République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

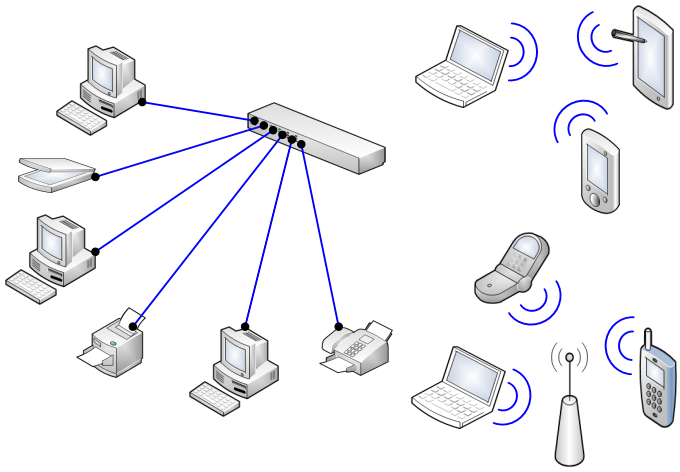
Université A. MIRA de Béjaia

Faculté des Sciences Exactes

Département d'Informatique

Polycopié de Cours Réseaux

Préparé par : Prof. Mohand YAZID



Année Universitaire 2023-2024

Préface

Ce polycopié de cours est organisé en 04 chapitres comme suit :

- Le premier chapitre présente des généralités sur les Réseaux Informatiques, à savoir : la définition, les objectifs, les topologies, et la classification des réseaux.
- Le deuxième chapitre décrit les trois concepts de base permettant de mettre en œuvre les communications au sein des Réseaux Informatiques, à savoir : l'adressage IP, le système de noms de domaine DNS, et le numéro de port.
- Le troisième chapitre est consacré à la présentation du modèle en couches TCP/IP le plus répandu dans les Réseaux Informatiques. En particulier, les deux célèbres protocoles TCP et IP seront détaillés.
- Le quatrième et le dernier chapitre est dédié aux réseaux locaux. La couche physique et les deux sous-couches MAC et LLC sont particulièrement étudiées. Quelques types de réseaux locaux sont également décrits.

Table des matières

Table des figures

Liste des tableaux

Chapitre 1

Introduction aux réseaux informatiques

1.1 Concept et définition d'un 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, nous parlerons parfois de : réseau de **transport**, réseau **téléphonique**, réseau de **neurones**, réseau de **malfaiteurs**, et enfin de réseau **informatique** Pillou [2015].

Un **Réseau Informatique** est un 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) Pillou [2015].

Dans ce présent support de cours, nous nous intéresserons bien évidemment aux Réseaux Informatiques.

1.2 Objectifs 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 objectifs différents :

- 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.

Par ailleurs, les réseaux permettent aussi de standardiser les applications, telles que : la messagerie électronique et les agendas de groupe qui permettent de communiquer plus efficacement et plus rapidement Pillou [2015].

1.3 Topologies 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** Servin [2003]. Nous distinguons généralement les topologies suivantes :

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

Par opposition à la topologie physique, la **topologie logique** représente la façon dont les données transitent dans les lignes de communication. Les topologies logiques les plus courantes sont Ethernet, Token Ring et Token Bus Servin [2003]. Ces dernières seront présentées dans le chapitre 4.

Dans ce qui suit, nous allons nous intéresser à la présentation de quelques unes des topologies physiques citées ci-dessus :

1.3.1 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 câbles, généralement de type coaxial. Le mot « bus » désigne la ligne physique qui relie les machines du réseau (voir Figure 1.1).

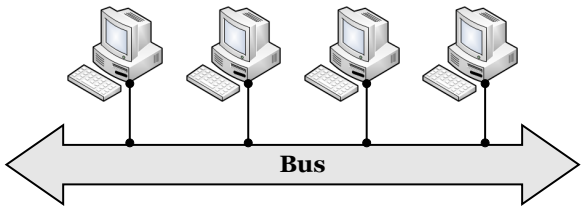


FIGURE 1.1: *Topologie en bus.*

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 tombe en panne, l'ensemble du réseau en est paralysé.

1.3.2 Topologie en étoile

Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel central appelé concentrateur ou hub (voir Figure 1.2). 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.

Contrairement aux réseaux construits sur une topologie en bus, les réseaux suivant une topologie en étoile sont beaucoup plus fiable car une des connexions peut être défectueuse sans paralyser le reste du réseau. L'inconvénient 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 coûteux qu'un réseau à topologie en bus car un matériel supplémentaire est nécessaire (le concentrateur).

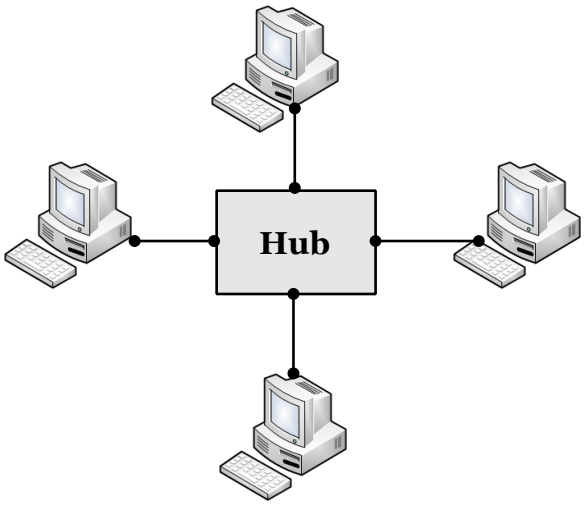


FIGURE 1.2: *Topologie en étoile.*

1.3.3 Topologie en anneau

Dans un réseau possédant une topologie en anneau, les ordinateurs sont théoriquement situés sur une boucle et communiquent chacun à son tour (voir Figure 1.3).

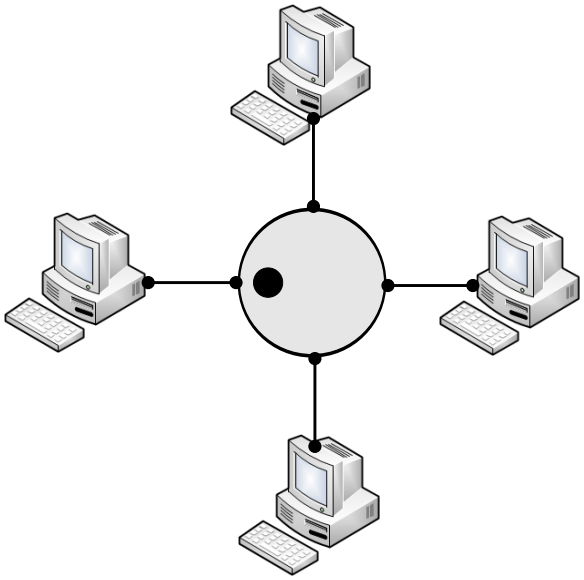


FIGURE 1.3: *Topologie en anneau.*

Les ordinateurs sont en réalité reliés à un répartiteur qui va gérer la communication entre eux en attribuant à chacun un « temps de parole ».

1.4 Modes de fonctionnement d'un réseau

En élargissant le contexte de la définition du réseau aux services qu'il apporte, il est possible de distinguer deux modes de fonctionnement Pujolle [2008] :

- le mode de fonctionnement **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,
- le mode de fonctionnement de type **client-serveur**, où un ordinateur (serveur) fournit des services réseau aux ordinateurs clients.

1.4.1 Mode de fonctionnement d'égal à égal

Dans une architecture d'égal à égal, 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.

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

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

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 d'installation et de mise en œuvre.

1.4.2 Mode de fonctionnement 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, une machine généralement très puissante en terme de capacités d'entrée-sortie, qui leur fournit des services. Ces services sont des programmes fournissant des données telles que l'heure, des fichiers, une connexion, etc.

Les services sont exploités par des programmes, appelés programmes clients, s'exécutant sur les machines clientes. Nous parlons ainsi de client FTP (File Transfer Protocol), client de messagerie, etc. 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).

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, 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.

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 seul maillon faible du réseau client/serveur, étant donné que tout le réseau est conçu autour de lui. Heureusement, le serveur a une grande tolérance aux pannes (notamment grâce à la redondance de données).

1.5 Classification des réseaux

On distingue différentes classes de réseaux selon leur taille (en terme de nombre de machines), leur vitesse de transfert des données ainsi que leur étendue. On définit généralement les catégories de réseaux suivantes Servin [2012] :

- **Réseaux corporels** ou BAN (Body Area Network).
- **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 Pillou [2015].

1.5.1 Réseaux corporels (BAN)

Les réseaux corporels (BAN, Body Area Network) est une nouvelle classe de réseau informatique qui consiste à interconnecter sur, autour ou dans le corps humain de minuscules dispositifs pouvant effectuer des mesures (capteurs) ou agir de façon active (actionneurs).

Ces capteurs très miniaturisés, disposant d'une grande autonomie et utilisant des courants de très faible puissance peuvent être capables de dialoguer avec un centre de service distant, pour alerter un service d'urgences hospitalières par exemple.

Les principales applications se trouvent dans les domaines de la santé, des premiers secours, du militaire, etc. La technologie la plus adaptée pour configurer un réseau BAN est le Zigbee.

1.5.2 Réseaux personnels (PAN)

Un réseau personnel (PAN, Personal Area Network) désigne une classe de réseau restreinte en terme d'équipements, généralement mis en œuvre dans un espace d'une dizaine de mètres. D'autres appellations pour cette classe de réseau sont : réseau domestique ou

réseau individuel.

Les technologies utilisées les plus courantes pour la mise en œuvre d'un réseau PAN sont le Bluetooth, l'infrarouge (IR), ou le Zigbee.

1.5.3 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 zone géographique par un réseau, souvent à l'aide d'une même technologie (Ethernet ou WIFI).

La vitesse de transfert de données d'un réseau local peut aller de 10 Mbps (pour un réseau Ethernet standard) à 1 Gbps (Gigabit Ethernet par exemple). La taille d'un réseau local peut atteindre jusqu'à 100 voire 1 000 machines.

1.5.4 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).

1.5.5 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.

Chapitre 2

Protocoles des réseaux informatiques

2.1 Notion de protocole

Un protocole est une méthode standard qui permet la communication entre des processus (s'exécutant éventuellement sur différentes machines), c'est-à-dire un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau Pillou [2015]. Il en existe plusieurs selon ce que l'on attend de la communication. Certains protocoles sont par exemple spécialisés dans l'échange de fichiers (le FTP), d'autres servent à gérer simplement l'état de la transmission et des erreurs (c'est le cas du protocole ICMP), etc.

On distingue généralement deux catégories de protocoles selon le niveau de contrôle des données que l'on désire Pillou [2015] :

- Les **protocoles orientés connexion** : il s'agit des protocoles opérant un contrôle de transmission des données pendant une communication établie entre deux machines. Dans un tel schéma, la machine réceptrice envoie des accusés de réception lors de la communication, ainsi la machine émettrice est garante de la validité des données qu'elle envoie. TCP (Transmission Control Protocol) est un protocole orienté connexion.
- Les **protocoles non orientés connexion** : il s'agit d'un mode de communication dans lequel la machine émettrice envoie des données sans prévenir la machine récep-

trice, et la machine réceptrice reçoit les données sans envoyer d'accusé de réception à la première. UDP (User Datagram Protocol) est un protocole non orienté connexion.

2.2 Adressage IP

Sur Internet, les ordinateurs communiquent entre eux grâce au protocole IP (Internet Protocol), qui utilise des adresses numériques, appelées **adresses IP**. C'est l'ICANN (Internet Corporation for Assigned Names and Numbers, remplaçant l'IANA, Internet Assigned Numbers Agency, depuis 1998) qui est chargée d'attribuer des adresses IP publiques, c'est-à-dire les adresses IP des ordinateurs directement connectés sur le réseau public Internet Lohier and Quidelleur [2010].

Ces adresses servent aux ordinateurs du réseau pour communiquer entre eux, ainsi chaque ordinateur d'un réseau possède une adresse IP unique sur ce réseau.

2.2.1 Signification d'une adresse IP

Une adresse IP est une adresse 32 bits, généralement notée sous forme de 4 nombres (4 octets) compris entre 0 et 255 comme xxx.xxx.xxx.xxx. Par exemple, 194.153.205.26 est une adresse IP. En fait, nous distinguons deux parties dans l'adresse IP :

- l'**ID de réseau** (*net-ID*) qui désigne le réseau et qui est donnée par les nombres de gauche ;
- l'**ID d'hôte** (*host-ID*) qui désigne les ordinateurs de ce réseau et qui est donnée par les nombres de droite.

Ainsi, un réseau noté 102.0.0.0 peut contenir des ordinateurs dont l'adresse IP peut varier entre 102.0.0.1 et 102.255.255.254 ($256 * 256 * 256 - 2 = 16777214$ possibilités), tandis qu'un réseau noté 194.26.0.0 ne pourra contenir que des ordinateurs dont l'adresse IP sera comprise entre 194.26.0.1 et 194.26.255.254 ($256 * 256 - 2 = 65534$ possibilités).

2.2.2 Adresses IP spécifiques

En annulant la partie host-ID, c'est-à-dire en remplaçant les bits réservés aux machines du réseau par des zéros (par exemple 194.28.12.0), on obtient ce que l'on appelle l'**adresse**

réseau. Cette adresse ne peut être attribuée à aucun des ordinateurs du réseau.

Lorsque la partie net-ID est annulée, c'est-à-dire lorsque les bits réservés au réseau sont remplacés par des zéros, on obtient l'**adresse machine**. Cette adresse représente la machine spécifiée par le host-ID, qui se trouve sur le réseau courant.

Lorsque tous les bits de la partie host-ID sont à 1, l'adresse obtenue est appelée l'**adresse de diffusion** (broadcast). Il s'agit d'une adresse spécifique, permettant d'envoyer un message à toutes les machines situées sur le réseau spécifié par le net-ID.

Enfin, l'adresse 127.0.0.1 est appelée **adresse de rebouclage** (loopback), car elle désigne la machine locale (localhost).

2.2.3 Classes d'adresses IP

Les adresses IP sont réparties en classes, selon le nombre d'octets qui représentent le réseau.

2.2.3.1 Classe A

Dans une adresse IP de classe A, le premier octet représente le réseau. Le bit de poids fort (le premier bit, celui de gauche) est à zéro, ce qui signifie qu'il y a 2^7 (00000000 à 01111111) possibilités de réseaux, soit 128 possibilités. Toutefois, le réseau 0 (bits valant 00000000) n'existe pas et le nombre 127 est réservé pour désigner votre machine.

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 les ordinateurs du réseau, le réseau peut donc contenir un nombre d'ordinateur égal à : $2^{24} - 2 = 16777214$ ordinateurs.

2.2.3.2 Classe B

Dans une adresse IP de classe B, les deux premiers octets représentent le réseau. Les deux premiers bits sont 1 et 0, ce qui signifie qu'il y a 2^{14} (10 000000 00000000 à 10 111111 11111111) possibilités de réseaux, soit 16 384 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 ordinateurs du réseau. Le réseau peut donc contenir un nombre d'ordinateurs égal à : $2^{16} - 2 = 65534$ ordinateurs.

2.2.3.3 Classe C

Dans une adresse IP de classe C, les trois premiers octets représentent le réseau. Les trois premiers bits sont 1, 1 et 0, ce qui signifie qu'il y a 2^{21} possibilités de réseaux, c'est-à-dire 2 097 152. 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 représente les ordinateurs du réseau, le réseau peut donc contenir : $2^8 - 2 = 254$ ordinateurs.

2.2.4 Adresses IP privées

Il arrive fréquemment dans une entreprise ou une organisation qu'un seul ordinateur soit relié à Internet, c'est par son intermédiaire que les autres ordinateurs du réseau accèdent à Internet (on parle généralement de proxy ou de passerelle).

Dans cette situation, seul l'ordinateur relié à Internet a besoin de réserver une adresse IP auprès de l'ICANN. Toutefois, les autres ordinateurs ont tout de même besoin d'une adresse IP pour pouvoir communiquer ensemble en interne.

Ainsi, l'ICANN a réservé une tranche d'adresses dans chaque classe pour permettre d'affecter une adresse IP aux ordinateurs d'un réseau local relié à Internet sans risquer de créer des conflits d'adresses IP sur le réseau des réseaux (Internet). Il s'agit des adresses suivantes :

- **Adresses IP privées de classe A** : 10.0.0.1 à 10.255.255.254, permettant la création de vastes réseaux privés comprenant des milliers d'ordinateurs.
- **Adresses IP privées de classe B** : 172.16.0.1 à 172.31.255.254, permettant de créer des réseaux privés de taille moyenne.
- **Adresses IP privées de classe C** : 192.168.0.1 à 192.168.0.254, pour la mise en place de petits réseaux privés.

2.2.5 Masque réseau

Un masque réseau (netmask) contient des 1 aux emplacements des bits que l'on désire conserver, et des 0 pour ceux que l'on veut annuler. Une fois ce masque créé, il suffit de

faire un ET logique entre la valeur que l'on désire masquer et le masque afin de garder seulement la partie que l'on désire et annuler le reste.

Ainsi, un masque réseau se présente sous la forme de 4 octets séparés par des points (comme une adresse IP), il comprend (dans sa notation binaire) des zéros au niveau des bits de l'adresse IP que l'on veut annuler (et des 1 au niveau de ceux que l'on désire conserver).

Le premier intérêt d'un masque réseau est de permettre d'identifier simplement le réseau associé à une adresse IP. En effet, le réseau est déterminé par un certain nombre d'octets de l'adresse IP (1 octet pour les adresses de classe A, 2 octets pour les adresses de classe B, et 3 octets pour la classe C). De plus, un réseau est noté en prenant le nombre d'octets qui le caractérise, puis en complétant avec des 0.

Pour connaître l'adresse du réseau associé à l'adresse IP 34.56.123.12, de classe A, il suffit d'appliquer un masque dont le premier octet ne comporte que des 1 (soit 255 en notation décimale), puis des 0 sur les octets suivants. Le masque est :

11111111.00000000.00000000.00000000

Le masque associé à l'adresse IP 34.208.123.12 est donc 255.0.0.0.
La valeur binaire de 34.208.123.12 est :

00100010.11010000.01111011.00001100

Un ET logique entre l'adresse IP et le masque donne ainsi le résultat suivant :

00100010.11010000.01111011.00001100
ET
11111111.00000000.00000000.00000000
=
00100010.00000000.00000000.00000000

Soit 34.0.0.0, qui est donc le réseau associé à l'adresse 34.208.123.12.

2.3 Système de noms de domaine

Chaque ordinateur directement connecté à Internet possède au moins une adresse IP propre. Cependant, les utilisateurs ne veulent pas travailler avec des adresses numériques du genre 194.153.205.26 mais avec des noms de machine ou des adresses plus explicites du type :

http ://www.google.com/

Ainsi, il est possible d'associer des noms en langage courant aux adresses numériques grâce à un système appelé DNS (Domain Name System) Lohier and Présent [2016].

On appelle résolution de noms de domaine (ou résolution d'adresses) la corrélation entre les adresses IP et le nom de domaine associé.

2.3.1 Noms d'hôtes

Les premiers réseaux étaient très peu étendus (le nombre d'ordinateurs connectés à un même réseau était faible), les administrateurs réseau créaient des fichiers appelés « tables de conversion manuelle ». Ces tables de conversion manuelle étaient des fichiers séquentiels, généralement nommés **hosts** ou **hosts.txt**, associant sur chaque ligne l'adresse IP de la machine et le nom littéral associé, appelé **nom d'hôte**.

2.3.2 Fonctionnement du DNS

Le système précédent de tables de conversion nécessitait néanmoins la mise à jour manuelle des tables de tous les ordinateurs en cas d'ajout ou de modification d'un nom de machine. Ainsi, avec l'explosion de la taille des réseaux, et de leur interconnexion, il a fallu mettre en place un système de gestion des noms hiérarchisé et plus facilement administrable. Le système nommé DNS (Domain Name System ou système de noms de domaine) a été mis au point en novembre 1983 par *Paul Mockapetris*, puis révisé en 1987. Le DNS a fait l'objet depuis de nombreuses révisions Pillou [2015].

Ce système propose :

– un **espace de noms** hiérarchique permettant de garantir l'unicité d'un nom dans une structure arborescente ;
– un système de **serveurs distribués** permettant de rendre disponible l'espace de noms ;
– un système de **clients** permettant de « résoudre » les noms de domaines, c'est-à-dire interroger les serveurs afin de connaître l'adresse IP correspondant à un nom.

2.3.2.1 Espace de noms

La structuration du système DNS s'appuie sur une structure arborescente dans laquelle sont définis des domaines de niveau supérieurs (appelés TLD, Top Level Domains), rattachés à un nœud racine représenté par un point (voir Figure 2.1).

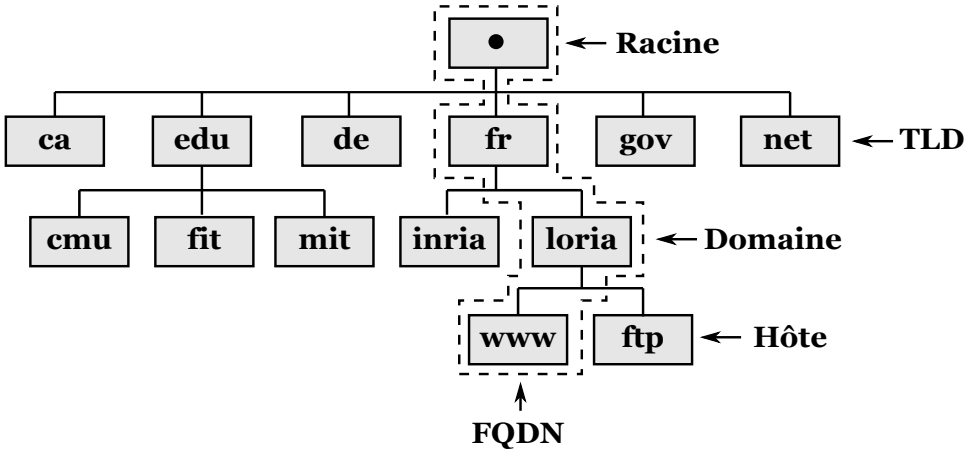


FIGURE 2.1: *Arborescence du DNS.*

On appelle nom de domaine chaque nœud de l'arbre. Chaque nœud possède une étiquette (label) d'une longueur maximale de 63 caractères. L'ensemble des noms de domaine constitue ainsi un arbre inversé où chaque nœud est séparé du suivant par un point « . ».

L'extrémité d'une branche est appelée **hôte**, et correspond à une machine ou une entité du réseau. Le nom d'hôte qui lui est attribué doit être unique dans le domaine considéré. À titre d'exemple le serveur web d'un domaine porte ainsi généralement le nom www.

Le mot domaine correspond formellement au suffixe d'un nom de domaine, c'est-à-dire l'ensemble des étiquettes de nœuds d'une arborescence, à l'exception de l'hôte.

Le nom absolu correspondant à l'ensemble des étiquettes des nœuds d'une arbores-

cence séparées par des points, et terminé par un point final, est appelé **adresse FQDN** (Fully Qualified Domain Name soit nom de domaine totalement qualifié). La profondeur maximale de l'arborescence est de 127 niveaux et la longueur maximale d'un nom FQDN est de 255 caractères. L'adresse FQDN permet de repérer de façon unique une machine sur le réseau des réseaux.

2.3.2.2 Serveurs de noms

Les machines appelées serveurs de noms de domaine permettent d'établir la correspondance entre le nom de domaine et l'adresse IP des machines d'un réseau.

Chaque domaine possède un serveur de noms de domaines, appelé serveur de noms primaire (primary domain name server), ainsi qu'un serveur de noms secondaire (secondary domaine name server) permettant de prendre le relais du serveur de noms primaire en cas d'indisponibilité.

Un serveur de noms définit une zone, c'est-à-dire un ensemble de domaines sur lequel le serveur a autorité. Le système de noms de domaine est transparent pour l'utilisateur, néanmoins il faudrait considérer les recommandations suivantes :

- Chaque ordinateur doit être configuré avec l'adresse d'une machine capable de transformer n'importe quel nom en une adresse IP. Cette machine est appelée DNS (Domain Name Server).
- L'adresse IP d'un second DNS (secondary Domain Name Server) doit également être définie : le serveur de noms secondaire peut relayer le serveur de noms primaire en cas de dysfonctionnement.

2.3.2.3 Résolution de noms de domaine

Le mécanisme consistant à trouver l'adresse IP correspondant au nom d'un hôte est appelé **résolution de noms de domaine**. L'application permettant de réaliser cette opération (généralement intégrée au système d'exploitation) est appelée résolveur (resolver).

Lorsqu'une application souhaite se connecter à un hôte connu par son nom de domaine (par exemple www.google.com), celle-ci va interroger un serveur de noms défini dans

sa configuration réseau. Chaque machine connectée au réseau possède en effet dans sa configuration les adresses IP de deux serveurs de noms de son fournisseur d'accès Internet :

- Une requête est ainsi envoyée au premier serveur de noms (serveur de noms primaire). Si celui-ci possède l'enregistrement dans son cache, il l'envoie à l'application, dans le cas contraire il interroge un serveur racine (dans notre cas un serveur racine correspondant au TLD « .com »).
- Le serveur de noms racine renvoie une liste de serveurs de noms faisant autorité sur le domaine (dans le cas présent les adresses IP des serveurs de noms primaire et secondaire de google.com).
- Le serveur de noms primaire faisant autorité sur le domaine va alors être interrogé et retourner l'enregistrement correspondant à l'hôte sur le domaine (dans notre cas www). La Figure 2.2 illustre la procédure de résolution de noms de domaine.

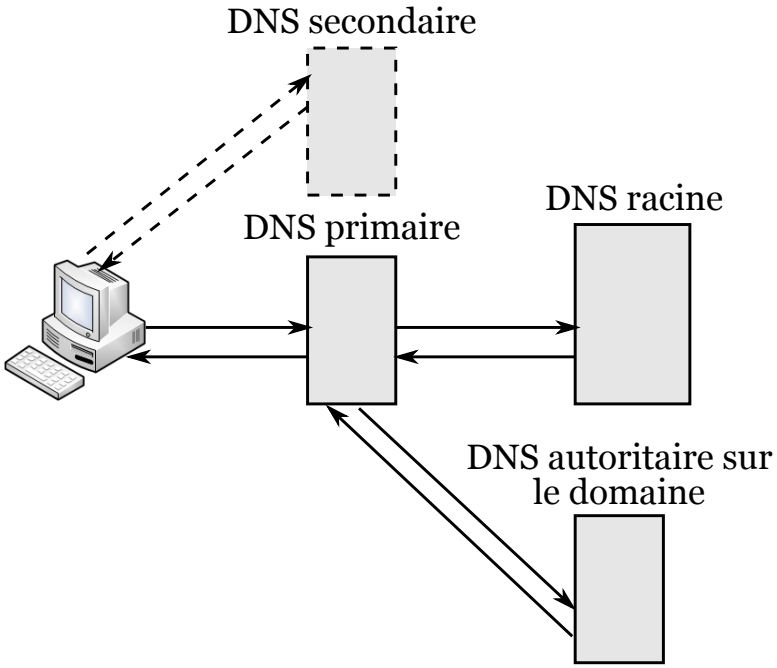


FIGURE 2.2: *Résolution de noms de domaine.*

2.4 Numéro de port

De nombreux programmes informatiques peuvent être exécutés simultanément sur Internet. Chacun de ces programmes travaille avec un protocole, toutefois l'ordinateur

doit pouvoir distinguer les différentes sources de données.

Ainsi, pour faciliter ce processus, chacune de ces applications se voit attribuer une adresse unique sur la machine, codée sur 16 bits : un **port** (la combinaison adresse IP + port est alors une adresse unique au monde, elle est appelée **socket**) Pillou [2015].

L'adresse IP sert donc à identifier de façon unique un ordinateur sur le réseau tandis que le numéro de port indique l'application à laquelle les données sont destinées. De cette manière, lorsque l'ordinateur reçoit des informations destinées à un port, les données sont envoyées vers l'application correspondante. S'il s'agit d'une requête à destination de l'application, l'application est appelée application serveur. S'il s'agit d'une réponse, on parle alors d'application cliente Lohier and Quidelleur [2010].

2.4.1 Multiplexage/Démultiplexage

Le processus qui consiste à pouvoir faire transiter sur une connexion des informations provenant de diverses applications s'appelle le **multiplexage**. De la même façon le fait d'arriver à mettre en parallèle (donc répartir sur les diverses applications) le flux de données s'appelle le **démultiplexage**. Les opérations de multiplexage et de démultiplexage sont illustrés dans la Figure 2.3.

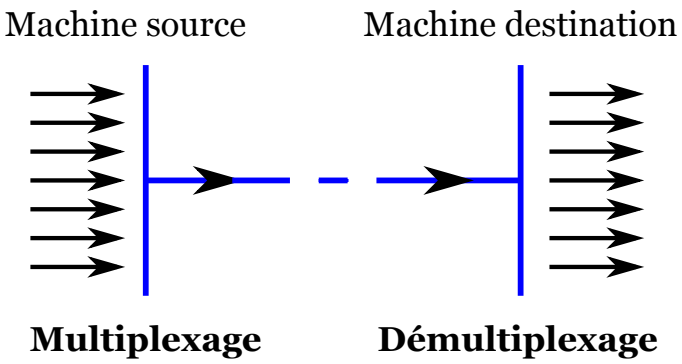


FIGURE 2.3: *Illustrations du multiplexage/démultiplexage de données.*

Ces opérations sont réalisées grâce au port, c'est-à-dire un numéro associé à un type d'application, qui, combiné à une adresse IP, permet de déterminer de façon unique une application qui tourne sur une machine donnée.

2.4.2 Assignation de numéros de port

Il existe des milliers de ports (ceux-ci sont codés sur 16 bits, il y a donc 65 536 possibilités), c'est pourquoi une assignation standard a été mise au point par l'IANA, afin d'aider à la configuration des réseaux :

- Les ports 0 à 1023 sont les ports reconnus ou réservés (Well Known Ports). Ils sont, de manière générale, réservés aux processus système (démons) ou aux programmes exécutés par des utilisateurs privilégiés.
- Les ports 1024 à 49151 sont appelés ports enregistrés (Registered Ports).
- Les ports 49152 à 65535 sont les ports dynamiques et/ou privés (Dynamic and/or Private Ports).

Le Tableau 2.1 présente quelques uns des ports reconnus les plus utilisés :

Port	**Service ou application**
21	FTP (File Transfer Protocol)
25	SMTP (Simple Mail Transfer Protocol)
53	DNS (Domain Name System)
119	NNTP (Network News Transfer Protocol)
80	HTTP (HyperText Transfer Protocol)
110	POP3 (Post Office Protocol 3)

TABLE 2.1: *Quelques ports reconnus les plus utilisés.*

Ainsi, un serveur (un ordinateur que l'on contacte et qui propose des services tels que FTP, Telnet, etc.) possède des numéros de ports fixes auxquels l'administrateur réseau a associé des services. Ainsi, les ports d'un serveur sont généralement compris entre 0 et 1023 (fourchette de valeurs associées à des services connus).

Du côté du client, le port est choisi aléatoirement parmi ceux disponibles par le système d'exploitation. Ainsi, les ports du client ne seront jamais compris entre 0 et 1023 car cet intervalle de valeurs représente les ports connus.

Chapitre 3

Pile protocolaire TCP/IP

3.1 Principe fondamentale de TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) est une suite de protocoles. Cette appellation provient des noms des deux protocoles majeurs de la suite, c'est-à-dire TCP et IP.

TCP/IP représente d'une certaine façon l'ensemble des règles de communication sur Internet et se fonde sur la notion d'adressage IP, c'est-à-dire le fait de fournir une adresse IP à chaque machine du réseau afin de pouvoir acheminer des paquets de données. La suite de protocoles TCP/IP est conçue pour répondre à un certain nombre de critères parmi lesquels Dromard and Seret [2008] :

- le fractionnement des messages en paquets ;
- l'utilisation d'un système d'adresses ;
- l'acheminement des données sur le réseau (routage) ;
- le contrôle des erreurs de transmission de données.

3.2 Modèle en couches des réseaux

Afin de pouvoir appliquer le modèle TCP/IP à n'importe quelle machine, c'est-à-dire indépendamment du système d'exploitation, le système de protocoles TCP/IP a été

décomposé en plusieurs modules effectuant chacun une tâche précise. Ces tâches sont réalisées les unes après les autres dans un ordre précis ; on obtient donc un système structuré que l'on appelle **modèle en couches** Kadoch [2012].

Le terme de couche est utilisé pour évoquer le fait que les données qui transitent sur le réseau traversent plusieurs niveaux de protocoles. Ainsi, les données (paquets d'informations) qui circulent sur le réseau sont traitées successivement par chaque couche, qui vient rajouter un élément d'information (en-tête) puis sont transmises à la couche suivante.

L'intérêt d'un modèle en couches est de séparer le problème en différentes parties (les couches) selon leur niveau d'abstraction. Ainsi, chaque couche du modèle communique avec une couche adjacente, utilise les services des couches inférieures et fournit des services à la couche de niveau supérieur.

3.2.1 Modèle OSI

Le **modèle OSI** (Open Systems Interconnection ou interconnexion de systèmes ouverts) a été mis en place par l'**ISO** (International Standard Organisation, l'organisation internationale de Normalisation) afin de normaliser les communications entre les ordinateurs d'un réseau. En effet, aux origines des réseaux chaque constructeur avait un système propre (système propriétaire) et de nombreux réseaux incompatibles coexistaient. Ce modèle a permis de standardiser la communication entre les machines afin que les différents constructeurs puissent mettre au point des produits (logiciels ou matériels) compatibles (pour peu qu'ils respectent intrinsèquement le modèle OSI). Le modèle OSI est un modèle qui comporte 7 couches (voir Tableau 3.1), tandis que le modèle TCP/IP n'en comporte que 4 Pujolle [2008].

Les rôles des différentes couches sont décrits comme suit :

- La **Couche Physique** définit la façon dont les données sont physiquement converties en signaux numériques sur le média de communication (impulsions électriques, modulation de la lumière, etc.).
- La **Couche Liaison de Données** définit l'interface avec la carte réseau et le partage du média de transmission.
- La **Couche Réseau** permet de gérer l'adressage et le routage des données, c'est-à-

Niveau	Couche
Niveau 7	Couche Application
Niveau 6	Couche Présentation
Niveau 5	Couche Session
Niveau 4	Couche Transport
Niveau 3	Couche Réseau
Niveau 2	Couche Liaison de données
Niveau 1	Couche Physique

TABLE 3.1: *Modèle OSI.*

dire leur acheminement via le réseau.

- La **Couche Transport** est chargée du transport des données, de leur découpage en segments et de la gestion des éventuelles erreurs de transmission.
- La **Couche Session** définit l'ouverture et la fermeture des sessions de communication entre les machines du réseau.
- La **Couche Présentation** définit le format des données manipulées par le niveau applicatif (leur représentation, éventuellement leur compression et leur chiffrement) indépendamment du système.
- La **Couche Application** assure l'interface avec les applications. Il s'agit donc du niveau le plus proche des utilisateurs, géré directement par les logiciels.

3.2.2 Modèle TCP/IP

Le **modèle TCP/IP** reprend l'approche modulaire du modèle OSI (utilisation de modules ou de couches) mais ne contient, lui, que quatre couches (voir Tableau 3.2). Ces couches ont des tâches beaucoup plus diverses étant donné qu'elles correspondent à plusieurs couches du modèle OSI.

Les rôles des différentes couches sont les suivants Pujolle [2008] :

- La **Couche Accès Réseau** spécifie la forme sous laquelle les données doivent être acheminées quel que soit le type de réseau utilisé.
- La **Couche Internet** est chargée de fournir le paquet de données (datagramme).

Niveau	Modèle TCP/IP	Modèle OSI	Protocoles TCP/IP
Niveau 4	Couche Application	Couche Application Couche Présentation Couche Session	Applications réseau (Telnet, SMTP, FTP, etc.).
Niveau 3	Couche Transport (TCP)	Couche Transport	TCP ou UDP
Niveau 2	Couche Internet (IP)	Couche Réseau	IP, ARP, RARP
Niveau 1	Couche Accès réseau	Couche Liaison données Couche Physique	Ethernet, Token Ring FDDI, PPP, etc.

TABLE 3.2: *Modèle TCP/IP.*

- La **Couche Transport** assure l'acheminement des données, ainsi que les mécanismes permettant de connaître l'état de la transmission.
- La **Couche Application** englobe les applications standards du réseau.

3.3 Encapsulation des données

Lors d'une transmission, les données traversent chacune des couches au niveau de la machine émettrice : à chaque couche, une information est ajoutée au paquet de données, il s'agit d'un en-tête, un ensemble d'informations qui garantit la transmission (voir Figure 3.1). Au niveau de la machine réceptrice, lors du passage dans chaque couche, l'en-tête est lu, puis supprimé. Ainsi, à la réception, le message est dans son état originel Dromard and Seret [2008].

À chaque niveau, le paquet de données change d'aspect, car on lui ajoute un en-tête, ainsi les appellations changent suivant les couches :

- Le paquet de données est appelé **message** au niveau de la couche Application.
- Le message est ensuite encapsulé sous forme de **segment** dans la couche Transport.
- Le segment une fois encapsulé dans la couche Internet prend le nom de **datagramme**.
- Enfin, on parle de **trame** au niveau de la couche Accès Réseau.

Dans les sous-sections suivantes, nous allons décrire la procedure d'encapsulation des données au niveau de chacune des couches du modèle TCP/IP.

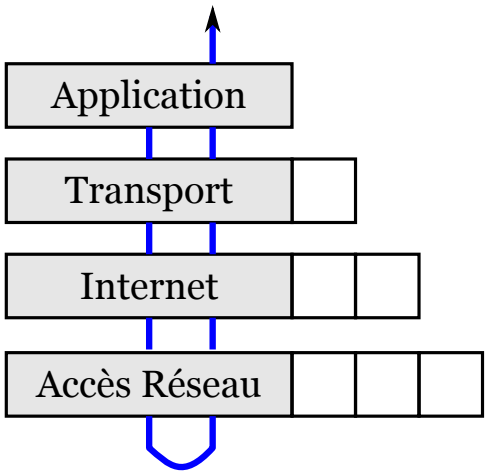


FIGURE 3.1: *Encapsulation des données.*

3.3.1 Couche Accès Réseau

La couche Accès Réseau est la première couche de la pile TCP/IP, elle offre les capacités à accéder à un réseau physique quel qu'il soit, c'est-à-dire les moyens à mettre en œuvre afin de transmettre des données via un réseau.

Cette couche contient toutes les spécifications concernant la transmission de données sur un réseau physique, qu'il s'agisse de réseau local (Ethernet, Token Ring, Token Bus, etc.), de connexion à une ligne téléphonique ou n'importe quel type de liaison à un réseau. Elle prend en charge les notions suivantes :

- acheminement des données sur la liaison ;
- coordination de la transmission de données (synchronisation) ;
- format des données ;
- conversion des signaux (analogique/numérique) ;
- contrôle des erreurs à l'arrivée, etc.

3.3.2 Couche Internet

La couche Internet est la couche la plus importante, car c'est elle qui définit les datagrammes (paquets de données), et qui gère les notions d'adressage IP.

Elle permet l'acheminement des datagrammes vers des machines distantes ainsi que de la gestion de leur fragmentation et de leur assemblage à réception.

La couche Internet contient cinq protocoles : IP, ARP, ICMP, RARP et IGMP. IP, ARP et ICMP sont les protocoles les plus importants. Ces protocoles sont décrits en détails dans Pillou [2015]

3.3.3 Couche Transport

Les protocoles des couches précédentes permettent d'envoyer des informations d'une machine à une autre. La couche Transport permet à des applications tournant sur des machines distantes de communiquer.

Le problème consiste à identifier ces applications. En effet, suivant la machine et son système d'exploitation, l'application pourra être un programme, une tâche, un processus, etc. De plus, la dénomination de l'application peut varier d'un système à un autre, c'est la raison pour laquelle un système de numéro a été mis en place afin de pouvoir associer un type d'application à un type de données, ces identifiants sont appelés ports.

La couche Transport contient deux protocoles permettant à deux applications d'échanger des données indépendamment du type de réseau emprunté, il s'agit des protocoles suivants :

- TCP, un protocole orienté connexion qui assure le contrôle des erreurs.
- UDP, un protocole non orienté connexion dont le contrôle d'erreur n'est pas garantit.

3.3.4 Couche Application

La couche Application est la couche située au sommet des couches de protocoles TCP/IP. Elle contient les applications réseaux permettant de communiquer grâce aux couches inférieures.

Les logiciels de cette couche communiquent donc grâce à un des deux protocoles de la couche inférieure (la couche Transport) c'est- à-dire TCP ou UDP.

Les applications de cette couche sont de différents types, mais la plupart sont des services réseau, c'est-à-dire des applications fournies à l'utilisateur pour assurer l'interface avec le système d'exploitation. Nous pouvons les classer selon les services qu'ils rendent en :

- services de gestion (transfert) de fichier et d'impression,

– services de connexion au réseau,
– services de connexion à distance,
– utilitaires Internet divers.

3.4 Protocole TCP

TCP (Transmission Control Protocol ou protocole de contrôle de transmission) est l'un des principaux protocoles de la couche Transport du modèle TCP/IP. Il permet, au niveau des applications, de gérer les données en provenance (ou à destination) de la couche inférieure du modèle (c'est-à-dire le protocole IP). Lorsque les données sont fournies au protocole IP, celui-ci les encapsule dans des datagrammes IP. TCP est un protocole orienté connexion, c'est-à-dire qu'il permet à deux machines qui communiquent de contrôler l'état de la transmission Kadoch [2012].

Les caractéristiques principales du protocoles TCP sont les suivantes :
– TCP permet de remettre en ordre les datagrammes en provenance du protocole IP.
– TCP permet de vérifier le flot de données afin d'éviter une saturation du réseau.
– TCP permet de formater les données en segments de longueur variable afin de les « remettre » au protocole IP.
– TCP permet de multiplexer les données, c'est-à-dire de faire circuler simultanément des informations provenant de sources distinctes sur une même ligne.
– TCP permet enfin l'initialisation et la fin d'une communication de manière sûre.

3.4.1 Objectifs du protocole TCP

Grâce au protocole TCP, les applications peuvent communiquer de façon sûre (grâce au système d'accusés de réception du protocole TCP), indépendamment des couches inférieures. Cela signifie que les routeurs (qui travaillent dans la couche Internet) ont pour seul rôle l'acheminement des données sous forme de datagrammes, sans se préoccuper du contrôle des données, car celui-ci est réalisé par la couche Transport (plus particulièrement par le protocole TCP).

Lors d'une communication à travers le protocole TCP, les deux machines doivent

établir une connexion. La machine émettrice (celle qui demande la connexion) est appelée client, tandis que la machine réceptrice est appelée serveur. On dit qu'on est alors dans un environnement client/serveur. Les machines dans un tel environnement communiquent en mode connecté, c'est-à-dire que la communication se fait dans les deux sens.

Pour permettre le bon déroulement de la communication et de tous les contrôles qui l'accompagnent, les données sont encapsulées, c'est-à-dire qu'on ajoute aux paquets de données un en-tête qui va permettre de synchroniser les transmissions et d'assurer leur réception.

Une autre particularité de TCP est de pouvoir réguler le débit des données grâce à sa capacité à émettre des messages de taille variable, ces messages sont appelés segments.

TCP permet aussi d'effectuer les opérations de multiplexage et de démultiplexage des données.

3.4.2 Fiabilité des transmissions avec TCP

Le protocole TCP permet d'assurer le transfert des données de façon fiable, bien qu'il utilise le protocole IP, qui n'intègre aucun contrôle de livraison de datagrammes.

En réalité, le protocole TCP possède un système d'accusé de réception permettant au client et au serveur de s'assurer de la bonne réception mutuelle des données.

Lors de l'émission d'un segment, un numéro d'ordre (appelé aussi numéro de séquence) est associé. À réception d'un segment de données, la machine réceptrice va retourner un accusé de réception accompagné d'un numéro égal au numéro d'ordre précédent (voir Figure 3.2).

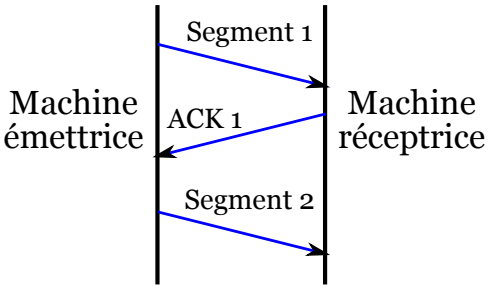


FIGURE 3.2: *Transmission de segments avec TCP : cas 1.*

De plus, grâce à une minuterie déclenchée dès émission d'un segment au niveau de la

machine émettrice, le segment est réexpédié dès que le temps imparti est écoulé, car dans ce cas la machine émettrice considère que le segment est perdu (voir Figure 3.3).

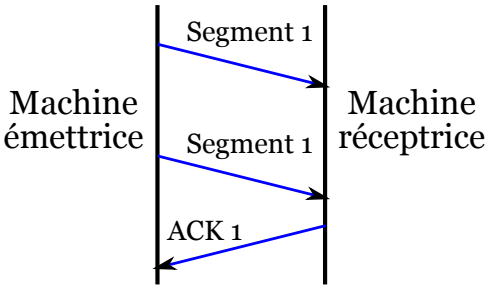


FIGURE 3.3: *Transmission de segments avec TCP : cas 2.*

Toutefois, si le segment n'est pas perdu et qu'il arrive tout de même à destination, la machine réceptrice saura grâce au numéro d'ordre qu'il s'agit d'un autre exemplaire et ne conservera que le dernier segment arrivé à destination.

3.4.3 Établissement d'une connexion TCP

L'établissement de la connexion entre deux applications s'effectue généralement suivant le schéma ci-dessous :

- les ports TCP doivent être ouverts,
- l'application sur le serveur est passive, c'est-à-dire que l'application est à l'écoute, en attente d'une connexion,
- l'application sur le client transmet une requête de connexion sur le serveur dont l'application est en ouverture passive. L'application du client est dite en ouverture active

Les deux machines doivent donc synchroniser leurs séquences grâce à un mécanisme communément appelé **three ways handshake** (poignée de main en trois temps), que l'on retrouve aussi lors de la clôture de session Pillou [2015].

Ce dialogue permet d'initier la communication, il se déroule en trois phases (voir Figure 3.4), comme sa dénomination l'indique :

- Dans un premier temps la machine émettrice (le client) transmet un segment dont le champ SYN est à 1 (pour signaler qu'il s'agit d'un segment de synchronisation), avec un numéro d'ordre N, que l'on appelle numéro d'ordre initial du client.

– Dans un second temps la machine réceptrice (le serveur) reçoit le segment initial provenant du client, puis lui envoie un accusé de réception, c'est-à-dire un segment dont le champ ACK est à 1 et le champ SYN est à 1 (car il s'agit là encore d'une synchronisation). Ce segment contient le numéro d'ordre de cette machine (du serveur). Le champ le plus important de ce segment est le champ accusé de réception qui contient le numéro d'ordre initial du client, incrémenté de 1.
– Enfin, le client transmet au serveur un accusé de réception, c'est-à-dire un segment dont le champ ACK est à 1, dont le champ SYN est à zéro (il ne s'agit plus d'un segment de synchronisation). Son numéro d'ordre est incrémenté et le numéro d'accusé de réception représente le numéro d'ordre initial du serveur incrémenté de 1.

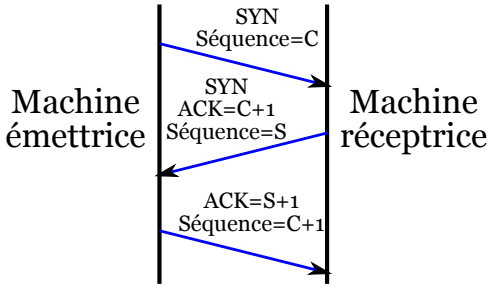


FIGURE 3.4: *Établissement d'une connexion TCP.*

3.5 Protocole IP

Le protocole **IP** (Internet Protocol) fait partie de la couche Internet de la suite de protocoles TCP/IP. C'est un des protocoles les plus importants d'Internet car il permet l'élaboration et l'expédition des datagrammes IP (les paquets de données), sans toutefois en assurer la « livraison ». En réalité, le protocole IP traite les datagrammes IP indépendamment les uns des autres en définissant leur représentation, leur routage et leur expédition Dromard and Seret [2008].

Les données circulent sur Internet sous forme de datagrammes (on parle aussi de paquets). Les datagrammes sont des données encapsulées, c'est-à-dire des données auxquelles on a ajouté des en-têtes correspondant à des informations sur leur expédition (telles que l'adresse IP de destination).

3.5.1 Datagramme IP

La Figure 3.5 représente un datagramme IP. Voici la signification des différents champs :

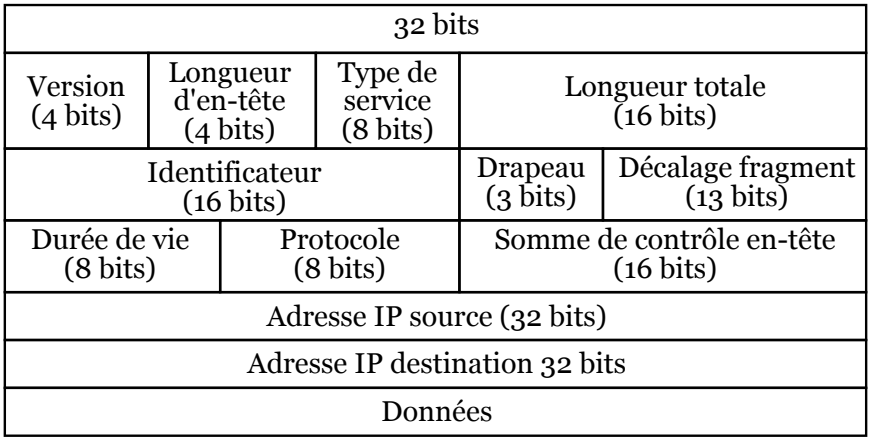


FIGURE 3.5: *Datagramme IP.*

- **Version** (4 bits) : il s'agit de la version du protocole IP que l'on utilise afin de vérifier la validité du datagramme. Elle est codée sur 4 bits.
- **Longueur d'En-Tête** (4 bits) : il s'agit du nombre de mots de 32 bits constituant l'en-tête (la valeur minimale est 5). Ce champ est codé sur 4 bits.
- **Type de Service** (8 bits) : il indique la façon avec laquelle le datagramme doit être traité.
- **Longueur Totale** (16 bits) : il indique la taille totale du datagramme en octets. La taille totale du datagramme ne peut dépasser 65 536 octets. Utilisé conjointement avec la taille de l'en-tête, ce champ permet de déterminer où sont situées les données.
- **Identification**, **Drapeau** et **Décalage Fragment** sont des champs qui permettent la fragmentation des datagrammes.
- **Durée de Vie** (8 bits) : ce champ indique le nombre maximal de routeurs à travers lesquels le datagramme peut passer. Ainsi ce champ est décrémenté à chaque passage dans un routeur, lorsque celui-ci atteint la valeur critique de 0, le routeur détruit le datagramme.
- **Protocole** (8 bits) : ce champ, en notation décimale, permet de savoir de quel protocole est issu le datagramme (1 pour ICMP, 2 pour IGMP, 6 pour TCP et 17 pour UDP).

– **Somme de Contrôle de l'En-Tête** (16 bits) : ce champ contient une valeur codée sur 16 bits qui permet de contrôler l'intégrité de l'en-tête afin de déterminer si celui-ci n'a pas été altéré pendant la transmission.
– **Adresse IP Source** (32 bits) : ce champ représente l'adresse IP de la machine émettrice, il permet au destinataire de répondre.
– **Adresse IP Destination** (32 bits) : adresse IP du destinataire du message.

3.5.2 Fragmentation des datagrammes IP

La taille maximale d'un datagramme est de 65 536 octets. Toutefois cette valeur n'est jamais atteinte car les réseaux n'ont pas une capacité suffisante pour envoyer de si gros paquets. De plus, les réseaux sur Internet utilisent différentes technologies, si bien que la taille maximale d'un datagramme varie suivant le type de réseau.

La taille maximale d'une trame est appelée MTU (Maximum Transfer Unit), elle entraînera la fragmentation du datagramme si celui-ci a une taille plus importante que le MTU du réseau (1 000 octets pour Arpanet, 1500 pour Ethernet et 4 470 pour FDDI).

La fragmentation d'un datagramme se fait au niveau des routeurs, c'est-à-dire lors de la transition d'un réseau dont le MTU est important à un réseau dont le MTU est plus faible. Si le datagramme est trop grand pour passer sur le réseau, le routeur va le fragmenter, c'est-à-dire le découper en fragments de tailles inférieures au MTU du réseau et de telle façon que la taille du fragment soit un multiple de 8 octets (voir Figure 3.6).

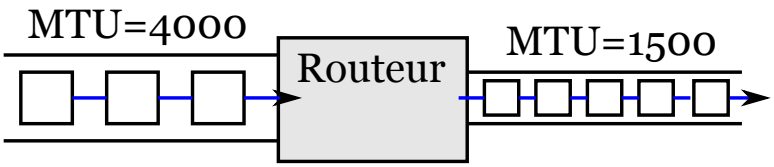


FIGURE 3.6: *Fragmentation des datagrammes IP.*

Le routeur va ensuite envoyer ces fragments de manière indépendante et les réencapsuler (ajouter un en-tête à chaque fragment) de façon à tenir compte de leur taille. De plus, le routeur ajoute des informations afin que la machine de destination puisse réassembler les fragments dans le bon ordre.

Chapitre 4

Réseaux locaux

4.1 Introduction aux réseaux locaux

4.1.1 Définition d'un réseau local

Un réseau local est un ensemble de moyens autonomes de calcul (micro-ordinateurs, stations de travail ou autres) reliés entre eux pour s'échanger des informations et partager des ressources matérielles (imprimantes, espace disque, etc.) ou logicielles (programmes, bases de données, etc.). Le terme de réseau local (LAN, Local Area Network) qui définit un LAN comme un système de communication entre unités centrales sur une étendue géographique limitée est restrictif. Faisant abstraction de la notion d'étendue géographique, le terme de réseau local d'entreprise (RLE) semble mieux approprié Servin [2003].

4.1.2 Constituants d'un réseau local

Architecture informatique dédiée à l'échange d'information et au partage de ressources physiques, un réseau local est essentiellement constitué par (voir Figure 4.1) :

- un câblage reliant les différents nœuds selon une certaine topologie ;
- une méthode d'accès au support pour assurer son partage ;
- une méthode d'adressage pour identifier chaque nœud ;
- un ensemble cohérent de protocoles (pile) pour permettre la communication ;

– un système d'exploitation spécifique (NOS, Network Operating System) capable de prendre en charge les périphériques distants partagés et d'en contrôler l'utilisation (administration et sécurité) ;
– un ensemble de programmes utilisant les ressources mises en commun.

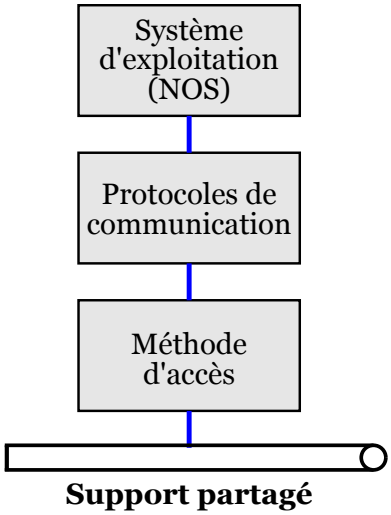


FIGURE 4.1: *Principaux constituants d'un réseau local.*

Pour assurer l'intégralité de ces fonctionnalités, il a fallu adapter l'architecture du modèle de référence de l'ISO. L'architecture OSI répond à l'interconnexion de systèmes en mode point à point, alors que les réseaux locaux partagent un support unique en mode diffusion. Les couches hautes du modèle qui gèrent la communication restent applicables aux réseaux locaux. Cependant, les couches basses qui organisent l'accès au support devront être adaptées (voir Figure 4.2) Montagnier [2004] :

– afin de décrire une interface indépendante du support, la couche physique a été scindée en deux. La sous-couche basse (sous-couche **PMD**, Physical Medium Dependent) assure le transfert des données (bits) sur une gamme de supports variés : câble coaxial, paire torsadée, fibre optique, réseaux sans fil. La sous-couche supérieure (**PMI**, Physical Medium Independent) est chargée de la détection de présence d'un signal, du codage et de la récupération de l'horloge (synchronisation) ;
– la couche liaison de données a, aussi, été divisée en deux. La sous-couche la plus basse contrôle l'accès au support partagé (sous-couche **MAC** ou Medium Access Control) et le contrôle d'erreur, la sous-couche supérieure (sous-couche **LLC**, Logical

Link Control ou Contrôle du lien logique) remplit les fonctions traditionnellement dévolues à la couche liaison (établissement d'un lien logique).

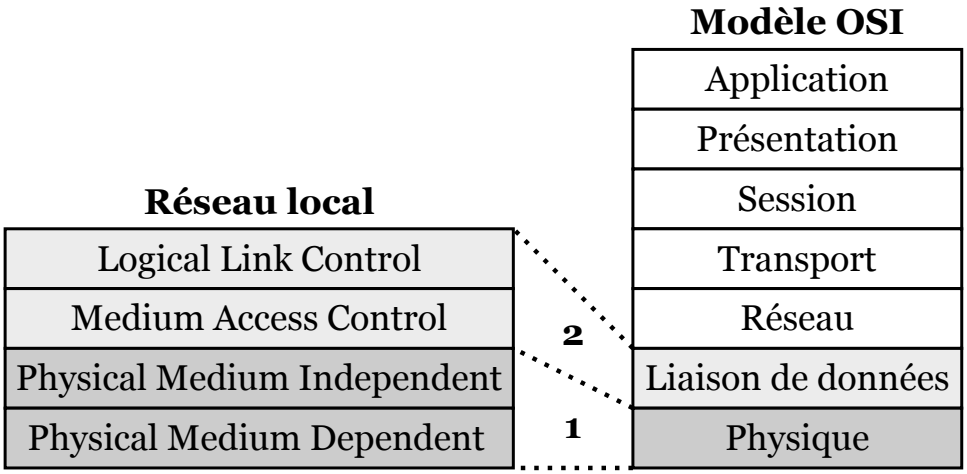


FIGURE 4.2: *Couches 1 et 2 des réseaux locaux.*

Le modèle de référence définit l'adressage des systèmes au niveau réseau (couche 3). Cette adresse détermine le point de raccordement de l'hôte dans le réseau étendu. Si, dans les réseaux locaux, ce système d'adressage était maintenu tel quel, chaque message circulant sur le réseau provoquerait, dans chaque poste raccordé, une interruption processeur. Le processeur examinerait l'adresse pour s'apercevoir que le message ne lui était pas destiné, ce qui diminuerait gravement les performances de toutes les stations du réseau.

Dans les réseaux locaux, il n'y a aucun besoin de localisation, il suffit de distinguer une interface parmi toutes celles raccordées localement sur un même réseau. Chaque interface sera distinguée par un numéro, appelé adresse physique ou adresse MAC (adressage à plat). Le message ne sera transmis aux couches supérieures que s'il concerne l'interface du nœud destinataire.

4.2 Étude des couches 1 et 2 des réseaux locaux

4.2.1 Couche physique

La couche physique spécifie les modes de raccordement (topologie et câblage), les niveaux électriques et le codage des informations émises Cateloin et al. [2012].

4.2.1.1 Topologie

La topologie d'un réseau décrit la manière dont les différents composants du réseau sont reliés. Les réseaux locaux utilisent les topologies de base comme le bus, l'anneau et l'étoile ou des combinaisons de celles-ci (étoile de bus, grappe d'étoiles, etc.).

Sur un bus, les unités sont au même niveau hiérarchique, les messages sont reçus par l'ensemble des stations (diffusion). Le système n'étant pas hiérarchisé, une station peut accéder au support à tout moment. Ce mode d'accès n'interdit pas à deux stations d'émettre en même temps, les messages sont alors altérés : il y a collision ou contention. Pour résoudre ce problème, des règles d'accès au support doivent être fixées :

- la station vérifie, avant d'émettre, qu'aucune autre n'est en émission (écoute du support), cette méthode d'accès est utilisée par les réseaux IEEE 802.3 appelés « **Ethernet** » ;
- selon une autre méthode, chaque station se voit successivement attribuer le droit d'émettre par un message particulier : le token ou jeton. Chaque station qui reçoit le jeton l'adresse à la suivante (jeton adressé). Cette méthode est utilisée dans les réseaux industriels de type IEEE 802.4 ou **Token Bus**.

L'anneau est un cas particulier d'une liaison multipoint, il implique une circulation unidirectionnelle des messages. Le message est relayé par toutes les stations jusqu'à son destinataire. Dans ce type de topologie le droit d'émettre (jeton) est transmis à la station qui suit physiquement celle qui le détient (jeton non adressé). Cette méthode d'accès est mise en œuvre dans le réseau IEEE 802.5 ou **Token Ring**.

Les topologies en étoile sont une variante des liaisons point à point, ils constituent n liaisons point à point autour d'un concentrateur. Une station qui désire émettre formule une demande au concentrateur qui lui alloue ou non le droit d'émettre.

4.2.1.2 Câblage

Les réseaux locaux utilisent tous les types de support : les câbles cuivre (coaxial, paires torsadées), les supports optiques (fibre optique) et les supports hertziens (réseaux sans fil). Le câble coaxial a longtemps été utilisé (réseaux de type Ethernet), mais il est aujourd'hui remplacé par la paire torsadée moins chère et plus facile à installer. La

fibre optique est essentiellement réservée aux réseaux haut débit et à l'interconnexion de réseaux. Le Tableau 4.1 présente une synthèse des différentes caractéristiques des câbles.

Type de câble	**Immunité électromagnétique**	**Débit courant**	**Utilisation**
Coaxial	Bonne	10 Mbit/s	Ethernet, en milieu perturbé ou confidentiel.
Paires torsadées UTP	Faible	10 à 100 Mbit/s	Ethernet sur paires torsadées.
Paires torsadées FTP	Moyenne	10 à 100 Mbit/s	Ethernet sur paires torsadées, Token Ring.
Fibre optique	Excellente	100 à 155 Mbit/s	FDDI

TABLE 4.1: *Câbles mis en œuvre dans les réseaux locaux.*

4.2.2 Sous-couche MAC

La sous-couche **MAC** (Medium Access Control) a pour mission essentielle de gérer l'accès au support physique, elle règle les problèmes d'adressage (adresse MAC) et effectue un contrôle d'erreurs (FCS, Frame Check Sequence) Montagnier [2004].

4.2.2.1 Méthodes d'accès MAC

Ce sont les méthodes d'accès qui distinguent les différents types de réseau et déterminent leurs performances dans tel ou tel environnement. Deux méthodes dominent le monde des réseaux locaux : les méthodes aléatoires ou à contention, mises en œuvre dans les réseaux de type Ethernet, et les méthodes à réservation fondées sur le passage du droit d'émettre (jeton) dont le Token Ring est l'implémentation la plus connue. Les méthodes à contention ou **CSMA** (Carrier Sense Multiple Access ou accès multiple avec écoute de la porteuse) sont utilisées dans deux types de réseaux :

– le réseau AppleTalk (**CSMA/CA**, Collision Avoidance ou à prévention de collision). L'architecture réseau d'Apple est essentiellement destinée au partage de l'im-

primante Laser-Writer. Cette architecture est, aujourd'hui, obsolète ;

– le réseau dit « Ethernet » ou **CSMA/CD** (Collision Detection ou à détection de collision). Ethernet utilise une méthode d'accès qui a été normalisée par l'IEEE et par l'ISO, il représente plus de 90 % des réseaux locaux installés.

Dérivées du polling/selecting (interrogation et sélection), les méthodes à réservation en diffèrent par une distribution décentralisée du droit d'émettre. L'autorisation d'émettre est matérialisée par une trame particulière : le jeton ou token qui circule d'équipement en équipement soit dans l'ordre physique des éléments (Token Ring ou anneau à jeton) soit dans l'ordre logique des stations (Token bus ou bus à jeton). Le jeton circule en permanence sur le réseau, toutes les stations le reçoivent successivement et ne peuvent émettre des données que s'il est libre.

4.2.2.2 Adressage MAC

L'adresse MAC désigne de manière unique une station sur le réseau. À des fins de facilité d'administration, elle est gravée dans l'adaptateur réseau (NIC, Network Interface Card) par le fabriquant. Pour garantir l'unicité d'adresse, c'est l'IEEE qui les attribue. L'IEEE propose deux formats d'adresse : un format long sur 48 bits et un format court sur 16 bits. La Figure 4.3 présente l'adressage IEEE, les bits sont représentés dans l'ordre d'émission sur le support (bits de poids faibles devant).

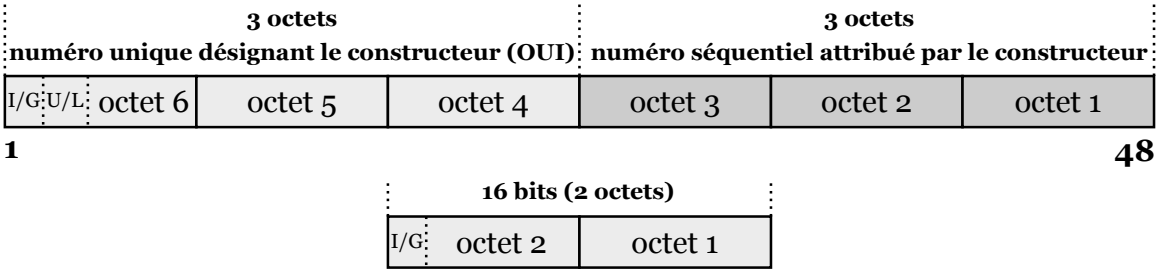


FIGURE 4.3: *Adressage MAC.*

Seul, en principe, l'adressage long est utilisé. Le premier bit (bit I/G) distingue une adresse individuelle ou unicast (I = 0) d'un adressage de groupe (multicast ou broadcast, I = 1). Le bit suivant (bit U/L) détermine si l'adresse qui suit est universelle : adressage IEEE (U = 0) ou local (U = 1). Dans ce dernier cas, c'est à l'administrateur de réseau

de gérer l'espace d'adressage et de garantir l'unicité d'adressage. L'adressage IEEE est un adressage à plat, il il désigne une machine mais ne permet pas d'en déterminer la position géographique.

Dans l'adressage universel, les 22 bits suivants désignent le constructeur ou le revendeur de l'adaptateur réseau. IEEE attribue à chaque constructeur un ou plusieurs numéros qui l'identifient (OUI, Organization Unit Identifier). Les 24 bits suivants appartiennent à une série séquentielle et sont inscrits dans l'adaptateur sous la responsabilité du fabricant (SN, Serial Number).

4.2.3 Sous-couche LLC

4.2.3.1 Présentation de la sous-couche LLC

La sous-couche LLC (Logical Link Control) assure un service comparable à celui offert par la couche liaison du modèle de référence. Elle masque à la couche supérieure le type de réseau utilisé (Ethernet, Token Ring, Token Bus, etc.). Les services de la sous-couche LLC sont accessibles à partir d'un point d'accès **LSAP** (Link Service Access Point ou point d'accès au service de liaison). Pour distinguer les deux extrémités de la relation, ces points sont respectivement appelés **DSAP** pour la machine destination (Destination Service Access Point) et **SSAP** pour la machine source (Source Service Access Point) Servin [2003]. La Figure 4.4 illustre ces notions.

Les unités de données délivrées par ou à la couche supérieure forment des **LSDU** (Link Service Data Unit), celles-ci transmettent à la couche liaison les informations nécessaires à l'envoi des données (adresses MAC source et destination, niveau de priorité, données, etc.). Les sous-couches LLC s'échangent par contre des LPDU (Link Protocol Data Unit).

4.2.3.2 Services de la sous-couche LLC

Service LLC de type 1

Le service LLC1 est un service en mode datagramme. Il n'y a, par conséquent, ni acquittement, ni contrôle de séquencement, ni contrôle de flux et de reprise sur erreur. Le contrôle d'erreur est réalisé par la couche MAC qui rejette toute trame erronée. C'est le

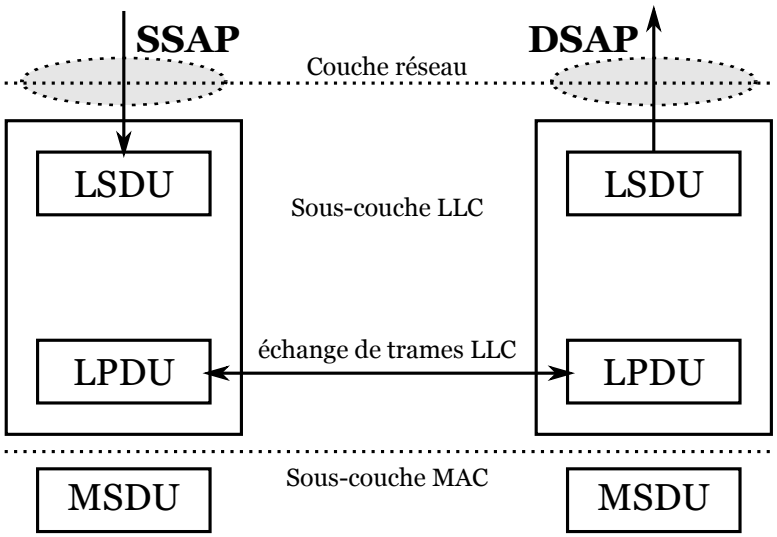


FIGURE 4.4: *Notions de point d'accès de la sous-couche LLC.*

service le plus simple et pratiquement le seul utilisé dans les réseaux locaux. Le service rendu à la couche supérieure est limité, c'est à celle-ci de prendre en compte les lacunes du service LLC1. Généralement, dans les réseaux locaux, c'est la couche transport qui assure ce rôle.

Service LLC de type 2

Le service LLC2 est un service en mode connecté. Il assure l'acquittement, le contrôle de flux, le contrôle de séquencement et la reprise sur erreur. Une connexion est identifiée par l'association de l'adresse LSAP et de l'adresse MAC de la station.

LLC2 est un service en mode connecté, un échange de données ne peut avoir lieu qu'au sein d'une connexion et, par conséquent, ce mode interdit la diffusion.

Service LLC de type 3

Intermédiaire entre le service LLC1, simple mais non sécurisé, et le service LLC2 complexe mais qui assure la délivrance des données, LLC3 implémente un service sans connexion (simplicité) mais avec acquittement (sécurisation des échanges) ; c'est un service de datagrammes acquittés. Si l'acquittement n'est pas arrivé à l'échéance du temporisateur, il n'y a pas de reprise, la perte est signalée aux couches supérieures. Ce sont elles qui décideront de l'éventuelle réémission de la même trame ou d'une nouvelle trame.

4.3 Réseaux IEEE 802.3/Ethernet (CSMA/CD)

4.3.1 Principe du CSMA/CD

Le principe de base du CSMA/CD (Carrier Sense Multiple Access, Collision Detection) repose sur la diffusion des messages à toutes les stations (réseau à diffusion). Lorsqu'une station désire émettre, elle écoute le réseau, si aucun message n'est en cours de diffusion (silence) elle émet, sinon, elle diffère son émission jusqu'à ce que le support soit libre (attente active) Kadoch [2012].

Cette méthode ne peut garantir que deux stations ne décèleront pas le silence en même temps et émettront simultanément leur message. Chaque message est pollué par l'autre (collision) et devient inexploitable. Il est, alors, inutile de continuer à émettre un message incompréhensible. Aussi, lorsqu'une station détecte une collision, elle cesse ses émissions.

Pour détecter les collisions, chaque station écoute le support durant son émission. Si elle décèle une perturbation de son message (les niveaux électriques sur le support ne correspondent pas à son émission), elle arrête son émission et arme un temporisateur (aléatoire, algorithme dit BEB, voir la sous-section 4.3.2.2). À l'échéance du temporisateur la station écoute le support, s'il est libre, elle retransmet le message tout en surveillant son émission (détection de collision). C'est la couche MAC qui réalise la reprise sur collision, ceci évite de remonter dans les couches hautes et de pénaliser les performances du réseau Servin [2003]. La Figure 4.5 illustre ce mécanisme.

La station **A** diffuse son message (t_0 à t_3). La station **B**, avant d'émettre, se met à l'écoute (t_1). Le support est occupé, elle diffère son émission, mais reste à l'écoute (attente active). De même **C**, en t_2, se porte à l'écoute et retarde son émission. En t_3, **A** cesse d'émettre, **B** et **C** détectent le silence, ils émettent simultanément. En t_4, chacune des stations détecte que son message est altéré, la collision est détectée. **B** et **C** cessent leur émission et déclenchent une temporisation aléatoire. En t_5, le timer de **B** arrive à échéance. Le canal étant libre, **B** émet. En t_6, **C** détecte le support occupé et diffère son émission jusqu'au temps t_7.

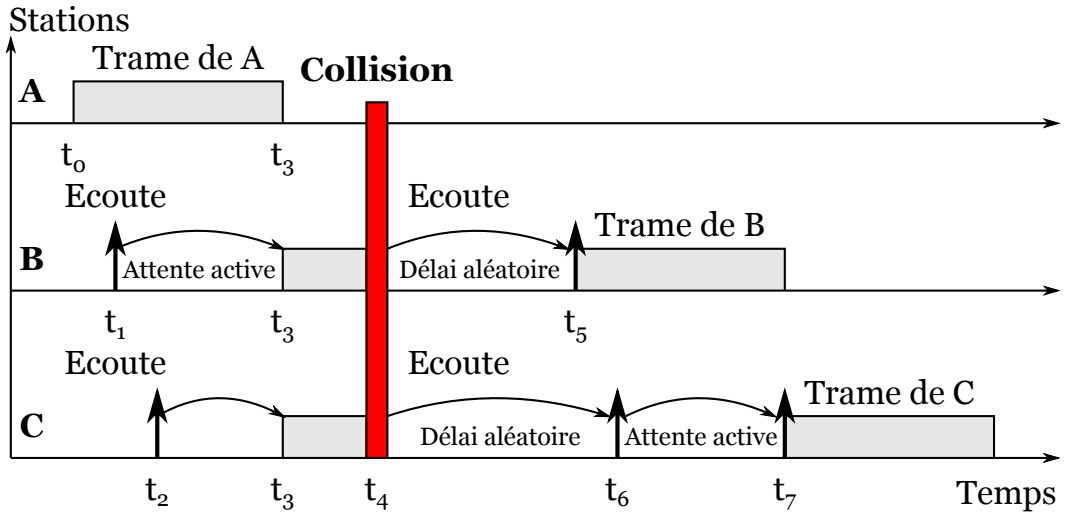


FIGURE 4.5: *Principe du CSMA/CD.*

4.3.2 Caractéristiques des réseaux IEEE 802.3/Ethernet

4.3.2.1 Fenêtre de collision

La fenêtre de collision correspond au temps minimal pendant lequel une station doit émettre pour détecter la collision la plus tardive que son message est susceptible de subir. Considérons (voir Figure 4.6) les deux stations les plus éloignées du réseau : **A** et **B**. En **1**, **A** émet, tant que le message de **A** n'est pas parvenu à **B**, cette dernière suppose le support libre (**2**). **B** émet alors un message juste au moment où le premier bit du message de **A** lui parvient (**3**). La station **B** détecte instantanément la collision et cesse son émission (**3**). Pour que **A** puisse détecter que son message a subi une collision, il est nécessaire que le petit message de **B** lui parvienne et qu'il soit encore en émission à cet instant (**4**). Ce temps minimal d'émission s'appelle **fenêtre de collision**, time slot ou encore tranche canal.

Ce temps minimal d'émission correspond à 2 fois le temps de propagation d'une trame sur la plus grande distance du réseau. Fixé à 51,2 ms, ce temps correspond, pour un débit de 10 Mbit/s, à l'émission de 512 bits, soit 64 octets. Cette exigence implique, en cas de message de longueur inférieure, qu'une séquence de bourrage (padding) soit insérée derrière les données utiles Servin [2012].

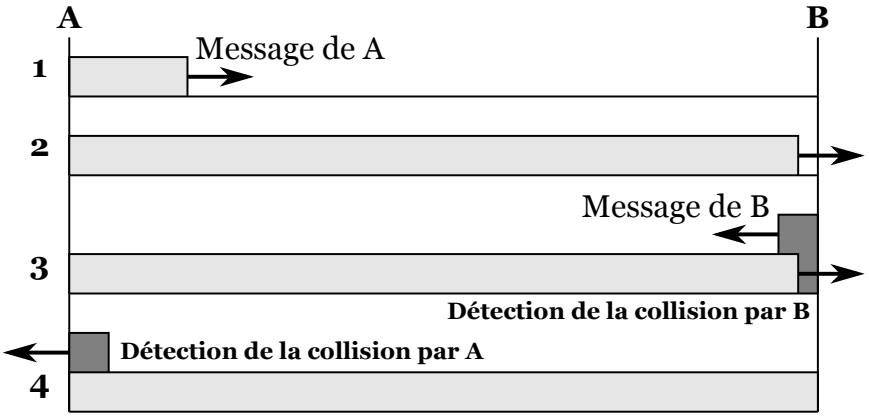


FIGURE 4.6: *Fenêtre de collision.*

4.3.2.2 Algorithme du BEB

Le **BEB** (Binary Exponentiel Backoff) ou encore algorithme de ralentissement exponentiel, détermine le délai aléatoire d'attente avant que la station ne réessaie, après collision, une émission (voir Figure 4.7). Après une collision, une station ne peut émettre qu'après un délai défini

$$T = K \times TimeSlot. \tag{4.1}$$

K est un nombre aléatoire entier généré par l'émetteur et compris dans l'intervalle :

$$K = [0, 2^n - 1] \quad avec \quad n \leq 10 \tag{4.2}$$

Où n représente le nombre de collisions successives détectées par la station pour l'émission d'un même message. Après 16 tentatives, l'émetteur abandonne l'émission.

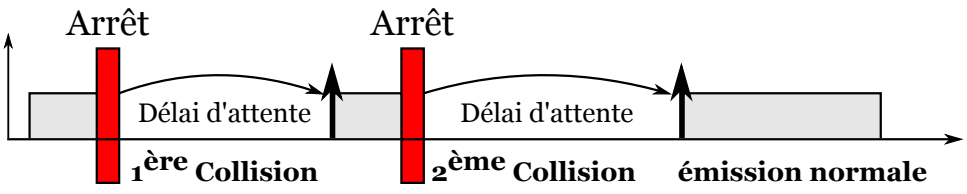


FIGURE 4.7: *Principe du BEB.*

4.4 Réseaux IEEE 802.5/Token Ring

4.4.1 Présentation de la norme IEEE 802.5

La norme IEEE 802.5 spécifie un réseau local en boucle (voir Figure 4.8) : chaque station est reliée à sa suivante et à sa précédente par un support unidirectionnel. Ce réseau est connu sous le nom de Token Ring ou Jeton sur Anneau Kadoch [2012].

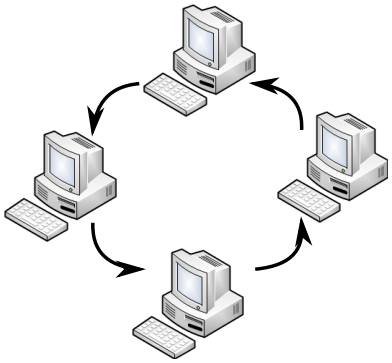


FIGURE 4.8: *Principe de l'anneau.*

Publiée en 1985, la norme IEEE 802.5 fut implémentée par IBM dès 1986. IBM est resté le principal acteur du monde Token Ring. L'implémentation d'IBM diffère quelque peu de la norme d'origine. Notamment, la topologie physique a évolué vers une étoile pour gérer la rupture de l'anneau. Les spécifications d'installation du Token Ring sont contraignantes. Les possibilités de connexion, distance et nombre de postes, dépendent du type de câble utilisé Servin [2003].

4.4.2 Principe de fonctionnement du Token Ring

Le droit d'émettre est matérialisé par une trame particulière « le jeton ou token ». Celui-ci circule en permanence sur le réseau. Une station qui reçoit le jeton peut envoyer une ou plusieurs trames, elle devient station maître. Si elle n'a rien à émettre, elle se contente de répéter le jeton, elle est dite : station répéteur. Dans un tel système, les informations (trames) transitent par toutes les stations actives.

Chaque station du réseau répète le jeton ou le message émis par la station maître, il n'y a pas de mémorisation du message, un bit reçu est immédiatement retransmis. Le

temps alloué à une station pour la répétition d'un bit correspond à un temps bit. Chaque station provoque ainsi un temps bit de retard dans la diffusion d'un message Servin [2012]. Le mécanisme du jeton est illustré par la Figure 4.9.

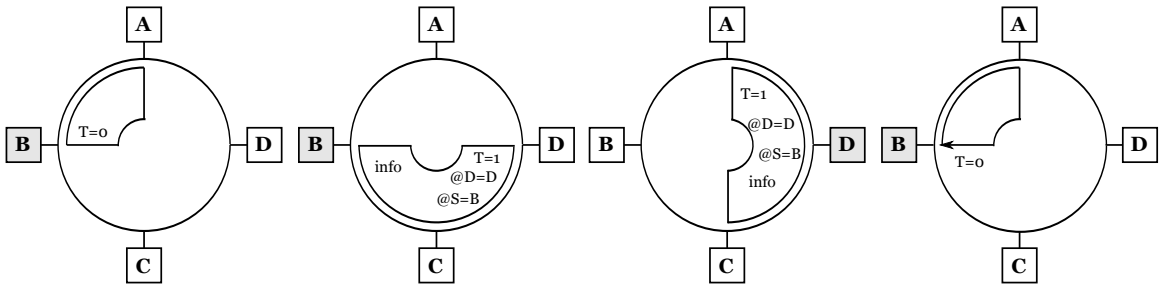


FIGURE 4.9: *Principe de fonctionnement du Token Ring.*

Sur le premier schéma de la Figure 4.9, la station **B**, qui a des données à émettre, reçoit un jeton libre. La disponibilité ou l'indisponibilité du jeton est indiquée par la valeur d'un bit : le bit **T** (Token) ; s'il est à zéro, le jeton est libre, sinon le jeton est marqué « occupé » ($\mathbf{T = 1}$). La station **B** marque le jeton occupé ($\mathbf{T = 1}$), émet à la suite du jeton son message (@Destination, @Source, informations), et devient, momentanément, le maître de l'anneau.

Pour éviter qu'une station monopolise l'anneau, le temps de détention du droit d'émission est limité. Ce temps est, par défaut, d'environ 10 ms. La station **C** lit le jeton, celui-ci est marqué occupé, elle lit l'adresse destination. N'étant pas le destinataire du message, elle ne fait que régénérer le message (fonction répéteur). La station **D** procède de même, mais elle reconnaît son adresse et recopie le message. **B** reçoit l'en-tête du message qu'il a émis. Elle l'ôte de l'anneau (ne le retransmet pas), dès qu'elle a reconnu son adresse (@Source) elle réémet un jeton libre sur le support ($\mathbf{T = 0}$).

4.5 Réseaux IEEE 802.4/Token Bus

4.5.1 Principe de fonctionnement du jeton sur bus

Dans la technique d'accès « jeton adressé sur bus », le jeton, circule de la station de plus faible adresse à celle de plus forte adresse, formant ainsi un anneau virtuel sur le bus (anneau logique/bus physique). Dans le système, représenté par la Figure 4.10, chaque

station, à tour de rôle, reçoit le jeton. Si elle a des données en attente d'émission, elle les émet, puis passe le jeton à la station suivante (celle dont l'adresse suit la sienne) Pujolle [2008].

Toutes les stations en fonctionnement sur le réseau perçoivent le message, mais seule celle dont l'adresse est contenue dans le jeton, considère l'avoir reçu (jeton adressé). Si elle n'a rien à émettre, elle transfère immédiatement le jeton à la station suivante.

Cet algorithme impose que chaque station connaisse l'adresse de celle qui la suit sur l'anneau (NS, Next Station address) et de celle qui la précède (PS, Previous Station address). C'est pourquoi, le problème de l'apprentissage, de l'insertion et du retrait d'une station se pose dans ce type de réseaux Servin [2003].

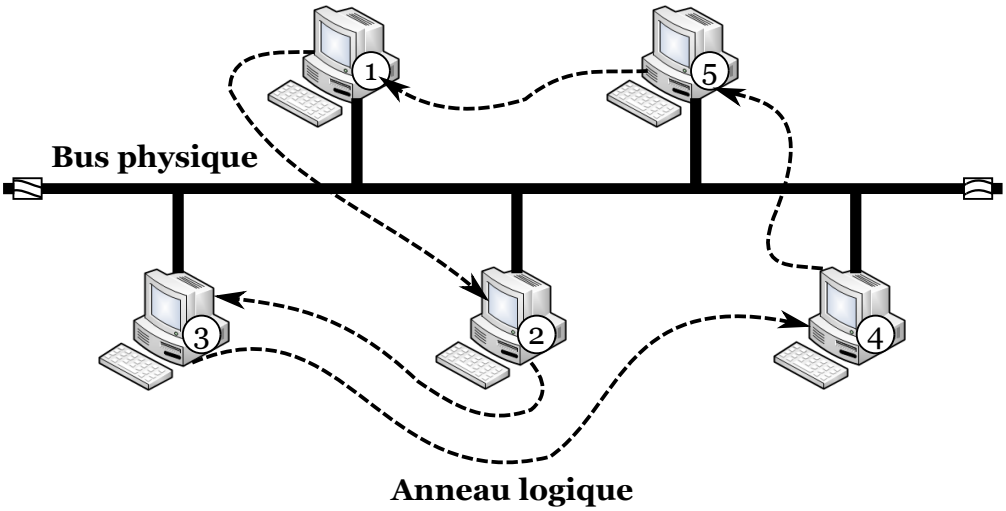


FIGURE 4.10: *Principe de fonctionnement du Token Bus.*

4.5.2 Gestion du jeton sur bus

4.5.2.1 Initialisation de l'anneau et perte du jeton

La perte du jeton ou l'initialisation de l'anneau sont traitées de manière identique. La procédure d'initialisation ou de réinitialisation est déclenchée par détection d'inactivité sur le support (timer d'inactivité remis à zéro à chaque détection d'activité). La station qui détecte l'inactivité passe en procédure d'appel du jeton (trame claim token).

La station émet alors une trame claim token dont la longueur est une fonction de

son adresse, puis, elle passe en écoute. Si elle détecte une activité elle abandonne, sinon elle réitère. Lorsque le silence persiste, elle se considère comme propriétaire du jeton et entreprend la procédure d'insertion pour reconfigurer l'anneau. Notons que cette procédure donne le jeton à la station de plus grande adresse (temps d'émission le plus long).

4.5.2.2 Insertion d'une station sur le réseau

Une station ne peut s'insérer dans l'anneau que si elle y est invitée par la station dont elle doit devenir le successeur sur l'anneau. À cet effet, la station qui détient le jeton déclenche périodiquement une procédure de réveil. La procédure de réveil est déclenchée tous les N passages de jeton. N compris dans l'intervalle [16, 255] est un paramètre défini par l'administrateur du réseau. La Figure 4.11 illustre le mécanisme d'insertion.

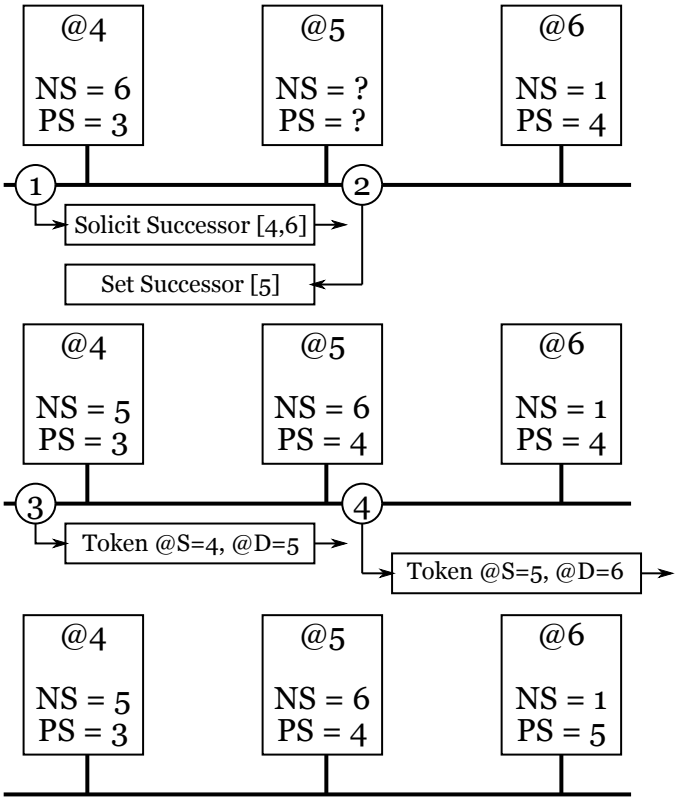


FIGURE 4.11: *Insertion d'une station avec Token Bus.*

La station **5** (que nous supposerons d'adresse **5** notée : **@5**) attend pour s'insérer de recevoir une invitation à le faire. Celle-ci est matérialisée par une trame particulière « solicit successor » dont l'adresse source et destination définissent l'intervalle d'insertion.

Ce message (**étape 1**) invite les stations, dont l'adresse est comprise entre celle de la station origine de l'invitation et sa suivante actuelle, à se manifester. Une réponse est attendue pendant un time slot.

La station **5**, détectant que son adresse (**@5**) est dans l'intervalle d'insertion, répond par le message « set successor » et met à jour ses variables NS et PS (**étape 2**). La station **4** apprend ainsi que son nouveau successeur est la station **5** et lui envoie le jeton (**étape 3**). La station **5** transmet alors le jeton à sa suivante qui apprend ainsi que la station **5** est sa nouvelle précédente (**étape 4**).

4.5.2.3 Retrait d'une station du réseau

Une station qui désire se retirer de l'anneau envoie, lorsqu'elle dispose du jeton, une trame set successor à sa précédente et le jeton à sa suivante, avec l'adresse source de sa précédente. Chaque station peut ainsi mettre ses variables à jour et la continuité de l'anneau est préservée (retrait normal d'une station).

Une station peut aussi se retirer anormalement de l'anneau (panne, par exemple). L'anneau est alors rompu. Lors du passage du jeton, l'émetteur écoute le support, s'il ne détecte aucune activité, c'est-à-dire que son successeur ne retransmet pas le jeton, il réémet le jeton. Si de nouveau il ne détecte aucune activité, il émet une trame « who follows ». Celle-ci contient l'adresse de la station défaillante (celle qui était destinataire du jeton et qui n'a pas répondu) et sa propre adresse.

La station qui reconnaît dans l'adresse destination (adresse de la station défaillante) l'adresse de sa station précédente, met à jour sa variable PS (station précédente) avec l'adresse de la station source et émet une trame set successor. La station défaillante est court-circuitée. Elle doit de nouveau attendre un polling d'insertion pour s'insérer dans l'anneau.

Glossaire

ARP ***A****ddress* ***R****esolution* ***P****rotocol*

BAN ***B****ody* ***A****rea* ***N****etwork*

BEB ***B****inary* ***E****xponentiel* ***B****ackoff*

CSMA ***C****arrier* ***S****end* ***M****ultiple* ***A****ccess*

CSMA/CA ***C****arrier* ***S****end* ***M****ultiple* ***A****ccess* ***C****ollision* ***A****voidance*

CSMA/CD ***C****arrier* ***S****end* ***M****ultiple* ***A****ccess* ***C****ollision* ***D****etection*

DNS ***D****omain* ***N****ame* ***S****ystem*

DSAP ***D****estination* ***S****ervice* ***A****ccess* ***P****oint*

FCS ***F****rame* ***C****heck* ***S****equence*

FDDI ***F****iber* ***D****istributed* ***D****ata* ***I****nterface*

FQDN ***F****ully* ***Q****ualified* ***D****omain* ***N****ame*

FTP ***F****ile* ***T****ransfer* ***P****rotocol*

HTTP ***H****yper****T****ext* ***T****ransfer* ***P****rotocol*

IANA ***I****nternet* ***A****ssigned* ***N****umbers* ***A****gency*

IBM ***I****nternational* ***B****usiness* ***M****achines*

ICANN ***I****nternet* ***C****orporation for* ***A****ssigned* ***N****ames and* ***N****umbers*

ICMP ***I****nternet* ***C****ontrol* ***M****essage* ***P****rotocol*

IEEE ***I****nstitute of* ***E****lectrical and* ***E****lectronics* ***E****ngineers*

IGMP ***I****nternet* ***G****roup* ***M****anagement* ***P****rotocol*

IP ***I****nternet* ***P****rotocol*

ISO ***I****nternational* ***S****tandard* ***O****rganisation*

LAN ***L****ocal* ***A****rea* ***N****etwork*

LLC ***L****ogical* ***L****ink* ***C****ontrol*

LSAP ***L****ink* ***S****ervice* ***A****ccess* ***P****oint*

MAC ***M****edium* ***A****ccess* ***C****ontrol*

MAN ***M****etropolitan* ***A****rea* ***N****etwork*

MTU ***M****aximum* ***T****ransfer* ***U****nit*

NIC ***N****etwork* ***I****nterface* ***C****ard*

NNTP ***N****etwork* ***N****ews* ***T****ransfer* ***P****rotocol*

NS ***N****ext* ***S****tation address*

OSI ***O****pen* ***S****ystems* ***I****nterconnection*

OUI ***O****rganization* ***U****nit* ***I****dentifier*

PAN ***P****ersonal* ***A****rea* ***N****etwork*

PMD ***P****hysical* ***M****edium* ***D****ependent*

PMI ***P****hysical* ***M****edium* ***I****ndependent*

POP3 ***P****ost* ***O****ffice* ***P****rotocol* ***3***

PPP ***P****oint-to-****P****oint* ***P****rotocol*

PS ***P****revious* ***S****tation address*

RARP ***R****everse* ***A****ddress* ***R****esolution* ***P****rotocol*

RLE ***R****éseau* ***L****ocal d'****E****ntreprise*

SMTP ***S****imple* ***M****ail* ***T****ransfer* ***P****rotocol*

SN ***S****erial* ***N****umber*

SSAP ***S****ource* ***S****ervice* ***A****ccess* ***P****oint*

TCP ***T****ransmission* ***C****ontrol* ***P****rotocol*

Telnet ***Ter****minal* ***net****work*

TLD ***T****op* ***L****evel* ***D****omains*

UDP ***U****ser* ***D****atagram* ***P****rotocol*

WAN ***W****ide* ***A****rea* ***N****etwork*

WWW ***W****orld* ***W****ide* ***W****eb*

Bibliographie

Stéphane Cateloin, Antoine Gallais, and Stella Marc-Zwecker. *Mini Manuel Réseaux Informatiques : Cours et Exercices Corrigés*. Dunod, Paris, 2012.

Danièle Dromard and Dominique Seret. *Architecture des Réseaux : Synthèse de Cours et Exercices Corrigés*. Collection Synthex, France, 2008.

Michel Kadoch. *Protocoles et Réseaux Locaux 2e Edition Revue et Augmentée*. Presses de l'Université du Québec, 2012.

Stéphane Lohier and Dominique Présent. *Réseaux et Transmissions : Protocoles, Infrastructures et Services*. Dunod, Paris, 2016.

Stéphane Lohier and Aurélie Quidelleur. *Le Réseau Internet : Des Services aux Infrastructures*. Dunod, Paris, 2010.

Jean-Luc Montagnier. *Réseaux d'Entreprise par la Pratique*. Eyrolles, Paris, 2004.

Jean-François Pillou. *Tout sur les Réseaux et Internet*. Dunod, Paris, 2015.

Guy Pujolle. *Les Réseaux*. Eyrolles, Paris, 2008.

Claude Servin. *Réseaux et Télécom : Cours et Exercices Corrigés*. Dunod, Paris, 2003.

Claude Servin. *Aide-Mémoire de Réseaux et Télécoms*. Dunod, Paris, 2012.