



Jean-François PILLOU
Fabrice LEMAINQUE

Comment
ça marche
.net

Tout sur les Réseaux et Internet

5^e édition



DUNOD

Routeur

Commutateur

Téléphonie 3G/4G/5G

CPL

TCP/IP

DNS

DHCP

NAT

VPN

Ethernet

Bluetooth

WiMAX

WiFi

WPA, etc.

Directeur de collection : Jean-François Pillou

Illustration de couverture : Rachid Marai

Le pictogramme qui figure ci-contre mérite une explication. Son objet est d'alerter le lecteur sur la menace que représente pour l'avenir de l'écrit, particulièrement dans le domaine de l'édition technique et universitaire, le développement massif du photocopillage.

Le Code de la propriété intellectuelle du 1^{er} juillet 1992 interdit en effet expressément la photocopie à usage collectif sans autorisation des ayants droit. Or, cette pratique s'est généralisée dans les établissements

d'enseignement supérieur, provoquant une baisse brutale des achats de livres et de revues, au point que la possibilité même pour

les auteurs de créer des œuvres nouvelles et de les faire éditer correctement est aujourd'hui menacée.

Nous rappelons donc que toute reproduction, partielle ou totale, de la présente publication est interdite sans autorisation de l'auteur, de son éditeur ou du Centre français d'exploitation du

droit de copie (CFC, 20, rue des Grands-Augustins, 75006 Paris).



© Dunod, 2020

11 rue Paul Bert, 92240 Malakoff

www.dunod.com

ISBN 978-2-10-080767-3

Le Code de la propriété intellectuelle n'autorisant, aux termes de l'article L. 122-5, 2° et 3° a), d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (art. L. 122-4).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.



Table des matières

Avant-propos	1
1. Initiation aux réseaux	3
Concept de réseau	3
Intérêt d'un réseau	4
Topologie d'un réseau	5
Architectures réseau	7
Familles de réseaux	11
2. Transmission de données	15
Représentation des données	15
Canal de transmission	16
Modes de transmission	21
Transmission analogique	26
Transmission numérique	27
Câblage coaxial	31
Câblage à paire torsadée	33
Fibre optique	36
Multiplexage	37
3. Protocoles réseau	43
Notion de protocole	43
Adresse IP	44
Système de noms de domaine	56
Notion de port	64

4. TCP/IP	67
Différence entre standard et mise en œuvre	68
Un modèle en couches	68
Modèle OSI	68
Modèle TCP/IP	70
Encapsulation des données	71
Protocole TCP	74
Protocole IP	81
5. Les autres protocoles du modèle TCP/IP	93
Protocole ARP	93
Protocole RARP	94
Protocole ICMP	95
Protocole UDP	98
Protocoles de routage	99
Protocoles d'accès au réseau	103
6. Protocoles applicatifs	107
Protocole HTTP	107
Protocole FTP	118
Protocole Telnet	127
Protocoles de messagerie	134
Protocole DHCP	141
7. Internet	147
Connexion à Internet	148
Courrier électronique	153
8. Équipements	157
Présentation	157
Répéteur	159
Concentrateur	160
Pont	161
Commutateur	163
Passerelle applicative	163
Routeur	164

B-routeur	167
Proxy	167
9. Réseaux sans fil	171
Catégories de réseaux sans fil	172
Propagation des ondes radio	183
Bluetooth	186
WiMAX	191
WiFi	194
Risques liés aux réseaux sans fil	203
Courant porteur en ligne (CPL)	206
10. Mise en place d'un réseau	211
Matériel nécessaire	211
Mise en œuvre	213
Mise en réseau	216
Mise en place d'un réseau sans fil	219
Mode infrastructure	222
11. Sécurité	225
Pare-feu	227
Sécurisation d'un réseau WiFi	233
Protocoles de sécurisation	241
12. Dépannage réseau	249
Outils de dépannage réseau	250
Dépannage de la connectivité réseau	264
Index	285

LES + EN

LIGNE



Téléchargez le chapitre 13, Travail en réseau,
sur le site www.dunod.com à l'adresse suivante :
<https://dunod.com/EAN/9782100807673>

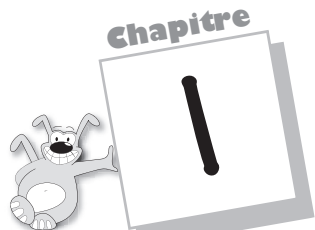


Avant-propos

Autrefois réservés aux seules entreprises, les réseaux touchent aujourd'hui tous les utilisateurs d'ordinateurs, en particulier ceux connectés à Internet. Les réseaux permettent d'accéder à d'innombrables fonctionnalités, telles que le partage de ressources, le jeu en réseau, le partage de fichiers, ainsi qu'à un volume d'informations sans précédent avec l'interconnexion des réseaux *via* Internet.

S'il est très facile de se connecter à Internet, le partage de ressources (partage de la connexion par exemple) ou la mise en place d'un réseau sans fil sécurisé nécessitent un certain nombre de compétences et de connaissances préalables. Le développement exponentiel des dispositifs sans fil liés à la téléphonie mobile étend le concept de réseau tel qu'il était auparavant perçu.

Le but de cet ouvrage est de faire un point sur les différentes notions à connaître pour acquérir une culture générale sur les réseaux et de pouvoir comprendre les discussions sur ce sujet, notamment dans un contexte professionnel.



Initiation aux réseaux

Concept de réseau

Un **réseau** est un ensemble d'objets interconnectés. Il permet de faire circuler des éléments entre chacun de ces objets selon des règles bien définies.

Selon le type d'objets, on parlera parfois de :

- **Réseau de transport** : ensemble d'infrastructures et de disposition 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 de neurones** : ensemble de cellules interconnectées entre elles.
- **Réseau de malfaiteurs** : ensemble d'escrocs qui sont en contact les uns avec les autres (un escroc en cache généralement un autre !)
- **Réseau informatique** : ensemble d'ordinateurs reliés entre eux grâce à des lignes physiques et échangeant des informations sous forme de données numériques (des valeurs binaires, c'est-à-dire codées sous forme de signaux pouvant prendre deux valeurs : 0 et 1).

Le présent ouvrage s'intéressera bien évidemment aux réseaux informatiques.

Il n'existe pas qu'un seul type de réseau, car historiquement il existe des types d'ordinateurs différents, communiquant selon des langages divers et variés. De plus, les supports physiques de transmission les reliant peuvent être très hétérogènes, que ce soit au niveau du transfert de données (circulation de données sous forme d'impulsions électriques, sous forme de lumière ou bien sous forme d'ondes électromagnétiques) ou bien au niveau du type de support (lignes en cuivres, en câble coaxial, en fibre optique...).

Les différents chapitres suivants s'attacheront à décrire les caractéristiques des supports physiques des transmissions, ainsi que la manière dont les données transitent sur le réseau.

Intérêt d'un réseau

Un **ordinateur** est une machine permettant de manipuler des données. 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).
- La communication entre personnes (courrier électronique, discussion en direct, etc.).
- La communication entre processus (entre des machines industrielles par exemple).
- La garantie de l'unicité de l'information (bases de données).
- Le jeu vidéo multijoueurs.

Les réseaux permettent aussi de standardiser les applications, on parle généralement de **groupware**. Par exemple, la messagerie électronique et les agendas de groupe qui permettent de communiquer plus efficacement et plus rapidement.

Voici les avantages qu'offrent de tels systèmes :

- diminution des coûts grâce aux partages des données et des périphériques,

- standardisation des applications,
- accès aux données en temps utile,
- communication et organisation plus efficaces.

Aujourd'hui, la tendance est au développement vers des **réseaux étendus** (WAN) déployés à l'échelle du pays, voire à l'échelle mondiale. Ainsi, les intérêts sont multiples, que ce soit pour une entreprise ou pour un particulier.

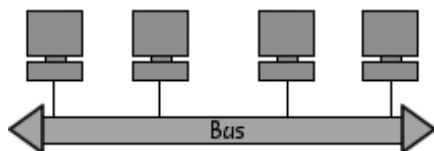
Topologie d'un réseau

Un réseau informatique est constitué d'ordinateurs reliés entre eux grâce à des lignes de communication (câbles réseaux, liaisons sans fil, 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 :

- la topologie en bus,
- la topologie en étoile,
- la topologie en anneau,
- la topologie en arbre,
- la 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.

Topologie en bus



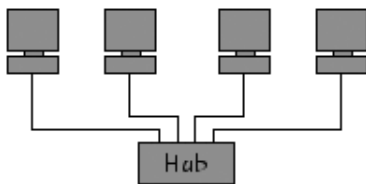
Une **topologie en bus** est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câbles, généralement de type coaxial. Le mot « bus » désigne la ligne physique qui relie les machines du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

Cette topologie a pour avantage d'être facile à mettre en œuvre 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.

Topologie en étoile

Dans une **topologie en étoile**, les ordinateurs du réseau sont reliés à un système matériel central appelé **concentrateur** (*hub*, littéralement *moyeu de roue*). 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. Le concentrateur a pour rôle d'assurer la communication entre les différentes jonctions.

Comparativement 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.

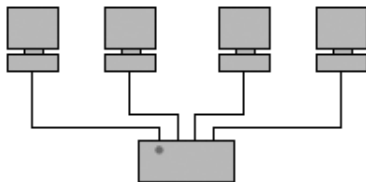


En revanche, un réseau à topologie en étoile est plus onéreux qu'un réseau à topologie en bus car un matériel supplémentaire est nécessaire (le concentrateur).

Topologie en anneau

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

Ils sont en réalité reliés à un **répartiteur** (MAU, *Multistation Access Unit*) qui va gérer la communication entre eux en impartissant à chacun un « temps de parole ».



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

Architectures réseau

En élargissant le contexte de la définition du réseau aux services qu'il apporte, il est possible de distinguer deux modes de fonctionnement :

- **l'architecture d'égal à égal** (*peer to peer*, parfois appelée « poste à poste »), dans lequel il n'y a pas d'ordinateur central et chaque ordinateur joue un rôle similaire,
- **l'architecture de type client-serveur**, où un ordinateur (serveur) fournit des services réseau aux ordinateurs clients.

Architecture d'égal à égal

Dans une architecture d'**égal à égal** (ou *poste à poste*), contrairement à une architecture de réseau de type client-serveur, il n'y a pas de serveur dédié. Ainsi, chaque ordinateur dans un tel réseau est un peu serveur et un peu client. Cela signifie que chacun des ordinateurs du réseau est libre de partager ses ressources. Un ordinateur relié à une imprimante pourra donc éventuellement la partager afin que tous les autres ordinateurs puissent y accéder *via* le réseau.

❑ Inconvénients

Les réseaux d'égal à égal ont énormément d'inconvénients :

- ce système n'est pas du tout centralisé, ce qui le rend très difficile à administrer,
- la sécurité est très peu présente,
- aucun maillon du système n'est fiable.

Ainsi, les réseaux d'égal à égal ne sont valables que pour un petit nombre d'ordinateurs (généralement une dizaine), et pour des applications ne nécessitant pas une grande sécurité (il est donc déconseillé pour un réseau professionnel avec des données sensibles).

❑ Avantages

L'architecture d'égal à égal a tout de même quelques avantages parmi lesquels :

- **un coût réduit** (les coûts engendrés par un tel réseau sont le matériel, les câbles et la maintenance),
- **une simplicité** à toute épreuve !

❑ Mise en œuvre d'un réseau poste à poste

Les **réseaux poste à poste** ne nécessitent pas les mêmes niveaux de performance et de sécurité que les logiciels réseau pour serveurs dédiés. On peut donc utiliser les différentes versions de Windows car tous ces systèmes d'exploitation intègrent toutes les fonctionnalités du réseau poste à poste.

La mise en œuvre d'une telle architecture réseau repose sur des solutions standards :

- placer les ordinateurs sur le bureau des utilisateurs,
- chaque utilisateur est son propre administrateur et planifie lui-même sa sécurité,
- pour les connexions, on utilise un système de câblage simple et apparent.

Il s'agit généralement d'une solution satisfaisante pour des environnements ayant les caractéristiques suivantes :

- moins de 10 utilisateurs,
- tous les utilisateurs sont situés dans une même zone géographique,
- la sécurité n'est pas un problème crucial,
- ni l'entreprise ni le réseau ne sont susceptibles d'évoluer de manière significative dans un proche avenir.

❑ Administration d'un réseau poste à poste

On désigne par le terme **administration** :

- la gestion des utilisateurs et de la sécurité,
- la mise à disposition des ressources,
- la maintenance des applications et des données,
- l'installation et la mise à niveau des logiciels utilisateurs.

Dans un réseau poste à poste typique, il n'y a pas d'administrateur. Chaque utilisateur administre son propre poste. Tous les utilisateurs peuvent partager leurs ressources comme ils le souhaitent (données dans des répertoires partagés, imprimantes, etc.).

❑ Notions de sécurité

La politique de **sécurité minimale** consiste à affecter un mot de passe à une ressource. Les utilisateurs d'un réseau poste à poste définissent leur propre sécurité et, comme tous les partages peuvent exister sur tous les ordinateurs, il est difficile de mettre en œuvre un contrôle centralisé. Ceci pose également un problème de sécurité globale du réseau car certains utilisateurs ne sécurisent pas du tout leurs ressources.

Architecture client/serveur

De nombreuses applications fonctionnent selon un environnement client-serveur. Cela signifie que des **machines clientes** (des machines faisant partie du réseau) contactent un **serveur** qui leur

fournit des **services**, programmes fournissant des données telles que l'heure, des fichiers, une connexion...

Les services sont exploités par des programmes, appelés **programmes clients**, s'exécutant sur les machines clientes. On parle ainsi de client FTP, client de messagerie... lorsque l'on désigne un programme, tournant sur une machine cliente, capable de traiter des informations qu'il récupère auprès du serveur (dans le cas du client FTP il s'agit de fichiers, tandis que pour le client messagerie il s'agit de courrier électronique).

Dans un environnement purement client/serveur, les ordinateurs du réseau (les clients) ne peuvent voir que le serveur, c'est un des principaux atouts de ce modèle.

Avantages

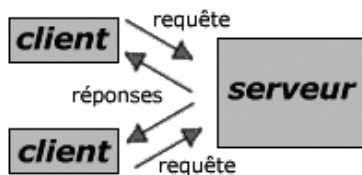
Le modèle client/serveur est particulièrement recommandé pour des réseaux nécessitant un grand niveau de fiabilité, ses principaux atouts sont :

- **des ressources centralisées** : étant donné que le serveur est au centre du réseau, il peut gérer des ressources communes à tous les utilisateurs, comme par exemple une base de données centralisée, afin d'éviter les problèmes de redondance et de contradiction ;
- **une meilleure sécurité** : car le nombre de points d'entrée permettant l'accès aux données est moins important ;
- **une administration au niveau serveur** : les clients ayant peu d'importance dans ce modèle, ils ont moins besoin d'être administrés ;
- **un réseau évolutif** : grâce à cette architecture il est possible de supprimer ou de rajouter des clients sans perturber le fonctionnement du réseau et sans modifications majeures.

Inconvénients

L'architecture client/serveur a tout de même quelques lacunes parmi lesquelles :

- **un coût élevé** : dû à la technicité du serveur ;



- **un maillon faible** : le serveur est le maillon faible du réseau client/serveur, tout le réseau étant architecturé autour de lui ! La mise en place d'un système de tolérance de panne et de récupération après incident est indispensable et comprend notamment le recours à la méthodologie RAID (*Redundant Array of Independent Disks*). En outre les différents rôles serveur (serveur d'applications, serveur DNS, serveur DHCP, serveur de base de données, serveur de messagerie, etc.) sont désormais fréquemment répartis sur différentes machines théoriquement chacune dotée d'un système de redondance, ce qui contribue également à répartir et diminuer le risque.

❑ **Fonctionnement d'un système client/serveur**

Un système client/serveur fonctionne selon le schéma suivant :

- Le client émet une requête vers le serveur grâce à son adresse et le port qui désigne un service particulier du serveur.
- Le serveur reçoit la demande et répond à l'aide de l'adresse de la machine client et son port.

Familles de réseaux

On distingue différents types de réseaux selon leur taille (en termes de nombre de machines), leur vitesse de transfert des données ainsi que leur étendue. On définit généralement les catégories de réseaux suivantes :

- **Réseaux personnels** ou PAN (*Personal Area Network*).
- **Réseaux locaux** ou LAN (*Local Area Network*).

- **Réseaux métropolitains** ou MAN (*Metropolitan Area Network*).
- **Réseaux étendus** ou WAN (*Wide Area Network*).

Il existe d'autres types de réseaux tels que les **TAN** (*Tiny Area Network*) identiques aux LAN mais moins étendus (deux à trois machines) ou les **CAN** (*Campus Area Network*) identiques au MAN avec une bande passante maximale entre tous les LAN du réseau.

Réseaux locaux (LAN)

Un réseau local (**LAN**, *Local Area Network*) désigne 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 (Ethernet ou WiFi).

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 (Ethernet standard) à 10 Gbps (10 Gigabit Ethernet), voire plus dans certaines entreprises ou *data centers*. Et cela ne devrait pas s'arrêter : le record actuel de débit sur fibre optique dépasse les 40 Tbps. Un réseau local peut comporter de moins d'une dizaine de machines à plusieurs milliers.

En élargissant le contexte de la définition aux services qu'apporte le réseau local, il est possible de distinguer deux modes de fonctionnement :

- dans un environnement **d'égal à égal** (*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.

Réseaux métropolitains (MAN)

Les réseaux métropolitains (**MAN**, *Metropolitan Area Network*) interconnectent plusieurs réseaux locaux géographiquement proches (au maximum quelques dizaines de kilomètres) avec un débit important. Ainsi, un réseau métropolitain permet à deux machines distantes de communiquer comme si elles faisaient partie d'un même réseau local.

Un MAN est formé d'équipements réseau interconnectés par des liens hauts débits (en général en fibre optique).

Réseaux étendus (WAN)

Un réseau étendu (**WAN**, *Wide Area Network*) interconnecte plusieurs réseaux locaux 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 équipements réseau appelés **routeurs**, qui permettent de déterminer le trajet le plus approprié pour atteindre une machine du réseau.

Réseaux locaux virtuels (VLAN)

Un **VLAN** (*Virtual Local Area Network* ou *Virtual LAN*, en français *Réseau local virtuel*) est un réseau local regroupant un ensemble de machines de façon logique et non physique.

En effet dans un réseau local la communication entre les différentes machines est régie par l'architecture physique. Grâce aux réseaux virtuels (VLAN), il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage...) en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole, etc.).

❑ Typologie de VLAN

Plusieurs types de VLAN sont définis par les normes IEEE 802.1, selon le critère de commutation et le niveau auquel il s'effectue :

- Un **VLAN de niveau 1** (aussi appelé **VLAN par port** ou *Port-Based VLAN*) définit un réseau virtuel en fonction des ports de raccordement sur le commutateur.
- Un **VLAN de niveau 2** (également appelé **VLAN MAC**, *VLAN par adresse IEEE* ou *MAC Address-Based VLAN*) définit un réseau virtuel en fonction des adresses MAC des stations.

Ce type de VLAN est beaucoup plus souple que le VLAN par port car le réseau est indépendant de la localisation de la station.

- Un **VLAN de niveau 3** : on distingue plusieurs types de VLAN de niveau 3 :
 - Le **VLAN par sous-réseau** (*Network Address-Based VLAN*) associe des sous-réseaux selon l'adresse IP source des datagrammes. Ce type de solution apporte une grande souplesse dans la mesure où la configuration des commutateurs se modifie automatiquement en cas de déplacement d'une station. En contrepartie une légère dégradation de performances peut se faire sentir dans la mesure où les informations contenues dans les paquets doivent être analysées plus finement.
 - Le **VLAN par protocole** (*Protocol-Based VLAN*) permet de créer un réseau virtuel par type de protocole (par exemple TCP/IP, IPX, AppleTalk...), regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même réseau.

□ Les avantages du VLAN

Le VLAN permet de définir un nouveau réseau au-dessus du réseau physique et à ce titre offre les avantages suivants :

- Plus de **souplesse pour l'administration et les modifications** du réseau car toute l'architecture peut être modifiée par simple paramétrage des commutateurs.
- Gain en **sécurité** car les informations sont encapsulées dans un niveau supplémentaire et éventuellement analysées.
- **Réduction de la diffusion du trafic** sur le réseau.

Transmission de données

Représentation des données

Le but d'un réseau est de transmettre des informations d'un ordinateur à un autre. Pour cela il faut dans un premier temps décider du type de codage de la donnée à envoyer, c'est-à-dire sa **représentation informatique**. Celle-ci sera différente selon le type de données, car il peut s'agir de : données sonores, données textuelles, données graphiques, données vidéo...

La représentation de ces données peut se diviser en deux catégories :

- Une **représentation numérique** : c'est-à-dire le codage de l'information en un ensemble de valeurs binaires, soit une suite de 0 et de 1.
- Une **représentation analogique** : c'est-à-dire que la donnée sera représentée par la variation d'une grandeur physique continue.

Support de transmission des données

Pour que la transmission de données puisse s'établir, il doit exister une ligne de transmission, appelée aussi **voie de transmission** ou **canal**, entre les deux machines.

Ces voies de transmission sont constituées de plusieurs tronçons permettant de faire circuler les données sous forme d'ondes électromagnétiques, électriques, lumineuses ou même acoustiques.

On a donc un phénomène vibratoire qui se propage sur le support physique.

Codage des signaux de transmission

Pour qu'il puisse y avoir un échange de données, un **codage des signaux de transmission** doit être choisi, celui-ci dépend essentiellement du support physique utilisé pour transférer les données, ainsi que de la garantie de l'intégrité des données et de la vitesse de transmission.

Transmission simultanée de données

La transmission de données est « simple » lorsque seules deux machines sont en communication, ou lorsque l'on envoie une seule donnée. Dans le cas contraire, il est nécessaire de mettre en place plusieurs lignes de transmission ou bien de partager la ligne entre les différents acteurs de la communication. Ce partage est appelé **multiplexage**.

Protocoles de communication

Un **protocole** est un langage commun utilisé par l'ensemble des acteurs de la communication pour échanger des données. Toutefois son rôle ne s'arrête pas là. Un protocole permet aussi :

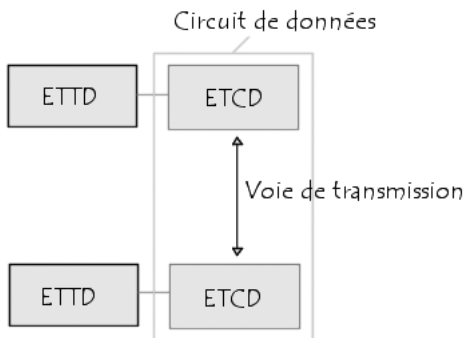
- > l'initiation de la communication,
- > l'échange de données,
- > le contrôle d'erreur,
- > une fin de communication « courtoise ».

Canal de transmission

Une ligne de transmission est une liaison entre les deux machines. On désigne généralement par le terme **émetteur** la machine qui envoie les données et par **récepteur** celle qui les reçoit. Les machines peuvent parfois être chacune à leur tour réceptrice ou émettrice (c'est le cas généralement des ordinateurs reliés par réseau).

La ligne de transmission, appelée aussi parfois **canal de transmission** ou **voie de transmission**, n'est pas forcément constituée d'un seul support physique de transmission, c'est pourquoi les machines d'extrémités (par opposition aux machines intermédiaires), appelées **ETTD** (Équipement terminal de traitement de données ou DTE, *Data Terminal Equipment*) possèdent chacune un équipement relatif au support physique auxquelles elles sont reliées, appelé **ETCD** (Équipement terminal de circuit de données ou DCE, *Data Communication Equipment*).

On nomme **circuit de données** l'ensemble constitué des ETCD de chaque machine et de la ligne de données.

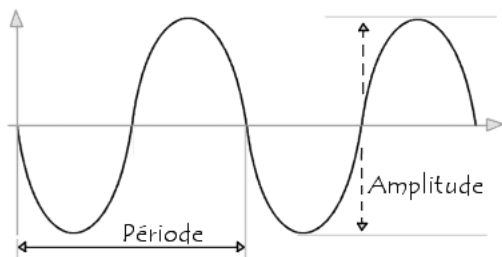


Notions sur les ondes électromagnétiques

La transmission de données sur un support physique se fait par propagation d'un phénomène vibratoire. Il en résulte un signal ondulatoire dépendant de la grandeur physique que l'on fait varier :

- dans le cas de la lumière, il s'agit d'une onde lumineuse ;
- dans le cas du son, il s'agit d'une onde acoustique ;
- dans le cas de la tension ou de l'intensité d'un courant électrique, il s'agit d'une onde électrique...

Les **ondes électromagnétiques** sont caractérisées par leur fréquence (l'inverse de leur période), leur amplitude et leur phase.



Types de supports physiques

Les **supports physiques de transmissions** sont les éléments permettant de faire circuler les informations entre les équipements de transmission. On classe généralement ces supports en trois catégories, selon le type de grandeur physique qu'ils permettent de faire circuler, donc de leur constitution physique :

- Les **supports filaires** permettent de faire circuler une grandeur électrique sur un câble généralement métallique.
- Les **supports aériens** désignent l'air ou le vide, ils permettent la circulation d'ondes électromagnétiques ou radioélectriques diverses.
- Les **supports optiques** permettent d'acheminer des informations sous forme lumineuse.

Selon le type de support physique, la grandeur physique a une vitesse de propagation plus ou moins rapide (par exemple le son se propage dans l'air à une vitesse de l'ordre de 300 m/s alors que la lumière a une célérité proche de 300 000 km/s).

Perturbations

La transmission de données sur une ligne ne se fait pas sans pertes. Tout d'abord le temps de transmission n'est pas immédiat, ce qui impose une certaine « synchronisation » des données à la réception.

D'autre part, des parasites ou des dégradations du signal peuvent apparaître :

- Les **parasites** (souvent appelés **bruit**) sont l'ensemble des perturbations modifiant localement la forme du signal. On distingue généralement deux types de bruit :
 - Le **bruit blanc** qui est une perturbation uniforme du signal, c'est-à-dire qu'il rajoute au signal une petite amplitude dont la moyenne sur le signal est nulle. Le bruit blanc est généralement caractérisé par un ratio appelé **rapport signal/bruit** qui traduit le pourcentage d'amplitude du signal par rapport au bruit (son unité est le décibel, dB). Celui-ci doit être le plus élevé possible.
 - Les **bruits impulsifs** qui sont de petits pics d'intensité provoquant des erreurs de transmission.
- L'**affaiblissement** du signal représente la perte de signal en énergie dissipée dans la ligne. L'affaiblissement se traduit par un signal de sortie plus faible que le signal d'entrée et est caractérisé par la valeur :

$$A = 20 \log (\text{niveau du signal en sortie/niveau du signal en entrée})$$

L'affaiblissement est proportionnel à la longueur de la voie de transmission et à la fréquence du signal.
- La **distorsion** du signal caractérise le déphasage entre le signal en entrée et le signal en sortie.

Bande passante et capacité

La **bande passante** (*bandwidth*) d'une voie de transmission est l'intervalle de fréquence sur lequel le signal ne subit pas un affaiblissement supérieur à une certaine valeur (généralement 3 dB, car 3 décibels correspondent à un affaiblissement du signal de 50 %).

Une ligne de téléphone classique (fil de cuivre) a par exemple, pour la voix, une bande passante comprise entre 300 et 3 400 hertz (Hz) environ pour un taux d'affaiblissement égal à 3 dB. Sur cette même ligne, un signal ADSL utilise une bande passante de 25 kHz à 1 MHz et présentera un affaiblissement (mesuré à 300 kHz) de 20 à 70 dB (la limite pour ADSL).