

1 Vivre dans un monde en réseau : un peu d'histoire

Depuis toujours, la transmission d'informations entre les personnes est un enjeu majeur. Autrefois réservé aux domaines militaires et diplomatiques, elle a pris une place de plus en plus importante au cours du temps et les moyens de transmission n'ont eu de cesse de s'améliorer grâce aux avancées et aux innovations technologiques.

1.1 Quelques repères historiques

- ★ 15^{ème} siècle : les tours génoises utilisaient le feu pour transmettre des signaux ;
- ★ fin 18^{ème} siècle : le sémaphore des frères Chappe est le premier télégraphe permettant d'envoyer des messages codés. Il s'agit d'un système à bras articulés dont le premier essai entre Paris et Lille eu lieu en 1794 et permit de transmettre un message en une dizaine de minutes. A une position des bras est associée un nombre entier compris entre 1 et 92 et à chaque couple de nombres est associé un mot français (soit un vocabulaire de 8464 mots).



FIGURE 1 – Tour génoise (à gauche) et télégraphe Chappe (à droite)

- ★ 19^{ème} siècle : avènement des transmissions électriques utilisées dans le télégraphe et le téléphone :
 - 1832 : télégraphe électrique de Morse ;
 - 1876 : invention du téléphone par Graham Bell.

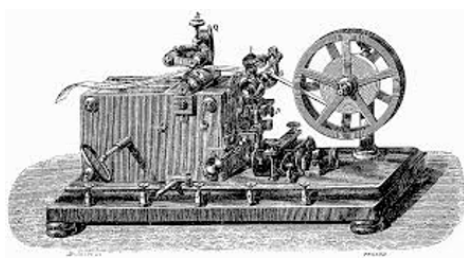


FIGURE 2 – Télégraphe de Morse (à gauche) et téléphone de Bell (à droite)

- ★ 20^{ème} siècle : avènement du transistor, des ordinateurs et d'internet :
 - 1948 : invention du transistor ;
 - 1969 : invention d'Arpanet, l'ancêtre d'internet ;
 - 1981 : invention du minitel en France ;
 - 1983 : naissance d'Internet avec le protocole TCP/IP ;
 - 1990 : démocratisation d'internet avec l'invention du web.

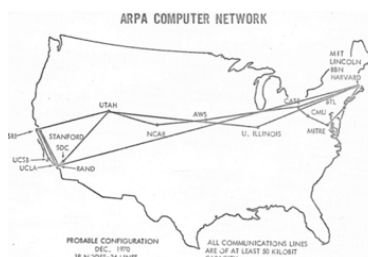


FIGURE 3 – Arpanet (à gauche) et le minitel (à droite)

1.2 Réseaux de communication

Les moyens de communication dont nous nous servons actuellement pour partager idées et informations changent et évoluent sans cesse. Chaque innovation les a développés et améliorés.

Autrefois séparés et bien distincts, avec des technologies différentes, ils convergent maintenant sur une plateforme commune. Les progrès technologiques nous permettent aujourd'hui de réunir ces réseaux disparates (informatique, téléphonie, diffusion, etc.) sur une même plateforme appelée *réseau convergent*.

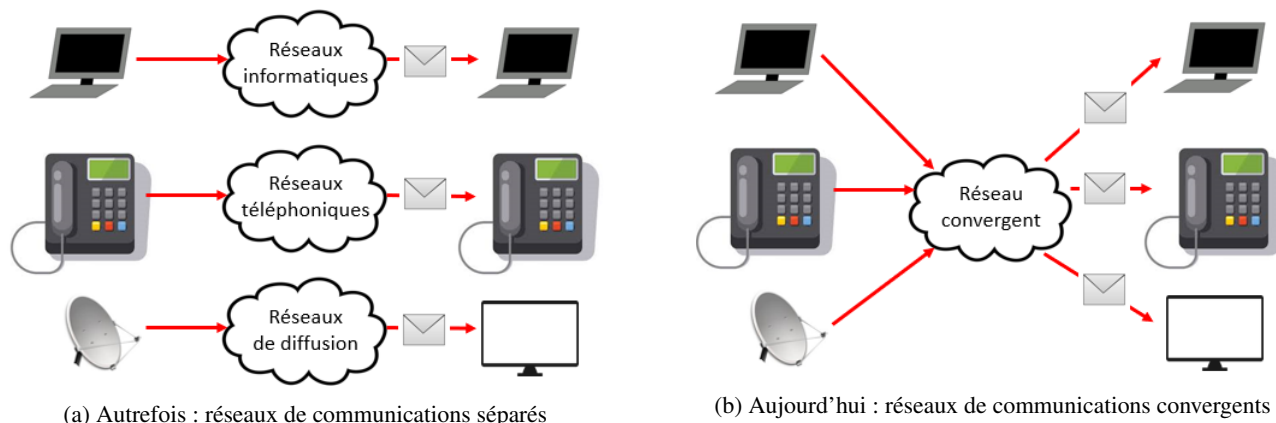


FIGURE 4 – Différence entre les réseaux de communications d'autrefois et d'aujourd'hui

À l'image de tous les progrès dans le domaine des technologies de la communication, la création et l'interconnexion de réseaux de données ont un profond impact sur la société. Par exemple, au cours d'une seule journée, les ressources disponibles sur Internet peuvent nous aider à :

- ★ choisir en ligne ce que nous allons porter en fonction des conditions météorologiques du jour ;
- ★ déterminer le trajet le moins embouteillé en visualisant les vidéos du trafic routier et des conditions météo transmises par les webcams ;
- ★ consulter notre compte bancaire et payer nos factures en ligne ;
- ★ recevoir et envoyer des courriels ou passer un appel téléphonique via Internet de quasiment partout ;
- ★ rechercher des informations médicales et obtenir des conseils nutritionnels d'experts du monde entier, puis publier un message sur un forum pour partager des renseignements sur une maladie ou un traitement ;
- ★ télécharger de nouvelles recettes pour préparer un Tiramisu mémorable ;
- ★ publier des photographies, vidéos personnelles et expériences et les partager avec des amis ou avec le monde entier.

2 Connexion et protocoles

Avant de commencer à communiquer, il faut établir des règles, ou conventions, qui régissent les communications. Ces règles ou *protocoles* doivent être respectés pour que le message soit correctement transmis et compris. Pour un déroulement correct des communications, on peut avoir comme protocoles :

- ★ l'identification de l'expéditeur et du destinataire ;
- ★ le recours à une méthode de communication convenue (face-à-face, téléphone, lettre, photographie) ;
- ★ l'utilisation d'une langue et d'une syntaxe communes ;
- ★ la vitesse et le rythme d'élocution ;
- ★ la demande de confirmation ou d'accusé de réception.



(a) Etape 1 : se mettre d'accord sur la méthode à utiliser pour communiquer



(b) Etape 2 : se mettre d'accord sur le langage à utiliser pour se comprendre



(c) Etape 3 : transmettre le message et accuser réception

FIGURE 5 – Exemple de protocoles de communication

Concernant les communications humaines, il existe de nombreux protocoles dont un certain nombre sont implicites ou intégrés à notre culture. En revanche, lorsqu'on construit des réseaux de données, il faut être beaucoup plus explicites sur la façon dont la communication s'effectuera et sur ce qui en assurera le succès.

3 Éléments physiques d'un réseau de données

3.1 Périphériques et connexions

Un réseau est un ensemble de *périphériques* et de *connexions* qui permettent à chaque périphériques de communiquer avec tous les autres, éventuellement en passant par des intermédiaires.

- ★ les périphériques (deux types) :
 - les périphériques *terminaux* : serveurs, ordinateurs, imprimantes, téléphones, voitures
 - les périphériques *intermédiaires* : concentrateurs (switch), routeurs, boxs
- ★ les connexions :
 - filaires (câble droit, croisé, téléphonique, série, etc.)
 - sans-fil (WiFi, GSM, GPRS, Bluetooth, 4G, 5G, etc.)
 - optique (fibre monomode, multimode, etc.)

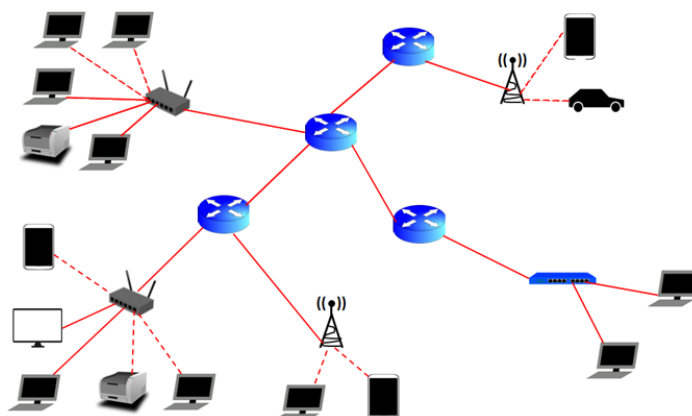


FIGURE 6 – Exemple de réseau de données

3.2 Topologie des réseaux

La manière dont sont interconnectées les machines est appelée *topologie*. On distingue deux types de topologie :

- ★ la *topologie physique* qui représente la configuration spatiale et visible du réseau ;
- ★ la *topologie logique* qui représente la manière dont les données transitent dans les câbles.

Les principales topologies physiques sont les topologies en bus, en étoile et en anneau.

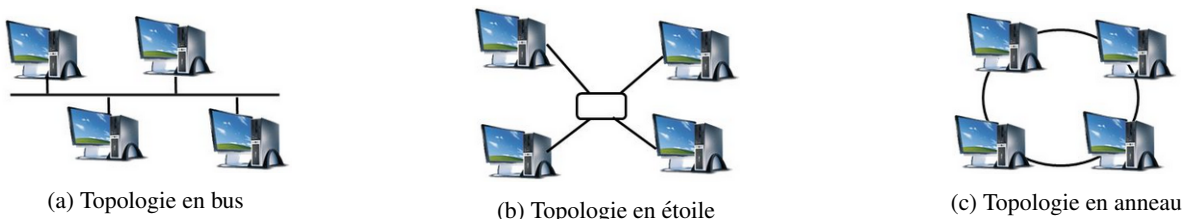


FIGURE 7 – Les principales topologies physiques d'un réseau

- ★ *Topologie en bus* : une topologie en bus est l'organisation la plus simple d'un réseau. Le mot « bus » désigne la ligne physique qui relie les machines du réseau. Cette topologie a pour avantages d'être facile à mettre en œuvre 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.
- ★ *Topologie en étoile* : dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel, le plus souvent un switch. 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. 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 switch sans pour autant paralyser le reste du réseau. C'est cette topologie qui est la plus couramment utilisée dans les réseaux de données.
- ★ *Topologie en anneau* : dans un réseau en topologie en anneau, les ordinateurs communiquent chacun à leur tour, on a donc une boucle d'ordinateurs (reliés à un répartiteur (appelé MAU, Multistation Access Unit) = sur laquelle chacun d'entre eux va « avoir la parole » successivement.

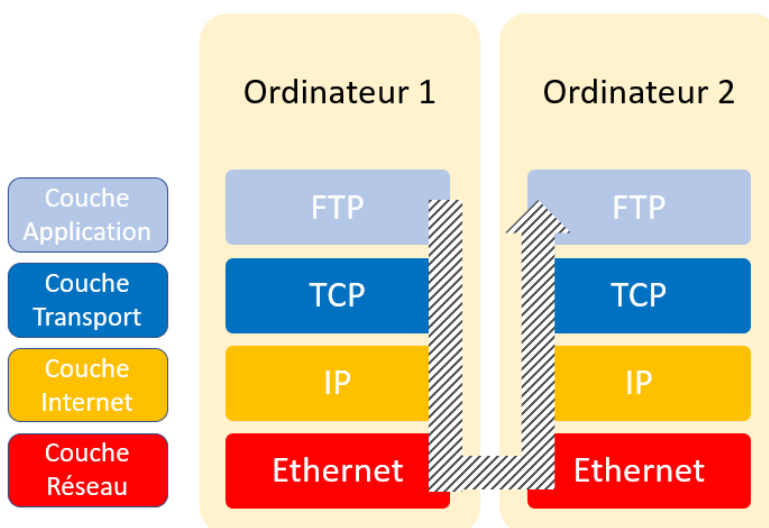
4 Les couches réseau

4.1 Le modèle TCP/IP

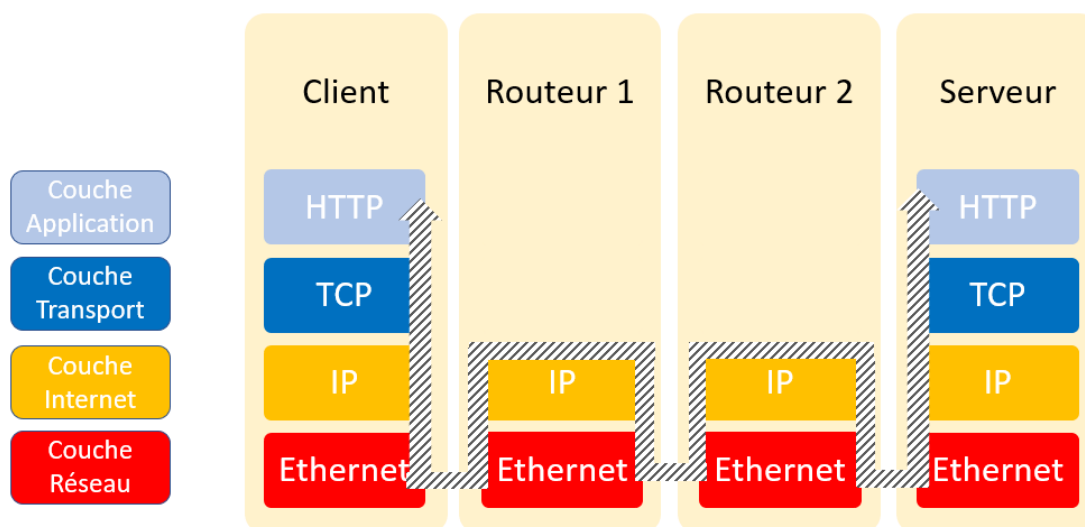
Les machines d'un réseau n'ont pas à être identiques (différence de systèmes d'exploitations, de logiciels, etc.) et ces différences ne doivent pas avoir le moindre impact sur la communication entre deux machines. Pour cela, il a fallu inventer un certain nombre de standards réseau appelés *protocoles réseaux*. Chacun de ces protocoles gère des choses aux noms bizarres, comme le routage, la transmission des bits, l'adressage logique ou physique, etc. Cependant, tous ces protocoles ne se situent pas au même « niveau d'abstraction ». En effet, standardiser le codage des bits dans un câble réseau est plus proche de la machine que la gestion du routage.

Ces différents niveaux d'abstraction sont classés en *couches réseau*. Rapidement dit, une couche réseau définit un ensemble de protocoles qui ont des fonctions similaires. Par exemple, la couche transport va rassembler tous les protocoles standardisant la façon d'empaqueter les données à transmettre et la façon de coordonner l'expéditeur et le destinataire de paquets afin d'assurer la fiabilité de leur transport de bout en bout.

Il existe différents modèles de classification. Parmi les plus classiques, on a le *modèle OSI* en sept couches qui est le plus complet, mais le plus difficile à manipuler, et le *modèle TCP/IP* en quatre couches auquel nous nous intéressons dans ce cours. Les deux figures ci-dessous modélisent la communication entre deux machines suivant le modèle TCP/IP lorsque celles-ci sont situées dans un même réseau local (figure 8a), et à travers deux routeurs (figure 8b). Dans ces deux figures, des exemples de protocoles sont indiqués pour chaque couche.



(a) Parcours des données lors d'une communication Internet sur un réseau local (exemple d'un transfert de fichier)



(b) Parcours des données lors d'une communication Internet à travers deux routeurs (exemple du chargement d'une page web)

FIGURE 8 – Modèle TCP/IP de communication

4.2 Encapsulation et décapsulation des données

Durant le passage d'une couche à l'autre, il y a un phénomène d'*encapsulation* et de *décapsulation* des données comme le montre la figure ci-dessous. Pour chaque couche, on a repris les exemples des protocoles donnés à la figure 8.

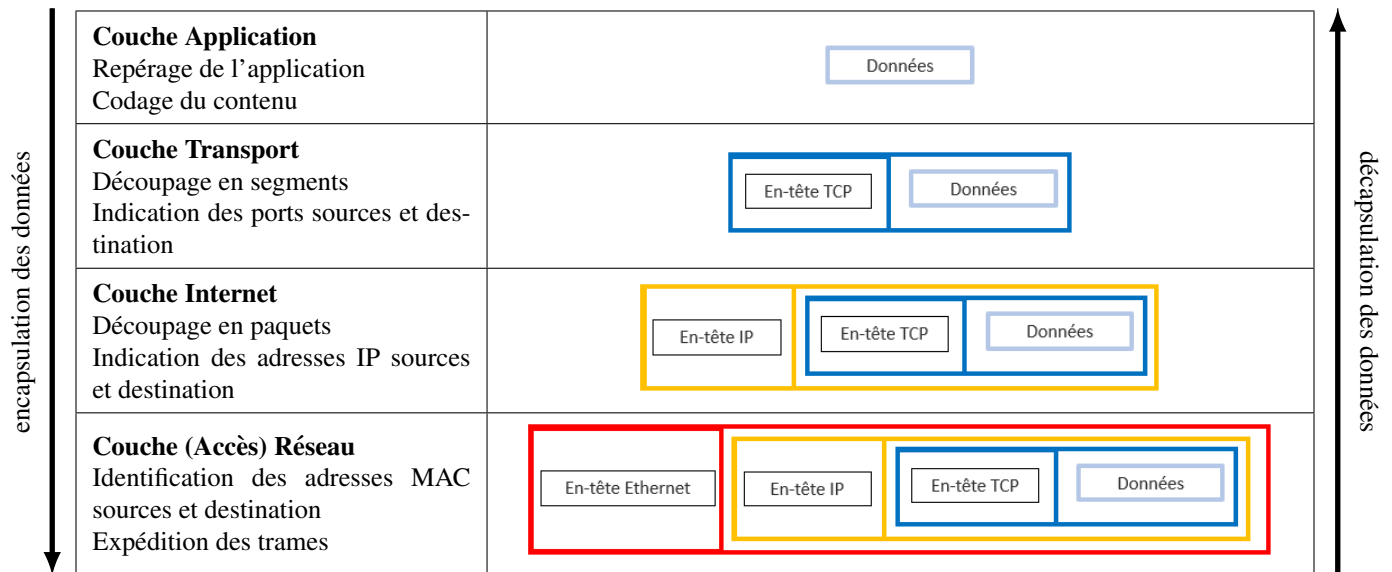


FIGURE 9 – Encapsulation et décapsulation des données suivant les couches

Des normes régissent les rôles de chaque couche, leurs interactions et les spécifications de chaque protocole. Ces normes permettent au réseau Internet de fonctionner à l'échelle mondiale et assurent la modularité du système : il est possible de modifier les protocoles à l'œuvre au sein d'une couche, sans modifier les protocoles des autres couches, et le système continue à fonctionner dans son ensemble. Cette modularité est analogue au fait de pouvoir changer un composant matériel d'un ordinateur, par exemple sa carte graphique, sans devoir rien changer d'autre. Cette modularité est essentielle pour permettre au système d'évoluer.

5 Couches réseau et protocoles

Un *protocole* est un ensemble de règles qui régissent la transmission d'informations sur un réseau. Il existe de nombreux protocoles, chacun spécialisé dans une tâche bien précise.

5.1 Protocoles de la couche Application

Cette couche est le point d'accès aux services réseaux et regroupent la plupart des programmes réseaux. Les protocoles qui se situent dans cette couche sont de haut niveau et sont associés à ces programmes (FTP, SMTP, HTTP, DNS, etc.). Cette couche devra choisir un protocole de transport adapté au service demandé.

5.2 Protocoles de la couche Transport

Les protocoles de la couche transport sont responsables de l'empaquetage des données à transmettre, ainsi que de la coordination entre l'envoyeur et le destinataire des paquets, pour assurer la fiabilité de leur transport de bout en bout.

Le protocole le plus connu est TCP (*Transmission Control Protocol*). Il se charge de la communication entre les applications, c'est-à-dire entre les logiciels utilisés par les ordinateurs. En effet quand on envoie un paquet IP sur Internet, il passe par des dizaines d'ordinateurs, et il peut arriver que des paquets IP se perdent ou arrivent en double exemplaire. Cela peut être gênant : imaginons un ordre de débit sur notre compte bancaire arrivant deux fois ou un ordre de crédit perdu ! Même si le paquet arrive à destination, rien ne vous permet de savoir si le paquet est bien arrivé (aucun accusé de réception).

Il vérifie donc que le destinataire est prêt à recevoir les données, puis il fractionne les messages en paquets plus petits (les paquets IP ont une taille limitée d'environ 1500 octets) et numérote les paquets. A la réception, il vérifie que tous les paquets sont bien arrivés et peut redemander les paquets manquants. Il réassemble ensuite les paquets avant de les transmettre aux logiciels, puis envoie des accusés de réception pour prévenir l'expéditeur que les données sont bien arrivées.

Exemple. La figure ci-dessous montre comment le protocole TCP procède pour envoyer le message « Salut, comment ça va ? » :

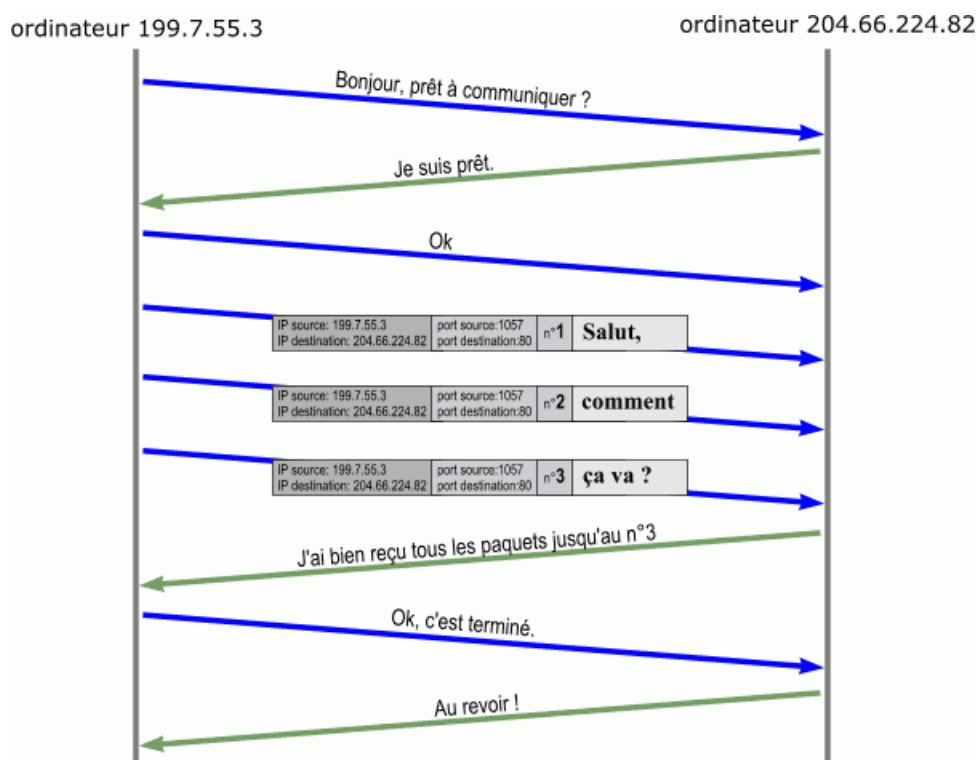


FIGURE 10 – Exemple de fonctionnement du protocole TCP (chaque flèche représente un paquet IP)

A l'arrivée, sur l'ordinateur 204.66.224.82, le protocole TCP reconstitue le message « Salut, comment ça va ? » à partir des trois paquets IP reçus et le donne au logiciel qui est sur le port 80.

5.3 Protocoles de la couche Internet

Les protocoles de la couche Internet sont responsables de l'aiguillage de chaque paquet vers sa destination, à chaque embranchement entre différents supports physiques rencontrés. Ces protocoles doivent également identifier les ordinateurs connectés sur le réseau. Le plus connu des protocoles de la couche Internet est le protocole IP (*Internet protocol*) qui utilise les adresses IP des différentes machines connectées au réseau.

5.3.1 Adresses IP

Chaque machine possède une adresse logique, appelée *adresse IP*, permettant de l'identifier sur un réseau. Celle-ci n'est pas associée de manière durable à un ordinateur : quand un ordinateur est remplacé par un autre, le nouveau peut hériter de l'adresse IP de l'ancien ; à l'inverse, si un ordinateur est déplacé d'un lieu à un autre, il change d'adresse IP.

Format d'une adresse IP. Une adresse IP classique (format IPv4) est un mot de 32 bits écrits sous forme d'un quadruplet de nombres compris entre 0 et 255 et séparés par un point. Par exemple, l'adresse IP

1010 1100 . 0001 0000 . 1000 0101 . 0001 0100

est exprimée en format décimal pointé de la manière suivante : 172.16.133.20

Constitution d'une adresse IP. Une adresse IP est constituée de deux parties :

- * une partie *réseau* permettant d'identifier le réseau local dans lequel se situe la machine ;
- * une partie *hôte* permettant d'identifier la machine dans le réseau local.

Par exemple, pour l'adresse 172.16.133.20 précédente, on a écrit ci-dessous en bleu les bits de la partie réseau et en rouge les bits de la partie hôte :

1010 1100 . 0001 0000 . 1000 0101 . 0001 0100

On en déduit en particulier que l'adresse réseau est 172.16.128.0 et que l'adresse de la partie hôte est 0.0.5.20.

5.3.2 Masque de sous-réseau

Pour définir les parties réseau et hôte d'une adresse, les périphériques utilisent une configuration de 32 bits appelée *masque de sous-réseau*. Le masque de sous-réseau s'exprime dans le même format décimal pointé que celui de l'adresse IPv4.

Pour déterminer la partie réseau et la partie hôte dans une adresse IP donnée à partir d'un masque de sous-réseau également donné, on procède de la manière suivante :

- * on écrit l'adresse IP et le masque de sous-réseau en binaire ;
- * on applique un ET binaire bit à bit entre les deux mots binaires :
 - le mot binaire obtenu donne la partie réseau et donc définit l'adresse réseau du réseau local de la machine (on remarque que les bits utilisés dans l'adresse IP initiale sont ceux qui correspondent aux bits égaux à 1 dans le masque de sous-réseau) ;
 - le mot binaire obtenu à l'aide des bits restants, c'est-à-dire ceux de l'adresse IP initiale qui n'ont pas été utilisés par la partie réseau (ce sont donc les bits de l'adresse IP initiale qui correspondent aux bits égaux à 0 dans le masque de sous-réseau) donne la partie hôte.

L'exemple illustre le calcul de l'adresse réseau et la partie hôte pour l'adresse IP 172.16.133.20 lorsque le masque de sous-réseau utilisé est 255.255.192.0.

Adresse IP en binaire :	1010 1100 . 0001 0000 . 1000 0101 . 0001 0100
Masque en binaire :	1111 1111 . 1111 1111 . 1100 0000 . 0000 0000
Adresse du sous-réseau en binaire :	1010 1100 . 0001 0000 . 1000 0000 . 0000 0000
Partie hôte en binaire :	0000 0000 . 0000 0000 . 0000 0101 . 0001 0100

On en déduit que l'adresse du sous-réseau est 172.16.128.0 et que la partie hôte est 0.0.5.20. On en déduit également que les adresses IP possibles dans ce réseau local sont, en binaire, de la forme

1010 1100 . 0001 0000 . 10** **** . **** ****

où le symbole * est soit 0, soit 1. Ainsi, la première adresse possible est obtenue en remplaçant tous les symboles * par 0, soit 172.16.128.0, et la dernière adresse possible est obtenue en remplaçant tous les symboles * par 1, soit 172.16.191.255. Ces deux adresses sont réservées : la première est celle du réseau local et la dernière est l'adresse de diffusion ou Broadcast (elle sert à envoyer à tout le réseau). Ainsi, l'adresse du premier hôte s'obtient en remplaçant tous les symboles * par 0 sauf celui du bit de poids faible qui est remplacé par 1, soit 172.16.128.1, et l'adresse du dernier hôte s'obtient en remplaçant tous les symboles * par 1 sauf celui du bit de poids faible qui est remplacé par 0, soit 172.16.192.254. Il y a donc en tout la possibilité de mettre $2^{14} - 2 = 16\,382$ hôtes dans ce sous-réseau.

5.3.3 Notation CIDR

Une forme plus courte pour les adresses IP est connue sous le nom de *notation CIDR* (Classless Inter-Domain Routing). Elle donne l'adresse IP suivie par une barre oblique (ou slash, « / ») et le nombre de bits consécutifs égaux à 1 dans la notation binaire du masque de sous-réseau, les autres bits valant 0.

Ainsi, dans l'exemple précédent, la masque 255 . 255 . 192 . 0 admettant 18 bits égaux à 1, l'adresse IP 172 . 16 . 133 . 20 s'écrit plus simplement 172 . 16 . 133 . 20/18.

5.3.4 Passerelle par défaut

Au sein d'un même réseau, les hôtes communiquent entre eux sans nécessiter de périphérique intermédiaire. En revanche, quand un hôte doit communiquer avec un autre réseau, un périphérique intermédiaire, appelé *routeur*, sert de passerelle avec l'autre réseau.

Le rôle d'un routeur est de décider, à partir de l'adresse du sous-réseau de destination, quel chemin doit prendre le paquet qu'il reçoit et donc de choisir vers quel autre routeur envoyer le paquet jusqu'à ce que la destination soit atteinte. Pour prendre sa décision, le routeur utilise une table de routage qui sert d'aiguillage : *pour telle destination, envoyer le paquet à mon routeur voisin de droite, pour telle autre destination envoyer le paquet à mon routeur voisin de gauche*, et ainsi de suite. Les tables de routages sont gérées par des algorithmes fondés sur des échanges entre les routeurs.

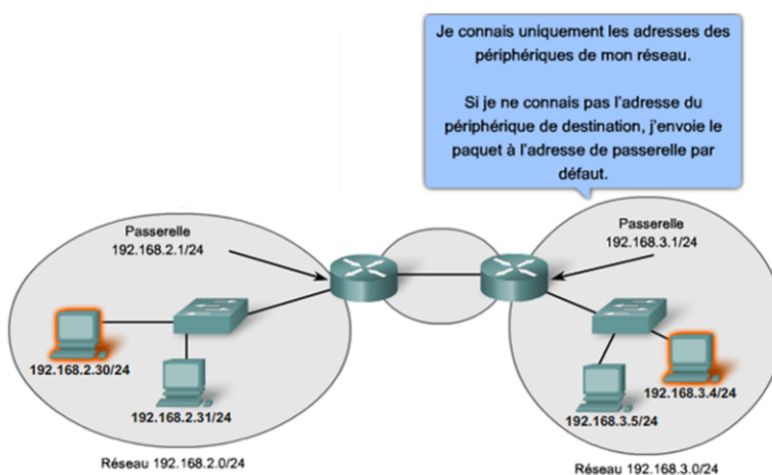


FIGURE 11 – Exemple de passerelles entre deux sous-réseaux

Les transmissions de paquets dans le réseau ne sont pas garanties d'arriver à destination : un paquet peut être perdu en chemin en cas de panne d'un routeur ou une ligne de transmission. Il est aussi possible qu'un paquet prenne un itinéraire qui s'avère inefficace ou tourne dans un cycle du réseau.

5.4 Protocoles de la couche (Accès) Réseau

Les protocoles de la couche (Accès) Réseau sont classiquement séparés en deux catégories :

1. les protocoles responsables de la coordination du transfert de trames (suite de bits structurés selon un certain format et destinée à être échangée sur le réseau) à travers un support physique, de l'identification des ordinateurs directement connectés à ce support et de la gestion du « temp de parole » de chacun sur ce support. L'identifiant est une interface identifiée par une adresse MAC constituée de 48 bits et généralement représentée sous la forme hexadécimale en séparant les six octets par un double point ou un tiret (par exemple : 5E:FF:56:A2:AF:15. Contrairement aux adresses IP, une adresse MAC est unique et durable car elle est attribuée à chaque carte réseau au moment de sa fabrication. Comme exemples typiques de ce type de protocoles, on a les protocoles Wifi, Ethernet ou Bluetooth.
2. les protocoles chargés de la communication des bits entre deux ordinateurs reliés par un câble ou par lien radio. Il existe plusieurs types de support physiques pour connecter les ordinateurs entre eux :
 - ★ des câbles métalliques véhiculant des électrons ;
 - ★ des câbles optiques véhiculant des photons ;
 - ★ le vide véhiculant des ondes radio.

Pour chacun de ces supports, il existe des protocoles spécialisés.

5.5 Quelques exemples de protocoles

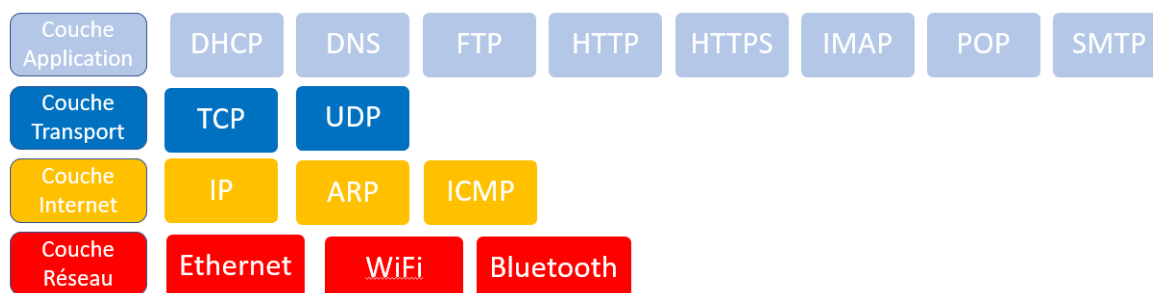


FIGURE 12 – Exemple de protocoles dans le modèle TCP/IP