

# Communiquer en réseau

Enseignement  
Technologique  
Transversal

## Synth.

### Séance 3 Synthèse : la structure d'un réseau

<b>1</b>	<b>Pourquoi et comment communiquer ?</b>	<b>2</b>
<b>2</b>	<b>Caractéristiques d'un réseau</b>	<b>2</b>
2.1	Tolérance aux pannes . . . . .	2
2.2	Evolutivité . . . . .	2
2.3	Qualité de services . . . . .	2
2.4	Sécurité . . . . .	3
<b>3</b>	<b>Elements d'un réseau</b>	<b>3</b>
3.1	Les périphériques terminaux . . . . .	3
3.2	Les périphériques intermédiaires . . . . .	4
3.3	Les connexions . . . . .	4
<b>4</b>	<b>Topologies des réseaux</b>	<b>4</b>
4.1	Quelques topologies physiques classiques . . . . .	4
<b>5</b>	<b>Le modèle OSI</b>	<b>5</b>
<b>6</b>	<b>Adressage et encapsulation</b>	<b>5</b>
6.1	Protocole TCP/IP et analogies utiles . . . . .	6
6.2	L'encapsulation des données . . . . .	7

# 1 Pourquoi et comment communiquer ?

De tout temps, les humains ont ressenti et ressentent le besoin de communiquer. Les méthodes dont nous nous servons pour partager idées et informations changent et évoluent sans cesse. Si le réseau humain se limitait autrefois à des conversations en face à face, aujourd'hui les découvertes en matière de supports étendent sans cesse la portée de nos communications. De la presse écrite à la télévision, chaque innovation a développé et amélioré nos moyens de communication.

## 2 Caractéristiques d'un réseau

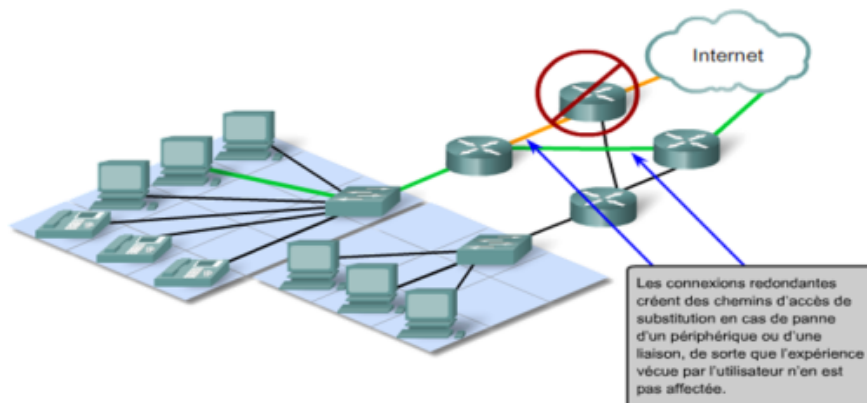
Pour être totalement fonctionnels et répondre aux besoins des utilisateurs, les réseaux doivent respecter quelques caractéristiques que nous décrivons dans cette section.

### 2.1 Tolérance aux pannes

La fréquence d'utilisation et la taille des réseaux soumettent les services disponibles en réseau à diverses pannes matérielles et/ou logicielles.

**Définition** Un réseau tolérant aux pannes est un réseau qui limite l'impact des pannes du matériel et des logiciels et qui peut être rétabli rapidement quand des pannes se produisent.

■ **Exemple** Pour pallier à des pannes de liaison entre deux organes du réseau, on peut mettre en place une redondance entre la source et la destination. Cela signifie qu'il y aura plusieurs chemins possibles pour joindre la destination depuis la source. En cas de défaillance d'une liaison (ou chemin) entre deux hôtes, des processus s'assurent que les messages sont routés (dirigés) sur un chemin différent et arrivent à bon port.



### 2.2 Evolutivité

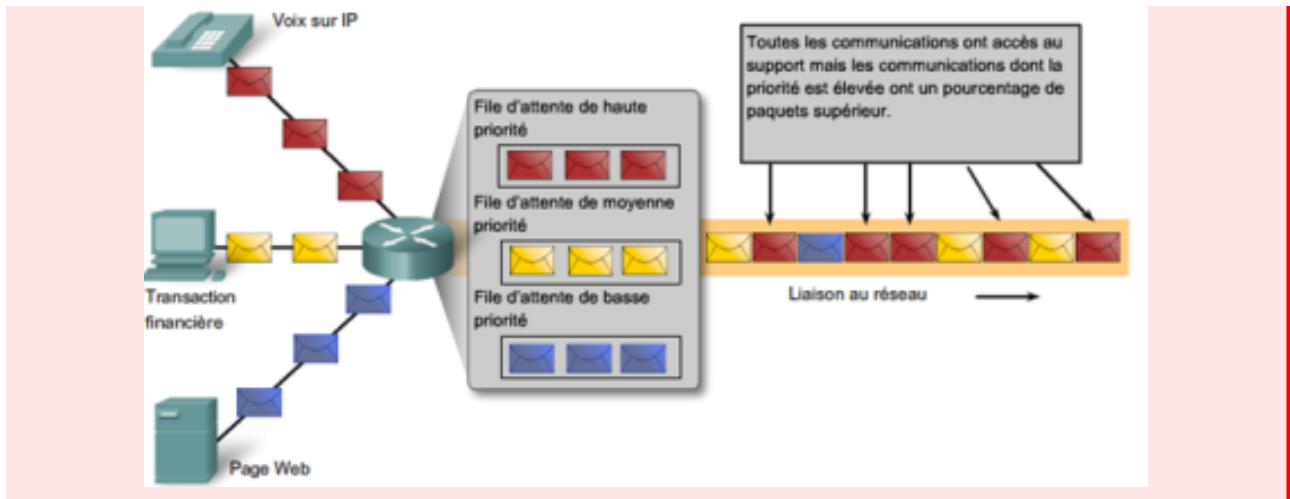
Le nombre croissant d'utilisateurs d'internet, l'évolution imprévisible d'une entreprise ou d'un organisme ou encore l'arrivée de matériel spécifique impose une évolution du réseau afin qu'il puisse répondre aux nouveaux besoins.

**Définition** Un réseau évolutif est en mesure de s'étendre rapidement afin de prendre en charge de nouveaux utilisateurs et de nouvelles applications sans que cela n'affecte les performances du service fourni aux utilisateurs existants.

### 2.3 Qualité de services

Les transmissions exigent des niveaux de qualités différents selon l'information qui circule. Par exemple, une transmission audio et vidéo exige un service ininterrompu et une qualité supérieure à l'envoi d'un simple mail.

**À retenir :** Sur un réseau, un niveau de priorité est défini pour chaque service en fonction de la qualité requise. Ainsi, plus un service exige une qualité importante, plus ses paquets seront prioritaires devant d'autre services.



## 2.4 Sécurité

En matière de sécurité des réseaux, deux points doivent être pris en considération pour éviter des conséquences graves : la sécurité de l'infrastructure réseau et la sécurité du contenu. En effet, les données qui transitent sur un réseau peuvent être plus ou moins sensibles (données bancaires par exemple) et doivent donc pouvoir être transmises en garantissant une certaine sécurité. Le réseau peut également subir des attaques malveillantes visant à le rendre hors service.

### À retenir :

- **Sécuriser l'infrastructure** réseau implique de **sécuriser matériellement et logiquement les périphériques qui assurent la connectivité du réseau** et d'empêcher tout accès non autorisé au logiciel de gestion qu'ils hébergent.
- **Sécuriser le contenu** consiste à protéger **les informations contenues dans les paquets transmis sur le réseau** ainsi que les informations stockées sur des périphériques reliés au réseau en les cryptant.

## 3 Elements d'un réseau



FIGURE 1: Périphériques et supports de transmissions

### 3.1 Les périphériques terminaux

**Définition** Les périphériques terminaux sont ceux qui envoient ou auxquels sont destinés les informations transitant sur le réseau.

■ Exemple

- Serveurs
- Ordinateurs
- Imprimantes
- Téléphones IP
- Smartphones
- Tablettes
- Télévisions
- ...

## 3.2 Les périphériques intermédiaires

**Définition** Ces périphériques assurent le bon acheminement des paquets sur le réseau tout en garantissant le respect des caractéristiques explicités dans la section 2

■ Exemple

- Commutateurs (utilisés pour interconnecter des réseaux locaux)
- Pare-feu (assure la sécurité du réseau)
- Routeur (contribue à orienter les messages transitant sur un réseau)
- Routeur sans fils (souvent présents dans les réseaux domiciles)
- ...

## 3.3 Les connexions

**Définition** Les connexions sont le support même du transfert d'informations. Ces connexions peuvent être filaires, sans-fil, optiques ou tout support capable de transporter une information.

Divers organismes de normalisation contribuent à la définition des propriétés physiques, électriques et mécaniques des supports disponibles pour différentes communications de données. Ces spécifications garantissent que les câbles et connecteurs fonctionnent comme prévu dans des conditions précises.

# 4 Topologies des réseaux

Afin de permettre à des éléments de communiquer, il est indispensable de les connecter entre eux. Il existe une multitude de connexions possibles.

**Définition** La **topologie physique** désigne la configuration spatiale du réseau. C'est la façon dont les organes sont connectés **physiquement**.

**Définition** La **topologie logique** désigne quant à elle la manière dont les données transitent dans les câbles.

## 4.1 Quelques topologies physiques classiques

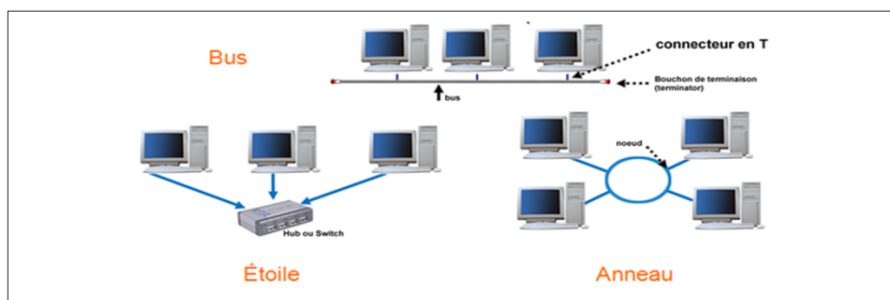


FIGURE 2: Trois exemples de topologies de réseau.

### 4.1.1 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 d'un câble, généralement coaxial. Le mot "bus" désigne la ligne physique qui relie les machines du réseau.

Cette topologie a pour avantages d'être **facile à mettre en oeuvre** et de fonctionner facilement, par contre elle est extrêmement **vulnérable** étant donné que si l'une des connexions est défectueuse, c'est l'ensemble du réseau qui est affecté.

Cette topologie est obsolète dans les réseaux de données mais couramment utilisé dans les réseaux de terrain (voitures ou automates par exemple).

### 4.1.2 Topologie en anneau

Dans un réseau en topologie en anneau, les ordinateurs sont reliés sur une boucle. Les ordinateurs doivent donc communiquer chacun à leur tour.

En réalité les ordinateurs d'un réseau en topologie anneau 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.

### 4.1.3 Topologie en étoile

Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel appelé switch (commutateur). Il s'agit d'une boîte comprenant un certain nombre de jonctions auxquelles on peut connecter les câbles en provenance des ordinateurs. Celui-ci a pour rôle d'assurer la communication entre les différentes jonctions. C'est la topologie la plus utilisée aujourd'hui.

Contrairement aux réseaux construits sur une topologie en bus, les réseaux suivant une topologie en étoile sont beaucoup moins vulnérables car on peut aisément retirer une des connexions en la débranchant du commutateur sans pour autant paralyser le reste du réseau.

## 5 Le modèle OSI

Au début des années 70, chaque constructeur a développé sa propre solution réseau autour d'architecture et de protocoles privés (SNA d'IBM, DECnet de DEC, DSA de Bull, TCP/IP du DoD,...) et il s'est vite avéré qu'il serait impossible d'interconnecter ces différents réseaux «propriétaires» si une norme internationale n'était pas établie. Cette norme établie par l'International Standard Organization (ISO) est la norme Open System Interconnection (OSI, interconnexion de systèmes ouverts).

Un système ouvert est un ordinateur, un terminal, un réseau, n'importe quel équipement respectant cette norme et donc apte à échanger des informations avec d'autres équipements hétérogènes et issus de constructeurs différents.

Le modèle de référence OSI est une représentation abstraite en couches servant de guide à la conception des protocoles réseau. Il divise le processus de réseau en sept couches logiques, chacune comportant des fonctionnalités uniques et se voyant attribuer des services et des protocoles spécifiques.

## 6 Adressage et encapsulation

### Nécessité d'un adressage

Lorsque deux organes sont connectés entre eux seuls, il est simple de savoir qui s'adresse à qui (il n'y a qu'un seul expéditeur et un seul destinataire possible selon le sens de communication). Par contre, lorsque plusieurs organes sont connectés sur le même réseau, il devient indispensable de savoir à qui s'adresse chaque paquet qui transite sur le réseau.

Le modèle OSI décrit des processus de codage, de mise en forme, de segmentation et d'encapsulation de données pour la transmission sur le réseau. Un flux de données envoyé depuis une source vers une destination peut être divisé en parties et entrelacé avec des messages transmis depuis d'autres hôtes vers d'autres destinations. À n'importe quel moment, des milliards de ces parties d'informations se déplacent sur un réseau. Il est essentiel que chaque donnée contienne les informations d'identification suffisantes afin d'arriver à bonne destination.

Il existe plusieurs types d'adresses qui doivent être incluses pour livrer correctement les données depuis une application source exécutée sur un hôte à l'application de destination correcte exécutée sur un autre. En utilisant le modèle OSI comme guide, nous apercevons les différents identificateurs et adresses nécessaires à chaque couche.

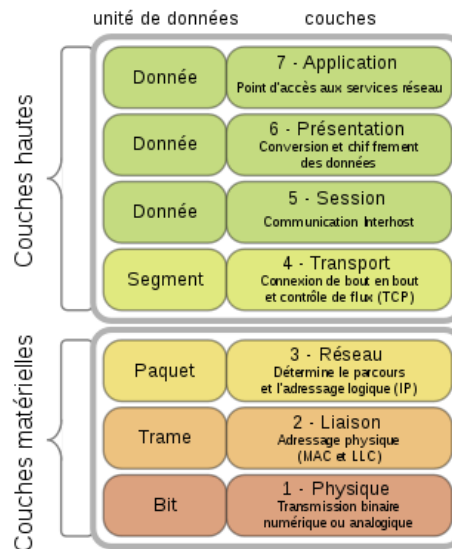


FIGURE 3: Les couches du modèle OSI

## 6.1 Protocole TCP/IP et analogies utiles

On s'intéresse dans cette partie aux couches 1 à 4 du réseau plus particulièrement. Ces couches permettent d'adresser et d'orienter un message vers la bonne application du bon destinataire. Les couches supérieures seront ici considérées comme un paquet de données.

Tout au long de cette section, une analogie sera faite avec l'envoi d'un courrier à une personne dans une entreprise.

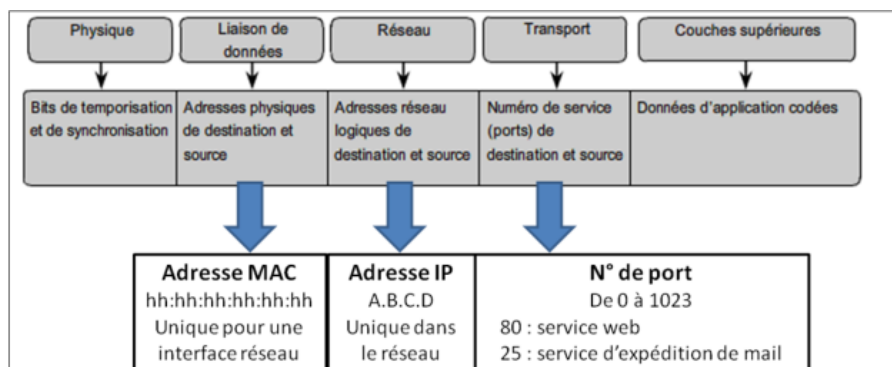


FIGURE 4: Principe de l'encapsulation des données

### 6.1.1 Les couches supérieures

Les couches supérieures (5 à 7) concernent les données, le message en tant que tel. Il s'agit donc **du contenu qui doit arriver à bon port**.

**R** Dans notre analogie, il s'agit ici du contenu de la lettre que nous souhaitons envoyer.

### 6.1.2 La couche de transport (TCP)

Cette couche détermine à quel service (port) **s'adressent les données**. Par exemple, par convention les données concernant les pages WEB sont envoyées sur le port 80 d'une machine.

**R** Dans notre analogie, il s'agit ici du service auquel nous nous adressons dans l'entreprise ou l'organisation (gestion des compte cantine des élèves par exemple).

### 6.1.3 La couche réseau (protocole IP)

Cette couche détermine **où doit être acheminée le paquet de données sur le réseau**. L'adresse IP est un identifiant unique sur le réseau permettant d'orienter le paquet vers le destinataire du message.

- R Dans notre analogie, il s'agit de l'adresse que l'on écrira sur l'enveloppe.

### 6.1.4 La couche Trame (adresse MAC)

L'adresse MAC identifie, de manière **unique** dans le monde, la machine destinataire du message.

- R Dans notre analogie, il s'agit de la personne précise s'occupant de la requête. On peut voir l'adresse IP comme l'identifiant de sécurité sociale, unique en France.

### 6.1.5 La couche physique

Il s'agit ici de la façon pour les données de transiter sur le réseau (bits de temporisation, synchronisation des signaux, *etc.*)

- R Dans notre analogie, ce serait le service de courrier en lui même, avec son architecture d'acheminement (camions, centre de tri, ...)

## 6.2 L'encapsulation des données

Toutes les informations présentées dans la partie précédentes sont indispensables au bon acheminement d'un paquet. De la même façon qu'un courrier est encapsulé dans une enveloppe sur laquelle sont écrites les informations d'adressage, les paquets internet sont encapsulé dans un message de la couche supérieur contenant les informations indispensables (voir Figure 5).

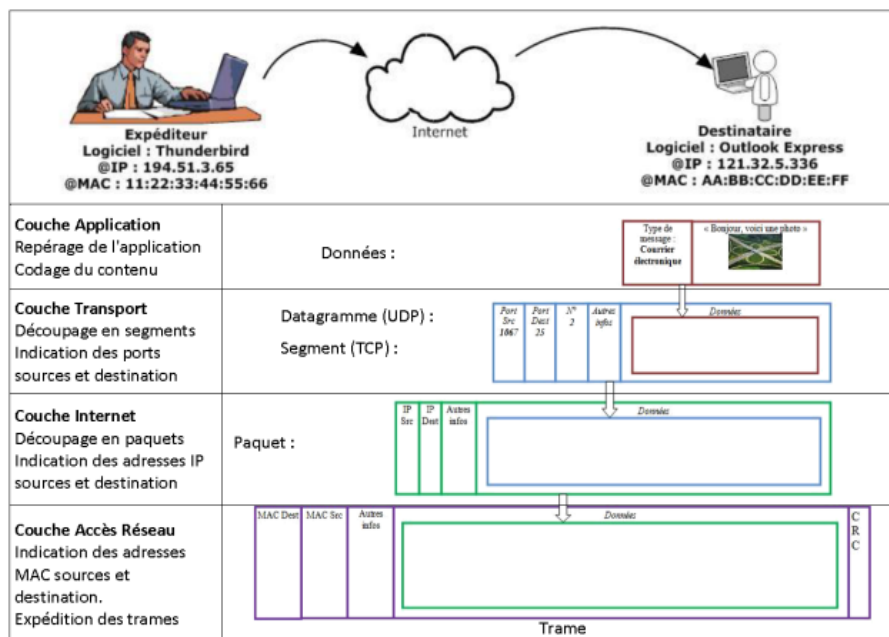


FIGURE 5: Exemple d'encapsulation de données