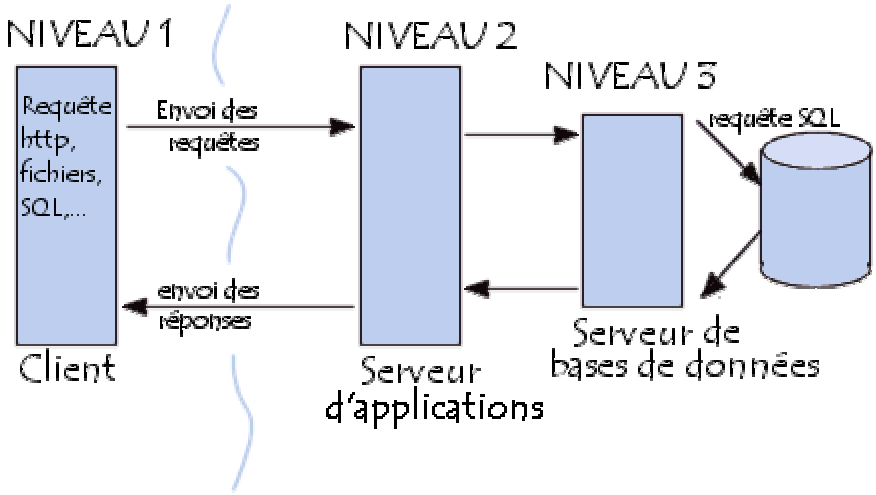
Un **intranet** est un ensemble de services internet (par exemple un serveur web, un serveur de messagerie, etc.) internes à un réseau local, c'est-à-dire accessibles uniquement à partir des postes d'un réseau local, ou bien d'un ensemble de réseaux bien définis, et invisibles (ou inaccessibles) de l'extérieur. Il consiste à utiliser les standards client-serveur de l'internet (en utilisant les protocoles TCP/IP), comme par exemple l'utilisation de navigateurs internet (client basé sur le protocole HTTP) et des serveurs web (protocole HTTP), pour réaliser un système d'information interne à une organisation ou une entreprise.



Un intranet repose généralement sur une architecture à trois niveaux, composée :

- de clients (navigateur Internet généralement) ;
- d'un ou plusieurs serveurs d'application (middleware): un serveur web permettant d'interpréter des scripts CGI, PHP, ASP ou autres, et les traduire en requêtes SQL afin d'interroger une base de données ;
- d'un serveur de bases de données.

De cette façon, les machines clientes gèrent l'interface graphique, tandis que les différents serveurs manipulent les données. Le réseau permet de véhiculer les requêtes et les réponses entre clients et serveurs.



Un intranet possède naturellement plusieurs clients (les ordinateurs du réseau local) et peut aussi être composé de plusieurs serveurs. Une grande entreprise peut par exemple posséder un serveur web pour chaque service afin de fournir un intranet composé d'un serveur web fédérateur liant les différents serveurs gérés par chaque service.

L'utilité d'un intranet

Un intranet dans une entreprise permet de mettre facilement à la disposition des employés des documents divers et variés; cela permet d'avoir un accès centralisé et cohérent à la mémoire de l'entreprise, on parle ainsi de *capitalisation de connaissances*. De cette façon, il est généralement nécessaire de définir des droits d'accès pour les utilisateurs de l'intranet aux documents présents sur celui-ci, et par conséquent une authentification de ceux-ci afin de leur permettre un accès personnalisé à certains documents.
Des documents de tous types (textes, images, vidéos, sons, ...) peuvent être mis à disposition sur un intranet. De plus, un intranet peut réaliser une fonction de groupware très intéressante, c'est-à-dire permettre un travail coopératif. Voici quelques unes des fonctions qu'un intranet peut réaliser :

- Mise à disposition d'informations sur l'entreprise (panneau d'affichage)
- Mise à disposition de documents techniques
- Moteur de recherche de documentations
- Un échange de données entre collaborateurs
- Annuaire du personnel
- Gestion de projet, aide à la décision, agenda, ingénierie assistée par ordinateur
- Messagerie électronique
- Forum de discussion, liste de diffusion, chat en direct
- Visioconférence
- Portail vers internet

Ainsi, un intranet favorise la communication au sein de l'entreprise et limite les erreurs dues à la mauvaise circulation d'une information. L'information disponible sur l'intranet doit être mise à jour en évitant les conflits de version.

Avantages d'un intranet

Un intranet permet de constituer un système d'information à faible coût (concrètement le coût d'un intranet peut très bien se réduire au coût du matériel, de son entretien et de sa mise à jour, avec des postes clients fonctionnant avec des navigateurs gratuits, un serveur fonctionnant sous Linux avec le serveur webApache et le serveur de bases de données MySQL).
D'autre part, étant donné la nature "universelle" des moyens mis en jeu, n'importe quel type de machine peut être connectée au réseau local, donc à l'intranet.

Mise en place de l'intranet

Un intranet doit être conçu selon les besoins de l'entreprise ou de l'organisation (au niveau des services à mettre en place). Ainsi, l'intranet ne doit pas être conçu par les seuls informaticiens de l'entreprise mais selon un projet prenant en compte les besoins de toutes les parties prenant de l'entreprise.
Pour ce qui est de la mise en place matérielle, il suffit de mettre en place un serveur web (par exemple une machine fonctionnant sous Linux avec le serveur web *Apache* et le serveur de bases de données*MySQL* ou bien un serveur sous wWindows avec le serveur web *Microsoft Internet Information Server*). Il suffit ensuite de configurer un nom de domaine pour le serveur (par exemple *intranet.votre_entreprise.com*. Il est à noter l'existence de CMS (systèmes de gestion de contenu) permettant de gérer la publication des pages par une équipe de rédacteurs.

7. Le concept d'Extranet

Un **extranet** est une extension du système d'information de l'entreprise à des partenaires situés au-delà du réseau. L'accès à l'extranet doit être sécurisé dans la mesure où cela offre un accès au système d'information à des personnes situées en dehors de l'entreprise.
Il peut s'agir soit d'une authentification simple (authentification par nom d'utilisateur et mot de passe) ou d'une authentification forte (authentification à l'aide d'un certificat). Il est conseillé d'utiliser HTTPS pour toutes les pages web consultées depuis l'extérieur afin de sécuriser le transport des requêtes et des réponses HTTP et d'éviter notamment la circulation du mot de passe en clair sur le réseau.
Un extranet n'est donc ni un intranet, ni un site internet. Il s'agit d'un système supplémentaire offrant par exemple aux clients d'une entreprise, à ses partenaires ou à des filiales, un accès privilégié à certaines ressources informatiques de l'entreprise par l'intermédiaire d'une interface Web.