ANNÉE PASSERELLE EN INGÉNIERIE

Introduction à la Téléinformatique

Notions fondamentales, théorie, exemples et exercices

v0.10

HEIA-FR

Vincent Audergon

Année académique 2026-2027

ANNÉE PASSERELLE EN INGÉNIERIE

Introduction à la Téléinformatique

Notions fondamentales, théorie, exemples et exercices

Vincent Audergon

HEIA-FR

Année académique 2026-2027

© 2026 Vincent Audergon, HEIA-FR

Ce document est un support de cours destiné aux étudiant·e·s dans le cadre du cours « Année Passerelle en Ingénierie » à HEIA-FR. Toute reproduction ou diffusion en dehors de ce cadre nécessite l'accord préalable de l'auteur.

Édition 0.10 .
Contact : vincent.audergon@hefr.ch

PRÉFACE

ATTENTION
Cette édition est publiée **progressivement** au fil du semestre : elle contient les chapitres des semaines 1 à **2** (voir le plan du cours ci-après). Les chapitres suivants seront ajoutés au fur et à mesure — consultez le site du cours pour la dernière version.

Ce livre accompagne le cours de base de téléinformatique. Il n'a pas vocation à remplacer les cours. Il rassemble, dans un même volume, la théorie essentielle, des exemples résolus et des exercices pour s'entraîner. La présence aux cours reste obligatoire.

L'ouvrage est pensé comme un **ouvrage de référence** pour le cours. Chaque chapitre s'ouvre sur ses objectifs et se lit de façon autonome : vous pouvez le parcourir dans l'ordre ou y revenir ponctuellement, lorsqu'une notion vous échappe ou qu'un exercice réclame un rappel. Les chapitres sont ordonnés dans le même ordre que les slides du cours.

Les concepts théoriques présentés dans cet ouvrage sont parfois simplifiés pour faciliter la compréhension. Des subtilités et des pans théoriques sont volontairement omis, car ils ne sont pas nécessaires pour atteindre les objectifs du cours. L'ouvrage est donc un **outil d'apprentissage**, et non un manuel de référence exhaustif pour une introduction à la téléinformatique. Il est important de compléter votre apprentissage avec les cours, les travaux pratiques et d'autres ressources pour obtenir une compréhension complète du sujet.

Les **définitions**, **exemples** et **exercices** sont numérotés par chapitre et signalés par des encadrés de couleur, afin de repérer d'un coup d'œil ce que l'on cherche. Les solutions figurent à la fin du livre : essayez d'abord, consultez ensuite.

Toute suggestion d'amélioration ou de correction est la bienvenue. N'hésitez pas à me contacter par mail à l'adresse vincent.audergon@hefr.ch ou à passer dans mon bureau pour en discuter (C10.08).

Transparence sur l'usage de l'IA: cet ouvrage est classé **DALIA D2**[1] (Augmenté par IA) : une intelligence artificielle est intervenue dans la création de petits éléments spécifiques, sans changer le sens de l'oeuvre. L'idéation, la rédaction et la validation finale du contenu restent humaines.

A travers le livre, divers blocs colorés sont utilisés pour signaler des éléments particuliers. Voici leur signification :

REMARQUE
Un point particulier, important ou délicat.

ATTENTION
Un point auquel il faut faire particulièrement attention.

ASTUCE
Une astuce qui permet de mieux assimiler une notion

DÉFINITION 0.1 · EXEMPLE

Une définition est un encadré de couleur, destiné à signaler une notion ou un concept à connaître.

EXEMPLE 0.1

Un exemple est un encadré de couleur, destiné à illustrer une notion ou un concept de manière concrète.

EXERCICE 0.1

Un exercice à résoudre. Les solutions sont disponibles à la fin du livre.

APPROFONDISSEMENT

[1] https://daliascale.org/fr/

Informations complémentaires, mais en dehors des critères d'évaluation du cours, c'est pour votre propre intérêt.

ANECDOTE

Complément d'information sous forme d'anecdote, également en dehors des critères d'évaluation du cours.

PLAN DU COURS

SEM.	CHAPITRE
1	Introduction à la téléinformatique
1	Signaux, topologies et classifications des réseaux
1	Binaire, hexadécimal et opérations logiques
2	Protocoles et modèles en couches
2	Matériel
2	Accès au médium
3	Ethernet et IP *(à venir)*
3	ARP et ICMP *(à venir)*
4	Routage *(à venir)*
4	TCP et UDP *(à venir)*
5	Linux *(à venir)*
6	*Semaine de relâche* *(à venir)*
8	DHCP et DNS *(à venir)*
8	HTTP *(à venir)*
9	Cryptographie, Telnet et SSH *(à venir)*
9	Mail et FTP *(à venir)*
10	NAT *(à venir)*
11	CISCO IOS *(à venir)*
11	RIP et OSPF *(à venir)*
12	Sécurité *(à venir)*
12	Wireless *(à venir)*

SEM.	CHAPITRE
12	Automatisation *(à venir)*

Table des matières

1 Introduction à la téléinformatique 11
1.1 Qu'est-ce que la téléinformatique ? 11
1.2 Historique 12
1.3 Enjeux sociétaux, éthiques et environnementaux 14
1.4 Qu'est-ce qu'un réseau ? 15
1.5 Éléments d'un réseau informatique 17
1.6 Médium de transmission 18
1.7 Applications et services 18
2 Signaux, topologies et classifications des réseaux 21
2.1 Chaîne de transmission 21
2.2 Signal numérique et signal analogique 22
2.3 Modes de transmission 24
2.4 Topologies de réseau 25
2.4.1 Topologie en bus 26
2.4.2 Topologie en anneau 27
2.4.3 Topologie en étoile 27
2.4.4 Topologie maillée 28
2.4.5 Topologie en arbre 28
2.4.6 Comparaison des topologies 29
2.5 Classification des réseaux 30
3 Binaire, hexadécimal et opérations logiques 33
3.1 Unités de mesure de l'information 33
3.1.1 Bit et octet 33
3.1.2 Ordres de grandeur 34
3.1.3 Notations 35
3.1.4 Débit 35
3.1.5 Latence 36
3.1.6 Résumé 36
3.2 Représentation des nombres 36
3.2.1 Binaire 37
3.2.2 Hexadécimal 38
3.2.3 Conversion de la base 10 à la base 2 et 16 39
3.3 Opérations logiques 42
3.3.1 Opérateur ET (AND) 42
3.3.2 Opérateur OU (OR) 43
3.3.3 Opérateur NON (NOT) 43

3.3.4 Opérateur OU exclusif (XOR) 44
3.3.5 Opérations sur plusieurs bits 44
3.4 Encodage ASCII 46
4 Protocoles et modèles en couches 49
4.1 Modèle OSI 50
4.1.1 Couche 1 : Physique 52
4.1.2 Couche 2 : Liaison de données 52
4.1.3 Couche 3 : Réseau 52
4.1.4 Couche 4 : Transport 53
4.1.5 Couche 5 : Session 53
4.1.6 Couche 6 : Présentation 54
4.1.7 Couche 7 : Application 54
4.1.8 Résumé des couches du modèle OSI 54
4.1.9 Exemple concret : Obtenir une page web 56
4.2 Modèle TCP/IP 57
4.2.1 Différences fondamentales entre les modèles OSI et TCP/IP 59
4.2.2 Normes IEEE (802.x) 59
4.2.3 Normes IETF (RFC) 60
4.3 Encapsulation et décapsulation des données 62
5 Matériel 65
5.1 Équipements réseau 65
5.1.1 Hub (Concentrateur) 66
5.1.2 Switch (Commutateur) 67
5.1.3 Routeur 68
5.1.4 Pare-feu (Firewall) 68
5.1.5 Résumé 69
5.2 Médiums physiques et sans fil 70
5.2.1 Cuivre 70
5.2.2 Fibre optique 74
5.2.3 Médiums sans fil 75
5.2.4 Exemples d'applications 76
6 Accès au médium 79
6.1 Domaines de diffusion et de collision 79
6.2 Types de transmission 81
6.3 Méthodes d'accès au médium 83
6.3.1 Par consultation 83
6.3.2 Par compétition 84

6.3.3 Par multiplexage 86
6.3.4 Comparaison des méthodes d'accès au médium 87
Corrigés des exercices 89
Symboles réseau 101
Glossaire 103
Bibliographie 111
Index 113

CHAPITRE 1

Introduction à la téléinformatique

OBJECTIFS DU CHAPITRE

À l'issue de ce chapitre, vous saurez :

- définir la téléinformatique
- situer l'état de l'art et les enjeux de la téléinformatique
- décrire les éléments d'une chaîne de transmission
- citer des exemples d'applications et de services de téléinformatique

1.1 Qu'est-ce que la téléinformatique ?

Avant de pouvoir définir ce qu'est la téléinformatique, il est nécessaire de rappeler ce que sont l'informatique et les télécommunications.

DÉFINITION 1.1 · INFORMATIQUE

Science du traitement automatique et rationnel de l'information considérée comme le support des connaissances et des communications. (larousse.fr)

DÉFINITION 1.2 · TÉLÉCOMMUNICATIONS

Transmission, émission ou réception d'informations par fil, radioélectricité, optique, ou d'autres systèmes électromagnétiques. (larousse.fr)

DÉFINITION 1.3 · TÉLÉINFORMATIQUE

Association de techniques des télécommunications et de l'informatique en vue de réaliser, à distance, l'échange de données et la commande des traitements automatiques. (larousse.fr)

1.2 Historique

Il y a fort longtemps

Transmission de signaux

Les Hommes communiquaient à distance par des signaux visuels (fumée, feu, drapeaux, etc.) ou sonores (trompes, tambours, etc.).

1837

Télégraphe électrique

Samuel Morse et Alfred Vail mettent au point un code de points et de traits : la première transmission numérique de masse.

1876

Téléphone

Graham Bell dépose le brevet du téléphone : la voix devient un signal électrique analogique transporté sur fil.

1969

ARPANET

Premier réseau à commutation de paquets reliant quatre universités américaines : l'ancêtre d'Internet.

1983

TCP/IP

ARPANET adopte la pile TCP/IP comme protocole unique : naissance de l'Internet moderne.

1991

Le Web

Tim Berners-Lee publie le premier site web au CERN et rend le protocole HTTP public.

2000

Internet devient grand public

L'Internet devient accessible au grand public. On dénombre environ 361 millions d'utilisateurs en 2000.

2007

iPhone

Apple lance l'iPhone, un smartphone qui révolutionne la téléinformatique en combinant téléphone, internet et applications mobiles. D'autres smartphones suivent rapidement, rendant l'accès à l'information et aux services en ligne omniprésent.

2010

2 milliards d'utilisateurs

Le nombre d'utilisateurs d'Internet atteint 2 milliards, marquant une adoption mondiale massive de la téléinformatique.

2012

Généralisation de la 4G

Le déploiement de la technologie 4G LTE permet des vitesses de transmission de données plus rapides et une meilleure connectivité mobile, facilitant l'utilisation d'applications en temps réel et le streaming vidéo sur les smartphones.

2013

Les smartphones en Suisse

En Suisse, le nombre de smartphones dépasse celui des téléphones mobiles traditionnels, avec environ 50 à 60% de la population équipée.

2019

5G

Le déploiement de la 5G commence, offrant des vitesses de transmission encore plus rapides, une latence réduite et la possibilité de connecter un grand nombre d'appareils simultanément, ouvrant la voie à de nouvelles applications de téléinformatique.

2020

Télétravail et pandémie

La pandémie de COVID-19 entraîne une adoption massive du télétravail et des outils de communication en ligne, mettant en évidence l'importance de la téléinformatique dans la vie professionnelle et personnelle.

2022

ChatGPT et IA générative

L'essor de l'intelligence artificielle générative, avec des modèles comme ChatGPT, transforme la manière dont les utilisateurs interagissent avec les systèmes informatiques, facilitant l'accès à l'information et la création de contenu.

2025

IA Omniprésente

L'intelligence artificielle devient omniprésente dans les applications de téléinformatique, offrant des assistants

virtuels, des recommandations personnalisées et des capacités d'automatisation avancées.

EXERCICE 1.1 · CHRONOLOGIE DE LA TÉLÉINFORMATIQUE

Sans regarder la frise ci-dessus, classez ces événements du plus ancien au plus récent : le Web, ARPANET, l'iPhone, le télégraphe électrique, l'adoption de TCP/IP.

1.3 Enjeux sociétaux, éthiques et environnementaux

Aujourd'hui, l'ITU (International Telecommunication Union) dénombre environ 6 milliards d'utilisateurs d'internet, soit près de 75% de la population mondiale [1]. La téléinformatique est devenue un élément central de la vie quotidienne, influençant la communication, l'éducation, le commerce, le divertissement et bien d'autres aspects de la société. Elle a transformé la manière dont les individus interagissent, accèdent à l'information et participent à l'économie mondiale. Selon l'étude JAMES 2024 [2], les jeunes Suisses passent en moyenne 3 à 4 heures par jour sur leur smartphone et 34% utilisent des outils à base d'IA générative au moins une fois par semaine.

Les retombées positives de cette révolution sont concrètes et mesurables. L'éducation s'est ouverte : le nombre d'apprenants inscrits à des cours en ligne ouverts à tous (MOOC) est passé de zéro en 2012 à environ 220 millions en 2021 [3]. En médecine, selon Flodgren et al. [4], la télémédecine améliore le contrôle de la glycémie chez les patients diabétiques, avec des résultats par ailleurs équivalents à ceux d'une prise en charge en face à face : un accès aux soins facilité, sans perte de qualité. À cela s'ajoutent des bénéfices quotidiens plus diffus : rester en contact avec ses proches, accéder à l'information en quelques secondes ou encore utiliser des robots pour effectuer des tâches dangereuses pour un humain à distance.

Les revers de la médaille sont également nombreux : cybercriminalité, désinformation, dépendance aux écrans, atteintes à la vie privée et à la sécurité des données, impact environnemental des data centers et de la blockchain, etc. La téléinformatique soulève donc des questions éthiques, sociales et environnementales importantes, nécessitant une réflexion sur son utilisation responsable et durable.

D'après l'étude JAMES 2024 [2], plus d'un quart des jeunes suisses déclarent avoir déjà reçu plusieurs fois des insultes en ligne, 20% ont été

victimes de diffusions de photos ou vidéos embarrassantes à leur sujet, et 7% ont déjà été victimes de menaces ou de chantage en ligne.

Du côté de la désinformation, l'OFS (Office fédéral de la statistique) indique qu'en 2025, 58% de la population suisse déclare avoir déjà rencontré du contenu faux ou douteux sur des sites ou des réseaux sociaux [5].

La consommation d'énergie des data centers est également un enjeu majeur. Selon l'Agence internationale de l'énergie (IEA), les data centers à travers le monde consomment environ 1.5% de l'électricité mondiale en 2024 pour un total de 415 TWh. Cette consommation devrait plus que doubler, pour atteindre 945 TWh d'ici 2030, soit la consommation électrique annuelle du Japon en 2025 [6]. Cette augmentation est due à la croissance exponentielle des données générées par les utilisateurs, l'essor de l'intelligence artificielle et le développement de services en ligne. Selon Freitag et al. [7], l'empreinte carbone du numérique en 2020 représente 2.1% à 3.9% des émissions mondiales de gaz à effet de serre, soit davantage que l'aviation civile.

Les datacenters ne sont pas les seuls responsables de l'empreinte carbone de la téléinformatique. Les blockchains et par extension les cryptomonnaies représentent une part significative de la consommation électrique mondiale. Selon le Cambridge Bitcoin Electricity Consumption Index (CBECI), le réseau du Bitcoin à lui seul consomme environ 201 TWh par an (état mi-juillet 2026), soit environ 0.7% de la consommation électrique mondiale [8].

En résumé, la révolution de la téléinformatique a apporté des avantages considérables à la société, mais elle pose également des défis importants en matière d'éthique, de sécurité et d'environnement. Il est crucial de continuer à développer des technologies et des pratiques responsables et durables pour maximiser les bénéfices tout en minimisant les impacts négatifs.

1.4 Qu'est-ce qu'un réseau ?

Au sens large, un réseau désigne un ensemble d'éléments (noeuds) interconnectés par des liens (arêtes), permettant la circulation d'une ressource ou d'une information.

L'un des réseaux les plus connus est probablement le réseau routier, qui relie des villes et des villages par des routes et autoroutes, permettant la circulation de véhicules et de personnes. Les autoroutes sont des liens à

grande capacité, tandis que les routes secondaires sont des liens à plus faible capacité. Les villes et villages sont les noeuds du réseau.

En téléinformatique, l'analogie avec le réseau routier est pertinente : les ordinateurs et autres équipements informatiques sont les noeuds, tandis que les câbles, fibres optiques et ondes radio sont les liens qui permettent la circulation des données. Certains liens sont à grande capacité (fibre optique, 5G), tandis que d'autres sont à plus faible capacité (ADSL, 3G). Les protocoles de communication jouent un rôle similaire aux règles de circulation, régissant la manière dont les données circulent dans le réseau.

DÉFINITION 1.4 · RÉSEAU INFORMATIQUE

Mise en relation d'au moins deux systèmes informatiques (ordinateurs, serveurs, périphériques) au moyen d'un médium de communication.

Un réseau informatique peut être de différentes tailles, formes et complexités, allant d'un simple réseau local dans une maison ou un bureau, à un vaste réseau mondial comme Internet.

EXEMPLE 1.1 · EXEMPLES DE RÉSEAUX INFORMATIQUES

- Internet
- Réseau d'entreprise
- Réseau de l'HEIA-FR
- Des écouteurs Bluetooth connectés à un smartphone
- Deux ordinateurs reliés par un câble Ethernet
- etc.

1.5 Éléments d'un réseau informatique

Un réseau informatique est composé de différents éléments, chacun ayant un rôle spécifique dans le système global. Dans le cadre du cours de téléinformatique, la nomenclature suivante est utilisée :

- **Périphérique / Hosts** : Un noeud du réseau, que ce soit un noeud dit « terminal » (ordinateur, smartphone, tablette, etc.) ou un noeud dit « intermédiaire » (routeur, switch, etc.).
- **Medium / Support de transmission** : Le lien physique ou logique qui permet la transmission des données entre les périphériques. Il peut s'agir de câbles (cuivre, fibre optique), d'ondes radio (Wi-Fi, 4G/5G) ou d'autres technologies de communication.
- **Messages / Données** : L'information qui transite à travers le réseau.
- **Protocoles / Règles de communication** : Les règles et conventions qui régissent la manière dont les périphériques communiquent entre eux, assurant que les messages sont correctement transmis, reçus et interprétés.

La Fig. 1 montre un exemple de réseau informatique utilisé pour envoyer un message d'un périphérique à un autre.

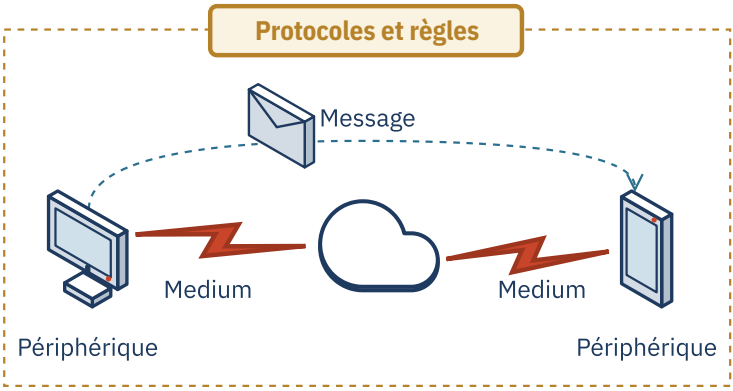


Fig. 1. – Illustration des différents éléments d'un réseau informatique. Dans cet exemple, l'ordinateur envoie un message au smartphone. La communication est régie par des règles.

EXERCICE 1.2 · NOMMER DES PÉRIPHÉRIQUES

Nommer des périphériques (terminaux et intermédiaires).

1.6 Médium de transmission

Les médiums (ou supports) de transmission sont les canaux par lesquels les données circulent dans un réseau informatique. Ils peuvent être classés en deux grandes catégories : les médiums filaires et les médiums sans fil. Pour transmettre une information d'un point A à un point B, des médiums de différents types peuvent être utilisés, chacun ayant ses propres caractéristiques, avantages et inconvénients.

EXEMPLE 1.2 · TRANSMISSION DE DONNÉES SUR DIFFÉRENTS MÉDIUMS

Alice envoie un message à Bob depuis son smartphone. Tout d'abord, les données sont transmises par les ondes radio entre le smartphone d'Alice et l'antenne relais la plus proche. Ensuite, les données voyagent à travers le réseau de l'opérateur mobile, composé de fibre optique. Enfin, elles atteignent l'ordinateur de Bob par le câble cuivre du réseau local.

EXERCICE 1.3 · IDENTIFIER LES ÉLÉMENTS D'UN RÉSEAU

Alice regarde une vidéo en streaming sur sa tablette, connectée au Wi-Fi de la maison. Le routeur de la maison est relié à Internet par une fibre optique. Identifiez dans ce scénario : les périphériques terminaux, les périphériques intermédiaires, les médiums de transmission et le message.

1.7 Applications et services

La téléinformatique permet la mise en place de nombreux services et applications qui facilitent la communication, l'accès à l'information et la collaboration à distance. Parmi les applications les plus courantes, on peut citer :

- La communication par messagerie
  - Email
  - Messagerie instantanée (WhatsApp, Telegram, Signal)
  - Réseaux sociaux (Facebook, Twitter, Instagram)
- Applications en temps réel
  - Jeux en ligne
  - Streaming vidéo (Netflix, YouTube, Twitch)

  - Streaming audio (Spotify, Apple Music)
  - Communication en temps réel (Discord, Slack, MS Teams)
- Applications partagées
  - Stockage en ligne (Google Drive, Dropbox, OneDrive)
  - Outils de collaboration (Google Docs, Microsoft Office 365)
  - Plateformes de gestion de projets (Trello, Asana, Jira)
- Partage de ressources
  - Impression à distance
  - Partage de fichiers
  - Accès à des bases de données distantes
- Gestion centralisée
  - Administration de systèmes et réseaux
  - Supervision et monitoring d'infrastructures
  - Gestion de serveurs et services cloud
- Cloud
  - Infrastructure as a Service (IaaS)
  - Platform as a Service (PaaS)
  - Software as a Service (SaaS)
- Etc.

Chaque application ou service possède des besoins spécifiques en termes de débit, latence et fiabilité. Le débit est la quantité de données pouvant transiter par seconde (ou autre unité de temps), la latence est le délai entre l'envoi et la réception d'un message, et la fiabilité est la capacité à transmettre les données sans perte ni corruption (le message arrive intact et complet).

EXERCICE 1.4 · FIABILITÉ, DÉBIT ET LATENCE SELON L'APPLICATION

Parmi les points suivants: débit, latence et fiabilité, quel est l'aspect le plus important pour l'envoi d'un email ? Pour le streaming vidéo (Netflix) ? Et pour les jeux en ligne ?

CHAPITRE 2

Signaux, topologies et classifications des réseaux

OBJECTIFS DU CHAPITRE

À l'issue de ce chapitre, vous saurez :

- définir les notions de signal, de bruit et de canal
- distinguer un signal analogique d'un signal numérique
- citer les modes de transmission unicast, multicast et broadcast
- citer les principales topologies de réseau et leurs caractéristiques
- citer les classifications des réseaux de téléinformatique

2.1 Chaîne de transmission

Une chaîne de transmission est un ensemble d'éléments qui permettent de transmettre des données d'un émetteur à un récepteur. Elle se compose de trois éléments principaux : l'émetteur, le canal et le récepteur. Le signal est émis par l'émetteur, transmis par le canal et reçu par le récepteur. Le bruit peut altérer le signal lors de sa transmission, ce qui peut entraîner des erreurs de communication. Ce modèle fonctionne autant pour la téléinformatique que pour tout autre type de communication (orale, écrite, radio, etc.). Par exemple, dans le cadre d'une communication orale, l'émetteur est la personne qui parle, le canal est l'air et le récepteur est la personne qui écoute. Le bruit peut être un bruit de fond ou une mauvaise prononciation qui altère le message.

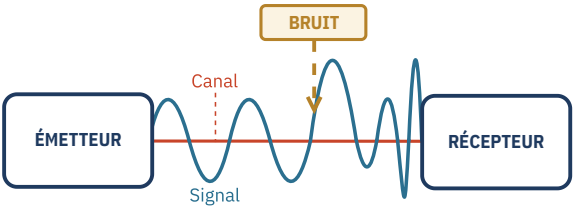


Fig. 2. – Illustration d'une chaîne de transmission. Le signal est émis par un émetteur, transmis par un canal et reçu par un récepteur. Le bruit peut altérer le signal lors de sa transmission, ce qui peut entraîner des erreurs de communication.

Dans le cadre de la téléinformatique, des mécanismes de correction d'erreurs sont mis en place pour détecter et corriger les erreurs de transmission. Ces mécanismes permettent d'assurer la fiabilité des communications, même en présence de bruit. Les différents types de médiums de transmission (câbles, fibres optiques, ondes radio, etc.) ont une sensibilité différente au bruit et aux interférences, ce qui peut influencer la qualité de la transmission.

EXERCICE 2.1 · IDENTIFIER LES ÉLÉMENTS D'UNE CHAÎNE DE TRANSMISSION

Pour le contexte ci-dessous, identifiez l'émetteur, le canal, le récepteur et les sources potentielles de bruit qui pourraient altérer le signal.

Alice envoie une lettre manuscrite à Bob. Le facteur transporte la lettre de la maison d'Alice à la maison de Bob. Pendant le transport, la lettre est exposée à des conditions météorologiques défavorables, comme la pluie et le vent, qui peuvent endommager le papier et rendre le texte illisible. De plus, il est possible que la lettre soit perdue ou volée pendant le transport.

2.2 Signal numérique et signal analogique

Il existe deux types de signaux : les signaux analogiques et les signaux numériques. Un signal analogique est un signal continu qui peut prendre une infinité de valeurs (Fig. 3), tandis qu'un signal numérique est un signal discret qui ne peut prendre qu'un nombre limité de valeurs (Fig. 4).

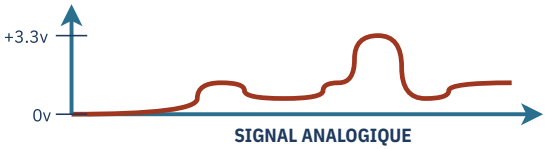


Fig. 3. – Illustration d'un signal analogique. Le signal analogique est continu et peut prendre une infinité de valeurs.

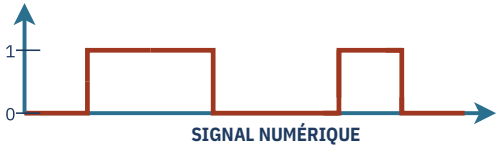


Fig. 4. – Illustration d'un signal numérique. Le signal numérique est discret et ne peut prendre qu'un nombre limité de valeurs.

Historiquement, les signaux analogiques étaient utilisés pour transmettre des informations, mais avec l'avènement de l'informatique et des technologies numériques, les signaux numériques sont devenus prédominants. Les signaux numériques présentent plusieurs avantages par rapport aux signaux analogiques, notamment une meilleure résistance au bruit et aux interférences.

ANECDOTE

Par abus de langage, le terme « numérique » est souvent remplacé par le terme « digital » en français. Cependant, ce terme est erroné car il signifie « relatif aux doigts » et n'a pas de rapport avec le traitement de l'information. Cette confusion est due à l'anglais, où le terme digital signifie « relatif aux chiffres » et est utilisé pour désigner les systèmes numériques.

EXERCICE 2.2 · ANALOGIQUE OU NUMÉRIQUE ?

Pour chaque élément ci-dessous, indiquez s'il s'agit d'un signal (ou support) analogique ou numérique.

A. La voix humaine se propageant dans l'air

B. Un fichier MP3

C. Un disque vinyle

D. Un SMS

E. La température affichée par un thermomètre à mercure

2.3 Modes de transmission

En télécommunication, la transmission peut se faire entre un émetteur et un ou plusieurs récepteurs. On distingue trois modes de transmission : le unicast, le multicast et le broadcast.

Le mode de transmission unicast (illustré par la Fig. 5) consiste à envoyer un signal d'un émetteur vers un récepteur unique. Ce mode est utilisé pour les communications directes entre deux appareils, comme dans le cas d'une conversation téléphonique ou d'une connexion Internet entre un ordinateur et un serveur.

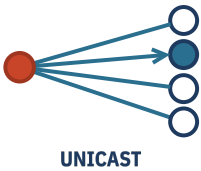


Fig. 5. – Illustration d'une transmission unicast. Le signal est envoyé d'un émetteur vers un récepteur unique.

Le mode de transmission multicast (illustré par la Fig. 6) consiste à envoyer un signal d'un émetteur vers un groupe de récepteurs. Ce mode est utilisé pour les communications de groupe, comme dans le cas d'une diffusion de vidéo en direct ou d'une conférence en ligne.

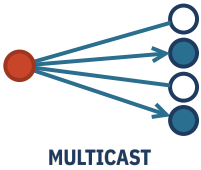


Fig. 6. – Illustration d'une transmission multicast. Le signal est envoyé d'un émetteur vers un groupe de récepteurs.

Le mode de transmission broadcast (illustré par la Fig. 7) consiste à envoyer un signal d'un émetteur vers tous les hôtes du domaine de diffusion (voir le chapitre *Accès au médium*). Il est utilisé pour transmettre des informations à tous les appareils d'un réseau, comme dans le cas d'une diffusion de messages ou d'annonces.

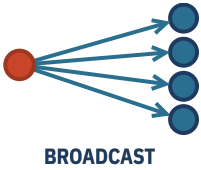


Fig. 7. – Illustration d'une transmission broadcast. Le signal est envoyé d'un émetteur vers tous les récepteurs du réseau.

EXERCICE 2.3 · IDENTIFIER LE MODE DE TRANSMISSION

Pour chaque situation, indiquez le mode de transmission : unicast, multicast ou broadcast.

A. Un appel vidéo entre deux personnes.

B. La transmission d'un flux vidéo en direct à un groupe d'abonnés.

C. Une annonce envoyée à tous les hôtes d'un réseau local.

D. Le téléchargement d'un fichier depuis un serveur.

2.4 Topologies de réseau

Un réseau peut prendre de nombreuses formes différentes, appelées topologies. Un certain nombre de topologies sont couramment utilisées dans les réseaux de téléinformatique, chacune ayant ses propres caractéristiques et avantages. Les principales topologies sont la topologie en bus, la topologie en anneau, la topologie en étoile, la topologie maillée et la topologie en arbre (ou hiérarchique). Chacune de ces topologies est décrite ci-dessous.

2.4.1 Topologie en bus

La topologie en bus est une topologie dans laquelle tous les périphériques du réseau sont connectés à un seul câble de transmission, comme illustré par la Fig. 8. Les données sont transmises le long du bus et chaque périphérique peut écouter les données qui passent. Cette topologie est simple à mettre en place et peu coûteuse, mais elle présente des limitations en termes de performance et de fiabilité. En effet, si le lien est coupé ou si le bus est endommagé, l'ensemble du réseau peut être affecté.

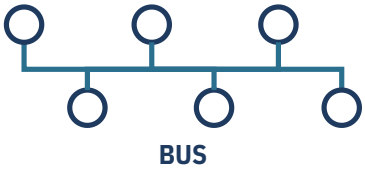


Fig. 8. – Illustration d'une topologie en bus. Chaque point représente un périphérique du réseau.

ANECDOTE

De nos jours, la topologie en bus n'est plus beaucoup utilisée à cause des nombreux défauts qu'elle présente. Dans les années 1980, une norme Ethernet appelée 10BASE5 avait pour principe d'utiliser une topologie en bus. Les périphériques se branchaient directement sur le câble du bus à l'aide de prises appelées « prises vampire » (Fig. 9). Ces prises étaient appelées ainsi car elles venaient s'accrocher au câble du bus comme un vampire s'accroche à sa victime.

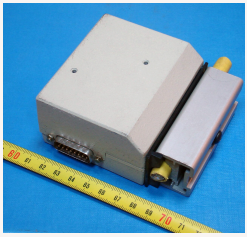


Fig. 9. – Illustration d'une prise vampire. Ces périphériques se branchaient directement sur le câble du bus.

2.4.2 Topologie en anneau

Dans la topologie en anneau, chaque périphérique est connecté à deux autres périphériques, formant ainsi un cercle. Les données circulent dans un seul sens autour de l'anneau, et chaque périphérique agit comme un répéteur, transmettant les données au périphérique suivant. Certaines implémentations avancées utilisent un double anneau avec circulation inverse pour assurer une redondance, mais cela augmente significativement la complexité et le coût. Dans un tel cas, la topologie supporte jusqu'à un lien coupé, mais pas deux.

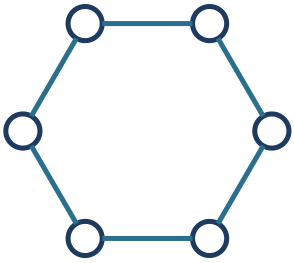


Fig. 10. – Illustration d'une topologie en anneau. Chaque point représente un périphérique du réseau.

La topologie en anneau fonctionne souvent avec un protocole de jeton, qui permet de réguler l'accès au réseau et d'éviter les collisions. Dans ce protocole, un jeton circule autour de l'anneau et seul le périphérique qui possède le jeton peut transmettre des données. Cela garantit que les données sont transmises de manière ordonnée et évite les conflits entre les périphériques.

2.4.3 Topologie en étoile

La topologie en étoile est la topologie la plus couramment utilisée dans les réseaux modernes. Dans cette topologie, tous les périphériques sont connectés à un périphérique d'interconnexion central. Si un lien tombe en panne, seul le périphérique concerné est affecté, et non l'ensemble du réseau. En revanche, le périphérique central représente un point de défaillance unique (« SPOF » pour « Single Point of Failure » en anglais). Si ce périphérique tombe en panne, l'ensemble du réseau est affecté. Cette topologie est facile à mettre en place et à maintenir, et elle offre de bonnes performances. Elle est parfois doublée (ou redondée) pour éviter le problème du SPOF, ce qui donne une étoile double (voir Fig. 11).

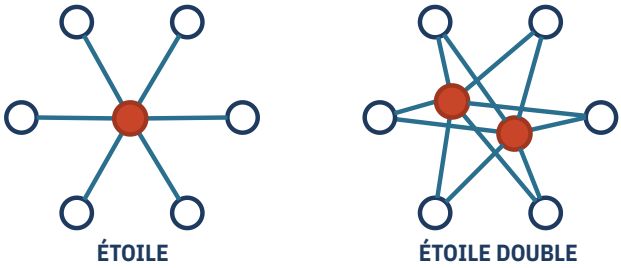


Fig. 11. – Illustration d'une topologie en étoile et d'une topologie en étoile double. Chaque point représente un périphérique du réseau.

2.4.4 Topologie maillée

La topologie maillée est la plus robuste de toutes les topologies, mais également la plus coûteuse. Dans cette topologie, chaque périphérique est connecté à tous les autres périphériques du réseau. Cela permet une redondance maximale, car si un périphérique tombe en panne, les données peuvent toujours circuler par d'autres chemins. Elle est généralement utilisée dans les réseaux de grande taille ou critiques, où la fiabilité est primordiale. Elle peut être complète (chaque périphérique est connecté à tous les autres) ou partielle (certains périphériques sont connectés à plusieurs autres, mais pas à tous), comme illustré par la Fig. 12. Internet est un exemple de réseau maillé partiel.

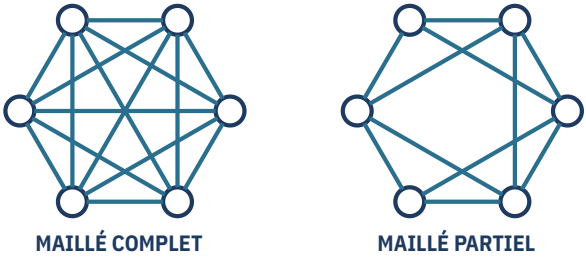


Fig. 12. – Illustration d'une topologie maillée. Chaque point représente un périphérique du réseau.

2.4.5 Topologie en arbre

La topologie en arbre (ou hiérarchique) est essentiellement un ensemble de topologies en étoile connectées entre elles, sous la forme d'une structure arborescente. Elle présente l'avantage de permettre une hiérarchisation des périphériques, ce qui facilite la gestion du réseau. Cependant, elle reste vulnérable aux pannes, car si un périphérique central tombe en panne, tous

les périphériques connectés à lui sont affectés. Cette topologie est souvent utilisée dans les réseaux d'entreprise ou les réseaux de campus.

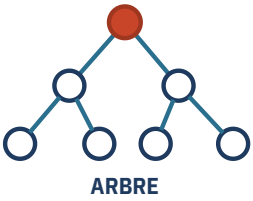


Fig. 13. – Illustration d'une topologie en arbre. Chaque point représente un périphérique du réseau.

2.4.6 Comparaison des topologies

Toutes les topologies ont leurs avantages et leurs inconvénients. Le Tableau 1 résume les principales caractéristiques de chaque topologie, en termes de coût, de fiabilité, de scalabilité (à quel point ce réseau peut être étendu facilement) et de difficulté de gestion.

Topo.	Avantages	Inconvénients	Exemples d'utilisation
Bus	Simple à mettre en place, peu coûteuse	Peu fiable, difficile à étendre	Anciens réseaux Ethernet (années 80-90)
Anneau	Accès déterministe, pas de collision (jeton)	Vulnérable aux pannes, complexe	Anciens réseaux Token Ring
Étoile	Facile à mettre en place et à maintenir, bonne performance	SPOF, nécessite un périphérique central	Réseaux locaux modernes
Maillée	Très robuste, redondance maximale	Coûteuse, complexe à mettre en place	Internet, réseaux critiques
Arbre	Hiérarchisation, facilité de gestion	La panne d'un nœud isole toute sa branche	Réseaux d'entreprise, réseaux de campus

Tableau 1. – Comparaison rapide des topologies principales

EXERCICE 2.4 · NOMBRE DE LIENS D'UN MAILLAGE COMPLET

A. Dans une topologie maillée complète de 6 périphériques, combien de liens sont nécessaires ?

B. Donnez la formule générale pour n périphériques.

C. Ce résultat explique l'un des inconvénients listés dans le Tableau 1. Lequel ?

2.5 Classification des réseaux

Un réseau est classé en fonction de sa taille. Les principales classes sont les réseaux locaux (LAN), les réseaux métropolitains (MAN) et les réseaux étendus (WAN). Le Tableau 2 présente les principales caractéristiques de chaque classe de réseau.

Classe	Nom complet	Portée (m)	Exemples d'utilisation
PAN	Personal Area Network	10^1	Bluetooth, casques audio, télécommandes
LAN	Local Area Network	10^3	Réseaux domestiques, réseaux d'entreprise
MAN	Metropolitan Area Network	10^4	Réseaux d'entreprise, réseaux de campus
WAN	Wide Area Network	10^6	Internet, réseaux interurbains
GAN	Global Area Network	10^7	Réseaux intercontinentaux, réseaux satellitaires

Tableau 2. – Classification des réseaux en fonction de leur taille

Un réseau local (LAN) est un réseau à l'échelle d'un bâtiment ou d'un site. Il couvre une zone géographique limitée et est généralement utilisé pour connecter des ordinateurs, des imprimantes et d'autres périphériques au sein d'une entreprise ou d'une maison. La gestion d'un LAN est souvent

privée et le débit de transmission est généralement élevé. Il existe une variante de LAN appelée WLAN (Wireless Local Area Network), qui utilise des technologies sans fil pour connecter les périphériques.

Un WAN est quant à lui à grande échelle, couvrant des zones géographiques étendues, comme des villes, des pays ou même des continents. Il est utilisé pour connecter plusieurs LAN entre eux et permet la communication entre des sites distants.

La Fig. 14 illustre les différences entre un réseau local (LAN) et un réseau étendu (WAN).

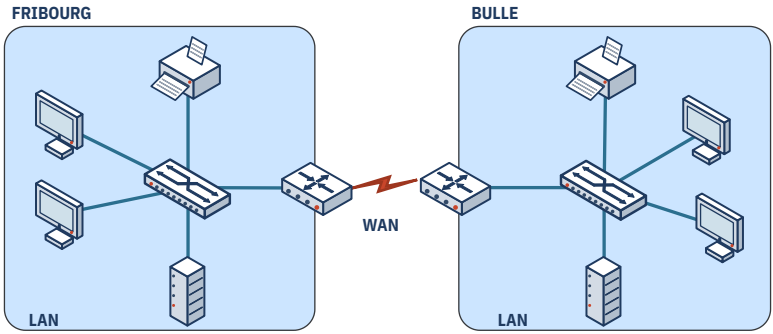


Fig. 14. – Illustration des différences entre un réseau local (LAN) et un réseau étendu (WAN). Dans cet exemple, une entreprise a un réseau local sur son site principal à Fribourg, et un autre réseau local sur son site secondaire à Bulle. Les deux sites sont connectés par un réseau étendu (WAN).

EXERCICE 2.5 · IDENTIFIER LA CLASSE DE RÉSEAU

Pour chaque exemple ci-dessous, identifiez la classe de réseau correspondante.

A. Un réseau domestique qui connecte plusieurs ordinateurs, smartphones et imprimantes dans une maison.

B. Un réseau d'entreprise qui connecte plusieurs bureaux dans une ville.

C. Une manette de jeu vidéo qui se connecte à la console de jeu via Bluetooth.

D. Le réseau de satellites de géolocalisation Galileo (« GPS » européen) qui permet la communication entre les satellites et les récepteurs sur Terre.

CHAPITRE 3

Binaire, hexadécimal et opérations logiques

OBJECTIFS DU CHAPITRE

À l'issue de ce chapitre, vous saurez :

- Définir les unités de mesure de l'information (bit, octet, kilo-octet, méga-octet, etc.)
- définir les systèmes de numération binaire et hexadécimal
- effectuer des conversions entre ces systèmes
- appliquer les opérations logiques de base (AND, OR, NOT, XOR)

Ce chapitre introduit les concepts fondamentaux de la logique binaire et des systèmes de numération utilisés en informatique et en téléinformatique. Il couvre les unités de mesure de l'information, les bases de la numération binaire et hexadécimale, ainsi que les opérations logiques de base qui sont essentielles pour la manipulation des données et la conception des circuits numériques. Il est important d'aborder ces concepts avant de plonger dans les protocoles de communication et les architectures réseau, car ils constituent le fondement de la compréhension des systèmes informatiques et des réseaux modernes.

3.1 Unités de mesure de l'information

Ce segment présente les unités de mesure de l'information, qui sont essentielles pour quantifier la taille des données et pour représenter une taille de stockage ou la quantité d'information transmise sur un réseau. Ces unités sont basées sur le bit, l'octet et leurs multiples.

3.1.1 Bit et octet

En informatique, l'information est mesurée en **bit** (pour binary digit), qui est l'unité de base. Un bit peut prendre deux valeurs : 0 ou 1. Cela est

lié à la nature binaire des systèmes informatiques, qui utilisent des états électriques (Off/On) pour représenter l'information.

Un ensemble de 8 bits constitue un **octet** (aussi appelé **byte** en anglais), qui est l'unité de mesure la plus couramment utilisée pour quantifier la taille des données.

> **APPROFONDISSEMENT** · Pourquoi 8 bits ?
>
> Pourquoi 8 bits ? Pourquoi pas 10 ? ou 100 ? La taille de 8 bits a été choisie pour des raisons historiques et pratiques. Elle permet de représenter 256 valeurs différentes (de 0 à 255), ce qui permet de coder un large éventail de caractères et de symboles, notamment dans les systèmes de codage comme ASCII; tout en restant suffisamment compacte pour être efficace en termes de stockage et de traitement.

Formellement, un byte n'est pas forcément égal à un octet, mais dans la pratique, ces deux termes sont souvent utilisés de manière interchangeable.

3.1.2 Ordres de grandeur

Les bits et les octets sont souvent regroupés en multiples pour représenter de plus grandes quantités d'information. Les multiples les plus courants sont le kilo-octet (Ko), le méga-octet (Mo), le giga-octet (Go), et ainsi de suite. Il est important de noter que ces multiples peuvent être basés sur des puissances de 10 ou de 2, ce qui peut prêter à confusion.

En suivant le système international d'unités (SI), les préfixes sont basés sur des puissances de 10 :

- 1 kilo-octet (Ko) = 1 000 octets
- 1 méga-octet (Mo) = 1 000 Ko = 1 000 000 octets
- 1 giga-octet (Go) = 1 000 Mo = 1 000 000 000 octets
- etc.

En revanche, on retrouve aussi des préfixes binaires, basés sur des puissances de 2 :

- 1 kibi-octet (Kio) = 1 024 octets
- 1 mébi-octet (Mio) = 1 024 Kio
- 1 gibi-octet (Gio) = 1 024 Mio

etc.

Il n'est pas rare de trouver les notations utilisant le **B** de **byte** pour les octets, et le **b** pour les bits, afin de distinguer clairement les deux unités.

3.1.3 Notations

Le Tableau 3 ci-dessous résume les principales unités de mesure de l'information, leurs symboles et leurs ordres de grandeur. Une « unité » peut être remplacée par un bit (**b**), un octet (**o**), ou un byte (**B**).

Unité	Symbole	Description	Ordre de grandeur
bit	**b**	unité fondamentale de l'information (0 ou 1)	
byte	**B**	8 bits	
octet	**o**	8 bits	
kilo	**k**	1 000 unités	10^3
méga	**M**	1 000 kilo	10^6
giga	**G**	1 000 méga	10^9
tera	**T**	1 000 giga	10^{12}
kibi	**Ki**	1 024 unités	2^{10}
mébi	**Mi**	1 024 kibi	2^{20}
gibi	**Gi**	1 024 mébi	2^{30}
tébi	**Ti**	1 024 gibi	2^{40}

Tableau 3. – Tableau des unités de mesure de l'information

EXERCICE 3.1 · CONVERSIONS

Convertir les quantités suivantes d'une unité à une autre:

A. 10 MB en Mb

B. 1000 kB en GB

C. 250 o en b

D. 1 Gb en GB

E. 500 ko en KiB

3.1.4 Débit

Un débit est la quantité d'information transmise par unité de temps. Il est généralement exprimé en bits par seconde (bit/s ou bps) ou en bytes par

seconde (B/s). Le débit peut varier en fonction de la technologie utilisée, de la qualité du canal de transmission et des protocoles de communication.

EXERCICE 3.2 · CALCUL DU TEMPS DE TÉLÉCHARGEMENT: MODEM 56K

Vous avez peut-être déjà entendu parler du modem 56k. Le « 56k » fait référence à un débit de 56 kilobits par seconde (kbps). En théorie, et avec une telle vitesse, combien de temps faudrait-il pour télécharger un PDF de 5 Mo ?

EXERCICE 3.3 · CALCUL DU TEMPS DE TÉLÉCHARGEMENT: FIBRE OPTIQUE

Une fibre optique peut offrir un débit de 1 Gbps. En théorie, combien de temps faudrait-il pour télécharger un PDF de 5 Mo ?

3.1.5 Latence

La latence est le temps nécessaire pour qu'un signal parcoure un canal de communication, de l'émetteur au récepteur. Elle est généralement mesurée en millisecondes (ms) et peut être influencée par divers facteurs tels que la distance, la qualité du canal, les protocoles utilisés et la congestion du réseau. Elle n'est pas à confondre avec le débit, qui mesure la quantité d'information transmise par unité de temps.

3.1.6 Résumé

Une quantité de données est mesurée en bits ou en octets, et peut être exprimée en multiples tels que kilo, méga, giga, etc. Le débit mesure la quantité d'information transmise par unité de temps, tandis que la latence mesure le temps nécessaire pour qu'un signal parcoure un canal de communication.

3.2 Représentation des nombres

Au cours de l'histoire, l'humanité a appris à compter et à représenter les nombres de différentes manières. Le système décimal est celui que nous utilisons le plus souvent dans la vie quotidienne. Pourquoi « décimal » ? Parce qu'il est basé sur 10 chiffres (0 à 9), probablement parce que nous avons 10 doigts.

Si on généralise, on parle de symbole à la place de chiffre, et de base à la place de dix. Ainsi, le système décimal est un système de base 10, utilisant

10 symboles (0 à 9). La position du symbole dans un nombre représente son poids, par rapport à la base. Le symbole le plus à droite a un poids de 1 (10^0), le suivant a un poids de 10 (10^1), puis 100 (10^2), et ainsi de suite. Par exemple, le nombre 305 en base 10 peut être décomposé comme ceci :

$$305 = 3 \times 10^2 + 0 \times 10^1 + 5 \times 10^0 = 300 + 0 + 5$$

ASTUCE

Si nous avons n positions à disposition pour représenter un nombre en base b, le nombre maximum que nous pouvons représenter est $b^n - 1$. Par exemple, avec 3 positions en base 10, le nombre maximum est $10^3 - 1 = 999$.

3.2.1 Binaire

Le binaire fonctionne de la même manière que le décimal, mais la base est **2**, et le nombre de symboles est également 2 : `0` et `1`. Chaque position dans un nombre binaire représente une puissance de 2, à partir de la droite.

Par exemple, le nombre binaire `1011` peut être décomposé comme ceci :

$$1011_2 = 1 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 1 \times 2^0 = 8 + 0 + 2 + 1 = 11_{10}$$

REMARQUE

Comment savoir si 101 est écrit en binaire ou en décimal ? 101 pourrait représenter le nombre cent un en décimal, ou le nombre cinq en binaire. Pour lever l'ambiguïté, on peut ajouter un indice à la base : 101_{10} pour le décimal, 101_2 pour le binaire ou encore 101_{16} pour l'hexadécimal. On peut aussi utiliser des préfixes (typiquement utilisé dans les langages de programmation) : 0b101 pour le binaire, 0x101 pour l'hexadécimal, et rien pour le décimal.

EXERCICE 3.4 · CONVERSION DE LA BASE 2 À LA BASE 10

Convertir les nombres suivants de la base 2 à la base 10:

A. 1011_2

B. 1101_2

C. 10010_2

D. 111111_2

ASTUCE
Apprenez par coeur les puissances de 2 de 2^0 à 2^{16}, elles vous serviront tout au long de votre vie professionnelle ! La suite est 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536.

EXERCICE 3.5 · VALEURS MAXIMALES SUR n BITS

A. Quelle est la plus grande valeur représentable sur 8 bits ? Sur 16 bits ?

B. Combien de bits faut-il au minimum pour représenter le nombre 1000 ?

3.2.2 Hexadécimal

La base 16, appelée **hexadécimal**, utilise 16 symboles : les chiffres de 0 à 9 et les lettres de A à F (ou a à f) pour représenter les valeurs de 10 à 15. Elle est souvent utilisée en informatique pour représenter des valeurs binaires de manière plus compacte, car chaque chiffre hexadécimal correspond à 4 bits (un **nibble**). Voici un exemple de nombre hexadécimal et sa décomposition mathématique :

$$2F_{16} = 2 \times 16^1 + F \times 16^0 = 2 \times 16 + 15 \times 1 = 32 + 15 = 47_{10}$$

La Tableau 4 montre les symboles hexadécimaux et leurs équivalents décimaux et binaires.

ASTUCE
Pour convertir un nombre hexadécimal en binaire, il suffit de remplacer chaque chiffre hexadécimal par son équivalent binaire à 4 bits. Par exemple, pour convertir le nombre hexadécimal `2F` en binaire, on remplace `2` par `0010` et `F` par `1111`, ce qui donne `00101111`.

Valeur hexadécimale	Valeur décimale	Valeur binaire
0	0	0000
1	1	0001
2	2	0010
3	3	0011

Valeur hexadécimale	Valeur décimale	Valeur binaire
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
A	10	1010
B	11	1011
C	12	1100
D	13	1101
E	14	1110
F	15	1111

Tableau 4. – Tableau des symboles hexadécimaux et leurs équivalents décimaux et binaires

EXERCICE 3.6 · CONVERSION DE LA BASE 16 AUX BASES 10 ET 2

Convertir les nombres suivants de la base 16 aux bases 10 et 2:

A. $1\mathrm{A}_{16}$

B. FF_{16}

C. $2\mathrm{B}_{16}$

D. $\mathrm{C3}_{16}$

3.2.3 Conversion de la base 10 à la base 2 et 16

Convertir un nombre de base 2 ou 16 à la base 10 est assez intuitif, on fait la somme des produits de chaque chiffre par sa puissance de base. La conversion inverse, de la base 10 à la base 2 ou 16, est un peu plus complexe et nécessite l'utilisation de divisions successives.

La méthode générale pour convertir un nombre décimal en binaire ou hexadécimal est la suivante :

1. Trouver la plus grande puissance de la base cible (2 pour binaire, 16 pour hexadécimal) qui est inférieure ou égale au nombre décimal.
2. Soustraire cette puissance du nombre décimal et noter le chiffre correspondant (1 pour binaire, le chiffre hexadécimal pour hexadécimal).
3. Répéter le processus avec le reste jusqu'à ce que le reste soit zéro.

Comme en notation décimale, des zéros peuvent être ajoutés à gauche pour compléter le nombre à un certain nombre de bits ou de chiffres hexadécimaux, si nécessaire. Ils n'ont aucune valeur et ne changent pas le nombre représenté (ce qui n'est pas le cas pour les zéros à droite, qui eux, changent la valeur du nombre).

$00000010_2 = 10_2 = 2_{10} = 00000002_{10} = 2_{16} = 002_{16}$

ATTENTION

La représentation octale (base 8) est rarement utilisée dans la programmation moderne, bien qu'on la retrouve encore dans certaines configurations (comme les permissions Unix/Linux : chmod 755) et quelques langages hérités. Historiquement, plusieurs langages utilisaient le préfixe « 0 » seul pour désigner un nombre octal — ainsi, 010 correspondrait à 8 en décimal ($1 \times 8 + 0$), non 10. Cependant, cette notation pose des risques d'erreur : Python 3 exige désormais 0o10, JavaScript (ES6+) préfère aussi 0o au lieu du simple 0. Pour éviter toute ambigüité, privilégiez donc 0o quand vous écrivez littéraux octaux, et évitez de remplir arbitrairement des valeurs numériques de zéros à gauche, sauf si requis par un formatage spécifique.

EXEMPLE 3.1 · CONVERSION DE LA BASE 10 À LA BASE 2

Nous souhaitons convertir le nombre décimal 45 en binaire.

Premièrement on se pose la question « Quelle est la plus grande puissance de 2 qui entre entièrement dans 45 ? 64 est trop grand, 32 est parfait. Donc on note un 1 pour la puissance de 2^5 (32).

Pour l'instant nous avons : 1xxxx_2

Ensuite, on soustrait 32 de 45, ce qui nous laisse avec 13. La plus grande puissance de 2 qui entre dans 13 est 8 (2^3), donc on note un 1 pour la puissance de 2^3. La puissance entre 32 et 8 est 16 (2^4), qui ne rentre pas dans 13, donc on note un 0 pour la puissance de 2^4.

Nous avons maintenant : 101xx_2

On soustrait 8 de 13, ce qui nous laisse avec 5. La plus grande puissance de 2 qui entre dans 5 est 4 (2^2), donc on note un 1 pour la puissance de 2^2.

Nous avons maintenant : 1011x_2

On soustrait 4 de 5, ce qui nous laisse avec 1. La plus grande puissance de 2 qui entre dans 1 est 1 (2^0), donc on note un 1 pour la puissance de 2^0.

Il n'y a pas de reste, donc on arrête ici. Ainsi, le nombre binaire correspondant à 45 est 101101_2. On peut vérifier cela en calculant la valeur décimale de 101101_2 : $1 \times 2^5 + 0 \times 2^4 + 1 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0 = 32 + 0 + 8 + 4 + 0 + 1 = 45$.

EXERCICE 3.7 · CONVERSION DE LA BASE 10 AUX BASES 2 ET 16

Convertir les nombres décimaux suivants :

A. 100_{10} en binaire

B. 173_{10} en binaire

C. 255_{10} en binaire

D. 300_{10} en hexadécimal

E. 4096_{10} en hexadécimal

3.3 Opérations logiques

Un opérateur logique (ou porte logique) est un dispositif qui prend une ou plusieurs entrées binaires (0 ou 1) et produit une sortie binaire en fonction d'une règle logique spécifique. Les opérateurs logiques sont fondamentaux en informatique et en électronique numérique, car ils permettent de manipuler des données binaires et de prendre des décisions basées sur des conditions.

ANECDOTE · Porte logique dans Minecraft

Vous avez peut-être déjà joué à Minecraft, auquel cas vous connaissez sûrement la Redstone. Cet élément du jeu permet de créer des circuits logiques. La Fig. 15 montre un exemple de porte AND réalisée avec de la Redstone dans Minecraft. Les portes logiques dans le jeu fonctionnent de manière similaire à leurs homologues dans le monde réel, permettant aux joueurs de créer des mécanismes complexes et des systèmes automatisés.

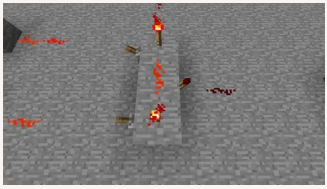


Fig. 15. – Porte AND dans Minecraft

L'ensemble des règles logiques qu'applique un opérateur logique peut être représenté sous forme de table de vérité. Une table de vérité énumère toutes les combinaisons possibles d'entrées et les sorties correspondantes pour un opérateur logique donné. Cela permet de visualiser et de comprendre le comportement de l'opérateur dans différentes situations. Dans ce document et dans le cours, nous nous concentrerons sur les quatre opérateurs logiques de base : AND, OR, NOT et XOR. Nous considérons le cas de deux entrées binaires, mais ces opérateurs peuvent être étendus à plus d'entrées si nécessaire (sauf pour NOT, qui n'a qu'une seule entrée, et le XOR, qui est souvent défini pour deux entrées).

3.3.1 Opérateur ET (AND)

L'opérateur logique ET (AND) nécessite que les deux entrées soient vraies (1) pour que la sortie soit vraie (1). Si l'une ou les deux entrées sont fausses

(0), la sortie sera fausse (0). La table de vérité pour l'opérateur AND est la suivante :

Entrée A	Entrée B	Sortie A AND B
0	0	0
0	1	0
1	0	0
1	1	1

Tableau 5. – Table de vérité pour l'opérateur AND

L'opérateur AND est aussi appelé l'intersection logique, ou le produit logique. Il est noté `AND`, `·`, `&`, ou encore `∧` selon le contexte.

3.3.2 Opérateur OU (OR)

L'opérateur logique OU (OR) nécessite qu'au moins une des deux entrées soit vraie (1) pour que la sortie soit vraie (1). Si les deux entrées sont fausses (0), la sortie sera fausse (0). La table de vérité pour l'opérateur OR est la suivante :

Entrée A	Entrée B	Sortie A OR B
0	0	0
0	1	1
1	0	1
1	1	1

Tableau 6. – Table de vérité pour l'opérateur OR

L'opérateur OR est aussi appelé l'union logique, ou la somme logique. Il est noté `OR`, `+`, ou encore `∨` selon le contexte.

3.3.3 Opérateur NON (NOT)

L'opérateur logique NON (NOT) prend une seule entrée et inverse sa valeur. Si l'entrée est vraie (1), la sortie sera fausse (0), et si l'entrée est fausse (0), la sortie sera vraie (1). La table de vérité pour l'opérateur NOT est la suivante :

Entrée A	Sortie NOT A
0	1

Entrée A	Sortie NOT A
1	0

Tableau 7. – Table de vérité pour l'opérateur NOT

L'opérateur NOT est aussi appelé la négation logique, ou l'inverse logique. Il est noté `NOT`, `!`, ou encore `¬` selon le contexte. En algèbre booléenne, il est souvent représenté par une barre au-dessus de la variable (par exemple, $\overline{A}$ pour NOT A).

3.3.4 Opérateur OU exclusif (XOR)

L'opérateur logique OU exclusif (XOR) nécessite que les deux entrées soient différentes pour que la sortie soit vraie (1). Si les deux entrées sont identiques (les deux vraies ou les deux fausses), la sortie sera fausse (0). La table de vérité pour l'opérateur XOR est la suivante :

Entrée A	Entrée B	Sortie A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

Tableau 8. – Table de vérité pour l'opérateur XOR

Le OU exclusif est noté `XOR`, `^`, ou encore `⊕` selon le contexte. Il est souvent utilisé dans les opérations de cryptographie.

APPROFONDISSEMENT · Autres portes logiques

D'autres portes logiques existent, comme NAND, NOR, XNOR, etc. Elles sont souvent utilisées dans la conception de circuits numériques et peuvent être combinées pour créer des fonctions logiques plus complexes. Elles ne sont pas abordées dans ce cours, mais vous pouvez les explorer si vous le souhaitez.

3.3.5 Opérations sur plusieurs bits

Il est possible d'appliquer un opérateur logique sur un ensemble de bits en appliquant l'opérateur sur chaque paire de bits correspondants. Par exemple, si nous avons deux mots binaires de 4 bits chacun :

$A = 1010_2, B = 1100_2$

$A \text{ AND } B = 1000_2$

On appelle souvent cet ensemble de bits un **mot binaire** (**machine word** ou simplement **word** en anglais). Les opérations logiques sur des mots binaires sont courantes en programmation basse niveau, notamment pour la manipulation de masques, le chiffrement simple, ou la compression de données.

REMARQUE

Opération bitwise: Ce terme technique décrit les opérations qui agissent bit par bit sur des mots entiers, plutôt que sur des nombres considérés comme des valeurs arithmétiques globales.

REMARQUE

La notion de **mot** dépend de l'architecture : sur un processeur 32 bits, un **word** correspond généralement à 32 bits et un **half-word** à 16 bits. Dans ces exemples, nous utiliserons des mots de 4 bits pour simplifier les calculs et les représentations.

EXERCICE 3.8 · OPÉRATEURS LOGIQUES FONDAMENTAUX

Appliquez les opérateurs logiques suivants. Calculez le résultat final pour chaque opération ci-dessous:

A. $0 \text{ AND } 1$

B. $1 \text{ XOR } 0$

C. $(0 \text{ AND } 1) \text{ OR } (1 \text{ XOR } 0)$

D. $1 \text{ AND } (0 \text{ OR } 1)$

E. $(1 \text{ XOR } 1) \text{ OR } (0 \text{ AND } 1)$

EXERCICE 3.9 · OPÉRATEURS LOGIQUES SUR DES MOTS BINAIRES

Appliquez les opérateurs logiques sur les mots binaires suivants. Calculez le résultat final pour chaque opération ci-dessous, avec $A = 1010_2$, $B = 1100_2$, et $C = 0110_2$:

A. A AND B

B. A XOR C

C. $(A$ OR $B)$ AND C

D. $(A$ XOR $B)$ OR $(B$ AND $C)$

E. $(A$ AND $C)$ XOR $(B$ OR $C)$

ASTUCE

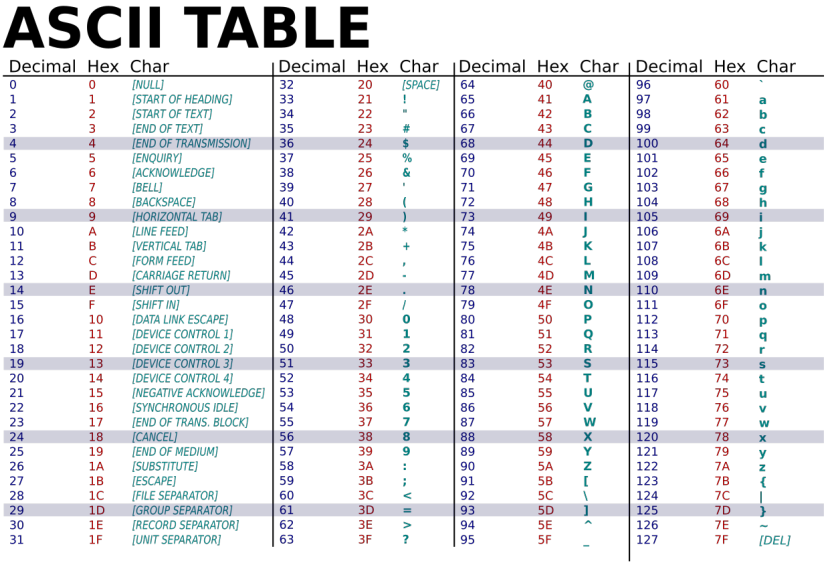
Pour mémoriser rapidement les tables de vérité, associez les opérateurs à leur nom français :

- ET (AND) demande que TOUT soit vrai: sortie 1 seulement si tout est 1
- OU (OR) accepte qu'UN SEUL soit vrai: sortie 0 seulement si tout est 0
- NON (NOT) est un simple inverseur
- XOR signifie « l'un ou l'autre mais pas les deux »: sortie 1 si différents

3.4 Encodage ASCII

L'informatique ne traite que des nombres binaires, mais nous avons besoin de représenter des caractères lisibles par l'homme. Comment faire cela ? C'est là qu'intervient l'encodage de caractères. L'un des encodages les plus connus est l'ASCII (American Standard Code for Information Interchange), qui a été développé dans les années 1960 pour standardiser la représentation des caractères dans les systèmes informatiques. Il utilise 7 bits pour représenter chaque caractère, permettant de coder 128 caractères différents, incluant les lettres majuscules et minuscules, les chiffres, la ponctuation et certains caractères de contrôle. Etant destiné à l'anglais, il ne contient pas de caractères accentués. L'ASCII étendu utilise 8 bits pour représenter 256 caractères, incluant des symboles supplémentaires et des caractères accentués pour certaines langues européennes. De nos jours, les encodages plus modernes comme UTF-8 sont largement utilisés, car ils permettent de représenter un plus grand nombre de caractères, y compris ceux des langues non latines.

En ASCII, chaque caractère est associé à un code numérique unique. Par exemple, le caractère “A” est représenté par le code 65 en décimal, ou 01000001 en binaire. La Fig. 16 montre la table ASCII sur 7 bits, avec les codes décimaux correspondants pour chaque caractère.



ASCII TABLE

Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char
0	0	[NULL]	32	20	[SPACE]	64	40	@	96	60	`
1	1	[START OF HEADING]	33	21	!	65	41	A	97	61	a
2	2	[START OF TEXT]	34	22	"	66	42	B	98	62	b
3	3	[END OF TEXT]	35	23	#	67	43	C	99	63	c
4	4	[END OF TRANSMISSION]	36	24	$	68	44	D	100	64	d
5	5	[ENQUIRY]	37	25	%	69	45	E	101	65	e
6	6	[ACKNOWLEDGE]	38	26	&	70	46	F	102	66	f
7	7	[BELL]	39	27	'	71	47	G	103	67	g
8	8	[BACKSPACE]	40	28	(	72	48	H	104	68	h
9	9	[HORIZONTAL TAB]	41	29	)	73	49	I	105	69	i
10	A	[LINE FEED]	42	2A	*	74	4A	J	106	6A	j
11	B	[VERTICAL TAB]	43	2B	+	75	4B	K	107	6B	k
12	C	[FORM FEED]	44	2C	,	76	4C	L	108	6C	l
13	D	[CARRIAGE RETURN]	45	2D	-	77	4D	M	109	6D	m
14	E	[SHIFT OUT]	46	2E	.	78	4E	N	110	6E	n
15	F	[SHIFT IN]	47	2F	/	79	4F	O	111	6F	o
16	10	[DATA LINK ESCAPE]	48	30	0	80	50	P	112	70	p
17	11	[DEVICE CONTROL 1]	49	31	1	81	51	Q	113	71	q
18	12	[DEVICE CONTROL 2]	50	32	2	82	52	R	114	72	r
19	13	[DEVICE CONTROL 3]	51	33	3	83	53	S	115	73	s
20	14	[DEVICE CONTROL 4]	52	34	4	84	54	T	116	74	t
21	15	[NEGATIVE ACKNOWLEDGE]	53	35	5	85	55	U	117	75	u
22	16	[SYNCHRONOUS IDLE]	54	36	6	86	56	V	118	76	v
23	17	[END OF TRANS. BLOCK]	55	37	7	87	57	W	119	77	w
24	18	[CANCEL]	56	38	8	88	58	X	120	78	x
25	19	[END OF MEDIUM]	57	39	9	89	59	Y	121	79	y
26	1A	[SUBSTITUTE]	58	3A	:	90	5A	Z	122	7A	z
27	1B	[ESCAPE]	59	3B	;	91	5B	[	123	7B	{
28	1C	[FILE SEPARATOR]	60	3C	<	92	5C	\	124	7C	|
29	1D	[GROUP SEPARATOR]	61	3D	=	93	5D	]	125	7D	}
30	1E	[RECORD SEPARATOR]	62	3E	>	94	5E	^	126	7E	~
31	1F	[UNIT SEPARATOR]	63	3F	?	95	5F	_	127	7F	[DEL]

Fig. 16. – Table ASCII, https://commons.wikimedia.org/wiki/File:ASCII-Table-wide.svg

EXERCICE 3.10 · DÉCODAGE D’UN MESSAGE BINAIRE EN ASCII

Décoder ce mystérieux message binaire, à l’aide de la table ASCII :

01000010 01110010 01100001 01110110 01101111 00100001

EXERCICE 3.11 · ENCODAGE D’UN MESSAGE EN ASCII

À l’aide de la table ASCII, encodez le message « Ok! » en binaire.

CHAPITRE 4

Protocoles et modèles en couches

OBJECTIFS DU CHAPITRE

À l'issue de ce chapitre, vous saurez :

- définir la notion de protocole et citer des exemples de protocoles
- définir le modèle OSI et citer ses couches
- définir le modèle TCP/IP et citer ses couches
- décrire le rôle des couches dans un modèle en couches
- citer les principaux protocoles et normes associés à chaque couche
- citer les principaux organismes de normalisation et leurs rôles
- décrire le principe d'encapsulation et de décapsulation des données

Le monde de la téléinformatique, et de l'informatique en général, est régi par des protocoles. Un protocole est **un ensemble de règles et de conventions** qui définissent comment les données sont transmises et reçues entre les différents périphériques d'un réseau. Les protocoles permettent aux périphériques de communiquer efficacement et de manière fiable, quel que soit le fabricant ou le système d'exploitation utilisé. Il existe de nombreux protocoles, chacun ayant des fonctions spécifiques et étant utilisé dans différents contextes. Par exemple, le protocole HTTP est utilisé pour la communication entre les navigateurs web et les serveurs web, tandis que le protocole FTP est utilisé pour le transfert de fichiers entre les périphériques.

DÉFINITION 4.1 · PROTOCOLE

Ensemble de règles définissant le mode de communication entre deux ordinateurs.

- Larousse.fr

Un réseau informatique est souvent représenté sous forme de couches, chaque couche ayant des fonctions spécifiques et communiquant avec les couches adjacentes. Cette approche en couches permet de simplifier la conception et la mise en oeuvre des réseaux, tout en assurant la compatibilité entre les différents périphériques et protocoles. Les deux modèles de référence les plus connus sont le modèle OSI (Open Systems Interconnection) et le modèle TCP/IP (Transmission Control Protocol/Internet Protocol). Ces modèles définissent les différentes couches d'un réseau et les protocoles associés à chaque couche.

4.1 Modèle OSI

Le modèle OSI (pour « Open Systems Interconnection ») est le modèle de référence, défini par l'ISO (International Organization for Standardization) en 1984. Il est composé de sept couches, chacune ayant des fonctions spécifiques et communiquant avec les couches adjacentes. Les sept couches du modèle OSI sont, de la couche la plus basse à la couche la plus haute : la couche physique, la couche liaison de données, la couche réseau, la couche transport, la couche session, la couche présentation et la couche application.

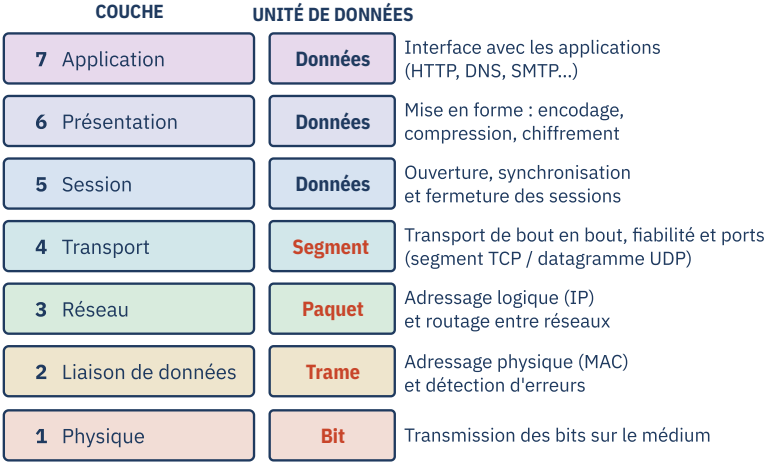


Fig. 17. – Les sept couches du modèle OSI, de la couche physique à la couche application. Chaque couche est responsable d'une partie spécifique du processus de communication et utilise des protocoles spécifiques pour accomplir ses fonctions.

Chaque couche est responsable d'une partie spécifique du processus et est conçue pour dialoguer avec son homologue sur l'autre périphérique, comme si une liaison virtuelle était établie entre elles. Une couche fournit des services à la couche supérieure et utilise les services de la couche inférieure.

Un tel modèle a pour but de promouvoir des normes universelles, d'assurer la compatibilité entre les différents constructeurs, de réaliser des systèmes ouverts et de faciliter la compréhension des réseaux. De plus, il permet de décomposer les problèmes complexes en sous-problèmes plus simples et de garantir l'interconnexion grâce à des interfaces normalisées et standardisées entre les couches, ce qui assure la cohérence globale du système.

Les quatre premières couches du modèle OSI (couches 1 à 4) sont appelées les couches basses, tandis que les trois dernières couches (couches 5 à 7) sont appelées les couches hautes. Les couches basses sont responsables de la transmission des données sur le réseau, tandis que les couches hautes sont responsables de la gestion des applications et des services utilisés par les utilisateurs finaux.

> **ASTUCE**
> Il existe des phrases mnémotechniques pour se souvenir de l'ordre des couches du modèle OSI. Par exemple, la phrase « Petit Lapin Rose Trouvé à la SPA » permet de se souvenir de l'ordre des couches : Physique, Liaison de données, Réseau, Transport, Session, Présentation et Application. Une autre phrase mnémotechnique est « Please Do Not Throw Sausage Pizza Away », qui correspond aux initiales des couches en anglais : Physical, Data Link, Network, Transport, Session, Presentation et Application.

Chaque couche du modèle OSI a sa propre PDU (Protocol Data Unit), qui est l'unité de données utilisée par cette couche pour communiquer avec les autres couches. La PDU de la couche physique est le bit, celle de la couche liaison de données est la trame, celle de la couche réseau est le paquet, celle de la couche transport est le segment, et les PDU des couches session, présentation et application sont les messages (ou « Data »). Cette distinction est importante car elle permet de comprendre et de mettre en lumière les principes d'encapsulation et de décapsulation des données, qui sont essentiels pour la communication entre les périphériques d'un réseau (voir Chapitre 4.3).

REMARQUE
Pour parler des couches du modèle OSI, on utilise souvent l'acronyme «Lx» pour «Layer» + le numéro de la couche. Par exemple «L1» désigne la couche physique, L4 la couche transport, etc.

4.1.1 Couche 1 : Physique

La couche physique est responsable de la transmission des bits sur le support physique. Elle transmet les bits bruts et ne s'occupe ni de la signification des données ni de la gestion des erreurs de transmission (c'est le rôle des couches supérieures). Son rôle est de s'assurer de suivre les spécifications du support physique utilisé pour la transmission des données, comme le type de câble, la vitesse de transmission, le codage des signaux, etc.

Sur la couche 1, on peut citer des normes comme Ethernet (IEEE 802.3), Wi-Fi (IEEE 802.11), Bluetooth (IEEE 802.15.1), USB (Universal Serial Bus), et les normes de câblage comme Cat5e, Cat6, et fibre optique. La PDU de cette couche est le bit.

4.1.2 Couche 2 : Liaison de données

La couche liaison de données fournit aux couches supérieures un service de communication sur un lien physique. Elle est responsable de la détection des erreurs de transmission (mais aucune correction n'est effectuée, une trame erronée est simplement rejetée), ainsi que de la gestion des adresses physiques (adresses MAC) pour identifier les périphériques sur le réseau. Elle organise les bits reçus de la couche physique en trames et assure leur livraison correcte à la couche réseau.

Cette couche permet également de gérer l'accès au support physique partagé, en utilisant des protocoles d'accès au média comme CSMA/CD (Carrier Sense Multiple Access with Collision Detection) pour Ethernet ou CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) pour les réseaux sans fil. Le PDU de cette couche est la trame.

4.1.3 Couche 3 : Réseau

La couche réseau, comme son nom l'indique, ajoute la notion de réseau à la communication. Lorsque des machines deviennent distantes, il n'est plus possible de se contenter d'envoyer des trames sur un lien physique. Il faut désormais savoir comment atteindre la machine distante, et c'est le rôle de la couche réseau. Elle est responsable de l'adressage logique et du routage des paquets de données entre les périphériques sur différents réseaux. La notion de routage apparaît à ce niveau, qui désigne le processus de déter-

mination du chemin optimal pour acheminer les paquets de données d'un périphérique source à un périphérique de destination à travers un réseau.

En plus de ces notions, elle gère la fragmentation et le réassemblage des paquets de données. Les protocoles les plus connus de cette couche sont IPv4, IPv6, ICMP (sert à faire des « ping ») ou encore RIP et OSPF qui sont des protocoles de routage. La PDU de cette couche est le paquet.

4.1.4 Couche 4 : Transport

La couche transport assure la communication de bout en bout entre les applications des périphériques source et destination. Elle introduit la notion de port, qui permet d'identifier les applications sur les périphériques. Elle est responsable de la segmentation et du réassemblage des données, ainsi que de la gestion de la fiabilité et du contrôle de flux. Les protocoles les plus connus de cette couche sont TCP (Transmission Control Protocol) et UDP (User Datagram Protocol). La PDU de cette couche est le segment.

TCP est le protocole qui permet d'assurer une communication fiable, orientée connexion, avec contrôle de flux et retransmission des segments perdus. Il est utilisé pour les applications nécessitant une transmission fiable des données, comme le web (HTTP/HTTPS), le courrier électronique (SMTP, IMAP, POP3) et le transfert de fichiers (FTP).

UDP, quant à lui, est un protocole qui permet d'assurer une communication non fiable, mais rapide (faible overhead et faible latence). Il est utilisé pour les applications nécessitant une transmission rapide des données, comme le streaming vidéo et audio, les jeux en ligne et la VoIP (Voice over IP). L'unité de données est le segment lorsque l'on parle de TCP, et le datagramme lorsque l'on parle d'UDP. Cependant, dans le contexte du modèle OSI, on parle de segment pour les deux protocoles.

4.1.5 Couche 5 : Session

La couche session est responsable de l'établissement, de la gestion et de la terminaison des sessions de communication entre les applications des périphériques source et destination. Elle est aujourd'hui la plus floue des couches du modèle OSI, car elle est souvent implémentée dans les couches supérieures. Elle gère la synchronisation des échanges de données, la reprise après une interruption de communication et la gestion des dialogues entre les applications. Les protocoles de cette couche sont des protocoles comme NetBIOS, RPC ou encore SOCKS. La PDU de cette couche est le message (ou « Data »).

4.1.6 Couche 6 : Présentation

La couche présentation est responsable de l'encodage / décodage des données, de la compression et du chiffrement. Elle assure que les données transmises par la couche application sont compréhensibles par la couche application du périphérique de destination. Comme la couche 5, elle est souvent implémentée dans la couche supérieure. Les couches présentation et session sont souvent regroupées dans la couche application, car elles sont étroitement liées aux applications et aux services utilisés par les utilisateurs finaux. Les protocoles de cette couche sont des protocoles comme SSL/TLS, JPEG, MPEG ou encore ASCII. La PDU de cette couche est le message (ou « Data »).

4.1.7 Couche 7 : Application

La couche application est la couche la plus proche de l'utilisateur final. Elle fournit des services et des interfaces pour les applications et les utilisateurs, permettant l'accès aux ressources du réseau. Elle est responsable de la communication entre les applications des périphériques source et destination, ainsi que de la gestion des protocoles de communication utilisés par ces applications. Les protocoles de cette couche sont des protocoles comme HTTP, FTP, SMTP, DNS ou encore SSH. La PDU de cette couche est le message (ou « Data »).

4.1.8 Résumé des couches du modèle OSI

Le Tableau 9 résume les principales caractéristiques de chaque couche du modèle OSI, y compris son rôle, les protocoles associés et la PDU correspondante. Les exemples de protocoles et de normes mentionnés dans le tableau ne sont pas exhaustifs, mais illustrent les protocoles les plus couramment utilisés pour chaque couche.

Couche	Rôle	Exemples de protocoles / normes	PDU
Physique	Transmission des bits sur le support physique	Ethernet (802.3), Wi-Fi (802.11)	Bit

Couche	Rôle	Exemples de protocoles / normes	PDU
Liaison de données	Communication sur un lien physique, gestion des adresses MAC et de l'accès au support physique partagé	Ethernet (802.3), Wi-Fi (802.11), CSMA/CD	Trame
Réseau	Adressage logique et routage des paquets de données entre les périphériques sur différents réseaux	IPv4, IPv6, ICMP, RIP, OSPF	Paquet
Transport	Communication de bout en bout entre les applications des périphériques source et destination, segmentation et réassemblage des données, gestion de la fiabilité et du contrôle de flux	TCP, UDP	Segment
Session	Établissement, gestion et terminaison des sessions de communication entre les applications des périphériques source et destination	NetBIOS, RPC, SOCKS	Message

Couche	Rôle	Exemples de protocoles / normes	PDU
Présentation	Encodage / décodage des données, compression et chiffrement	SSL/TLS, JPEG, MPEG, ASCII	Message
Application	Fourniture de services et d'interfaces pour les applications et les utilisateurs finaux, communication entre les applications des périphériques source et destination	HTTP, FTP, SMTP, DNS, SSH	Message

Tableau 9. – Résumé des couches du modèle OSI, de la couche physique à la couche application. Chaque couche est décrite avec son rôle, les protocoles associés et la PDU correspondante.

EXERCICE 4.1 · ASSOCIER LES ÉLÉMENTS AUX COUCHES OSI

Pour chaque élément ci-dessous, indiquez la couche du modèle OSI à laquelle il appartient.

A. Le protocole HTTP

B. Une adresse MAC

C. Le protocole TCP

D. Un câble Cat 6

E. Le protocole IP

F. La compression d'une image JPEG

G. La notion de port

4.1.9 Exemple concret : Obtenir une page web

Que se passe-t-il lorsque vous tapez l'adresse d'un site web dans votre navigateur et appuyez sur « Entrée » ? Le processus de communication entre

votre navigateur web et le serveur web implique toutes les couches du modèle OSI, comme illustré par la Fig. 18.

Dans cet exemple, un utilisateur demande une page web en tapant l'URL dans son navigateur. Le navigateur utilise le protocole HTTP (couche application) pour envoyer une requête au serveur web. La requête est ensuite segmentée par la couche transport (TCP), encapsulée dans un paquet par la couche réseau (IP), et enfin encapsulée dans une trame par la couche liaison de données (Ethernet). La trame est transmise sur le support physique par la couche physique (câble Ethernet ou Wi-Fi). De l'autre côté de la chaîne, la requête est décapsulée couche par couche jusqu'à ce que le serveur web reçoive la requête HTTP et renvoie la page web demandée. Le processus inverse se produit pour la réponse du serveur, qui est transmise de la même manière jusqu'à ce que le navigateur affiche la page web à l'utilisateur.

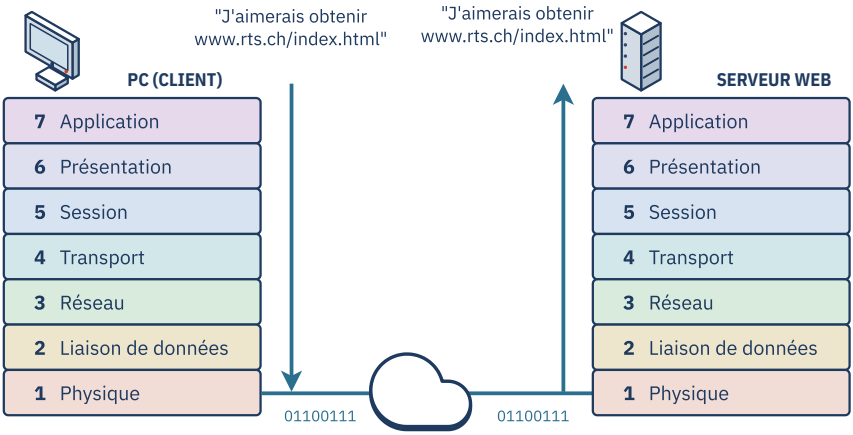


Fig. 18. – Exemple concret d'utilisation du modèle OSI pour obtenir une page web. Chaque couche du modèle OSI est impliquée dans le processus de communication entre le navigateur web et le serveur web, en utilisant les protocoles appropriés à chaque couche. Des bits sont transmis sur le médium physique.

4.2 Modèle TCP/IP

Le modèle TCP/IP (pour « Transmission Control Protocol/Internet Protocol ») est le modèle de référence utilisé pour Internet. Il s'agit d'un modèle simplifié en quatre couches à la place de sept couches. Les quatre

couches du modèle TCP/IP sont, de la plus basse à la plus haute, la couche d'accès réseau, la couche Internet, la couche transport et la couche application. Chaque couche du modèle TCP/IP correspond à une ou plusieurs couches du modèle OSI, comme illustré par la Fig. 19.

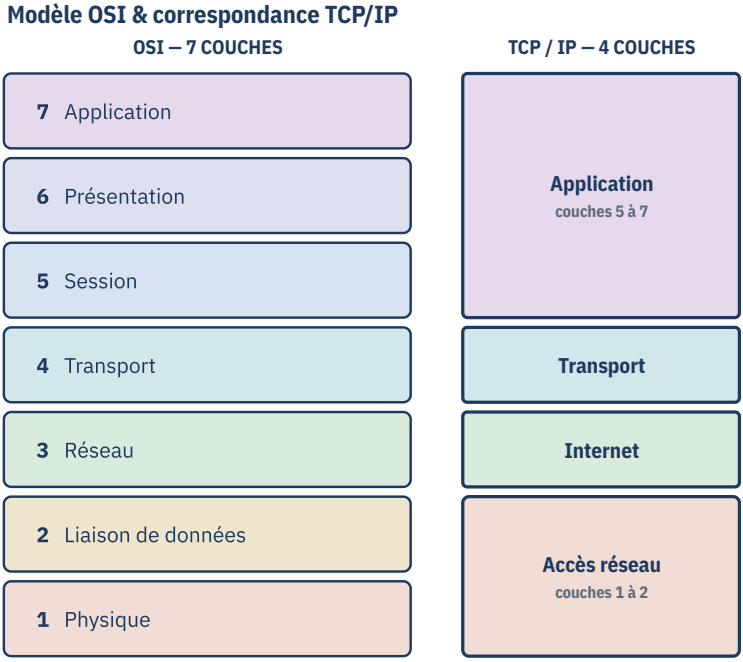


Fig. 19. – Comparaison entre le modèle OSI et le modèle TCP/IP. Le modèle OSI comporte sept couches, tandis que le modèle TCP/IP en comporte quatre. Chaque couche du modèle TCP/IP correspond à une ou plusieurs couches du modèle OSI.

Le Tableau 10 résume les principaux protocoles et normes associés à chaque couche du modèle TCP/IP.

Couche	Rôle	Exemples de protocoles / normes
Accès réseau	Transmission des bits sur le support physique et communication sur un lien physique	Ethernet (802.3), Wi-Fi (802.11), CSMA/CD

Couche	Rôle	Exemples de protocoles / normes
Internet	Adressage logique et routage des paquets de données entre les périphériques sur différents réseaux	IPv4, IPv6, ICMP, RIP, OSPF
Transport	Communication de bout en bout entre les applications des périphériques source et destination, segmentation et réassemblage des données, gestion de la fiabilité et du contrôle de flux	TCP, UDP
Application	Fourniture de services et d'interfaces pour les applications et les utilisateurs finaux, communication entre les applications des périphériques source et destination	HTTP, FTP, SMTP, DNS, SSH

4.2.1 Différences fondamentales entre les modèles OSI et TCP/IP

OSI est un modèle **théorique** utilisé pour comprendre le fonctionnement des réseaux et la communication entre les périphériques. Il est utilisé comme référence pour la conception et l'implémentation des protocoles de communication. TCP/IP, quant à lui, est un modèle **pratique** utilisé pour la communication sur Internet. Il est basé sur un ensemble de protocoles standardisés qui permettent aux périphériques de communiquer efficacement et de manière fiable sur Internet.

Attention toutefois, il ne faut pas voir TCP/IP comme une « implémentation » du modèle OSI. Il s'agit de deux modèles différents, chacun ayant ses propres caractéristiques et objectifs. Les deux ont été développés indépendamment et ont évolué séparément au fil du temps. Cependant, il est possible de faire des correspondances entre les couches des deux modèles, comme illustré par la Fig. 19.

4.2.2 Normes IEEE (802.x)

Les normes IEEE (Institute of Electrical and Electronics Engineers) sont des normes techniques qui définissent les spécifications et les protocoles utili-

sés dans les réseaux informatiques. Elles sont développées par l'IEEE, une organisation internationale à but non lucratif qui regroupe des professionnels de l'ingénierie électrique et électronique. Les normes IEEE sont notées 802.x dans le cadre des réseaux locaux et métropolitains (IEEE 802 LMSC pour « Local and Metropolitan Area Networks Standards Committee »). Elles couvrent un large éventail de technologies, y compris Ethernet (IEEE 802.3), Wi-Fi (IEEE 802.11), Bluetooth (IEEE 802.15) et d'autres technologies de communication sans fil.

On retrouve beaucoup ces normes dans les couches 1 et 2 du modèle OSI, ainsi que dans la couche d'accès réseau du modèle TCP/IP, comme illustré par la Fig. 20.

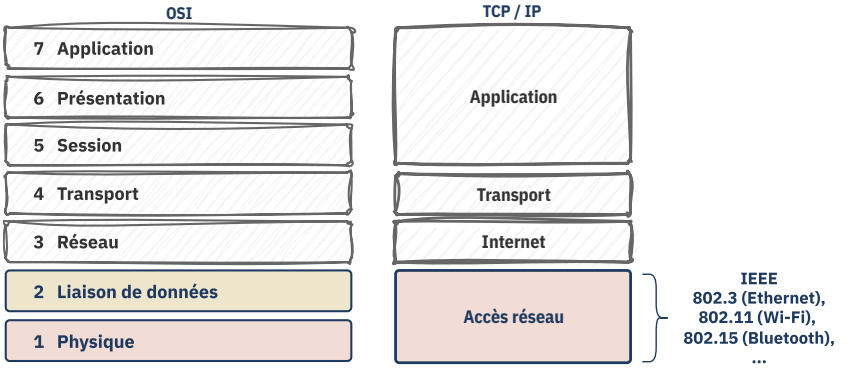


Fig. 20. – Illustration des normes IEEE 802.x et de leur correspondance avec les couches du modèle OSI et du modèle TCP/IP.

4.2.3 Normes IETF (RFC)

Les RFC (Request for Comments) sont des documents publiés par l'IETF (Internet Engineering Task Force) qui définissent les protocoles, les normes et les meilleures pratiques pour Internet. Chaque RFC est identifié par un numéro unique et peut être consulté librement sur le site de l'IETF[2]. Les RFC sont complémentaires aux normes IEEE et sont souvent utilisés pour définir les protocoles de communication utilisés dans les couches supérieures du modèle OSI et du modèle TCP/IP, comme HTTP, FTP, SMTP, DNS ou encore SSH, tel qu'illustré par la Fig. 21.

Voici une liste non exhaustive de quelques RFC importantes et leurs numéros correspondants :

[2] https://www.ietf.org/standards/rfcs/

- RFC 791 : Internet Protocol (IP), définit le protocole IP utilisé pour l'adressage logique et le routage des paquets de données sur Internet.
- RFC 8200 : Internet Protocol version 6 (IPv6), définit la version 6 du protocole IP, qui utilise des adresses sur 128 bits et permet d'adresser un nombre quasi infini d'hôtes.
- RFC 9293 : Transmission Control Protocol (TCP), définit le protocole TCP utilisé pour assurer une communication fiable, orientée connexion, avec contrôle de flux et retransmission des segments perdus.
- RFC 768 : User Datagram Protocol (UDP), définit le protocole UDP utilisé pour assurer une communication non fiable, sans connexion, avec un faible overhead et une faible latence.
- RFC 9110-9112 : Hypertext Transfer Protocol (HTTP), définit le protocole HTTP utilisé pour la communication entre les navigateurs web et les serveurs web.
- RFC 959 : File Transfer Protocol (FTP), définit le protocole FTP utilisé pour le transfert de fichiers entre les périphériques.
- RFC 5321 : Simple Mail Transfer Protocol (SMTP), définit le protocole SMTP utilisé pour l'envoi de courriers électroniques.

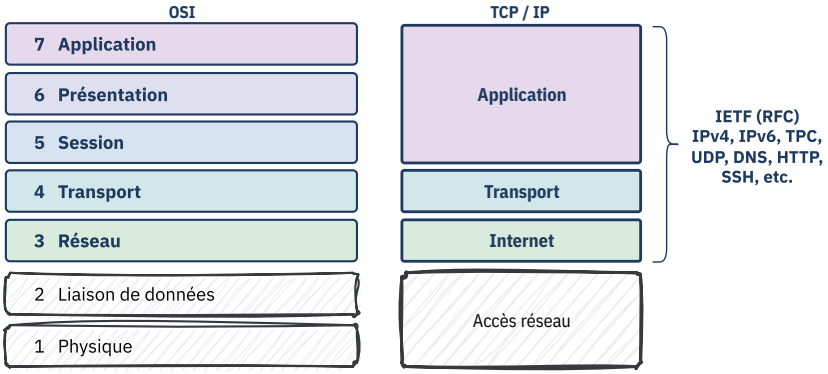


Fig. 21. – Illustration des RFC (Request for Comments) publiées par l'IETF (Internet Engineering Task Force) et de leur correspondance avec les couches du modèle OSI et du modèle TCP/IP.

REMARQUE

Naturellement, il n'est pas nécessaire de connaître les normes par coeur, et leur contenu est parfois assez indigeste. Mais savoir où aller chercher l'information est essentiel pour un ingénieur réseau. Pour

trouver une RFC, il suffit de taper « RFC » suivi du numéro de la RFC dans un moteur de recherche, ou de se rendre directement sur le site de l'IETF. Les normes 802.x de l'IEEE sont également disponibles sur le site de l'IEEE, mais elles sont souvent payantes ou difficiles d'accès.

APPROFONDISSEMENT · Autres organismes de normalisation

IEEE et IETF ne sont pas les seuls organismes de normalisation dans le domaine de l'informatique. On peut citer par exemple l'ISO (International Organization for Standardization), qui est responsable de la définition du modèle OSI, ou encore le W3C qui est responsable de la définition des standards du web, comme HTML, CSS et JavaScript. Dans le cadre du cours, nous nous concentrerons principalement sur les normes IEEE et IETF, car elles sont les plus pertinentes pour la compréhension des réseaux informatiques.

4.3 Encapsulation et décapsulation des données

L'encapsulation et la décapsulation des données sont des concepts fondamentaux dans les modèles en couches. Le principe est que chaque couche du modèle OSI ou TCP/IP ajoute des informations supplémentaires aux données qu'elle reçoit de la couche supérieure avant de les transmettre à la couche inférieure. Ces informations supplémentaires sont appelées en-têtes (ou « headers »).

Lorsqu'une donnée descend dans les couches du modèle, les en-têtes sont ajoutés au fur et à mesure que la donnée est transmise vers la couche inférieure. Ce processus est appelé **encapsulation**. À l'inverse, lorsqu'une donnée remonte dans les couches du modèle, les en-têtes sont retirés au fur et à mesure que la donnée est transmise vers la couche supérieure. Ce processus est appelé **décapsulation**.

La Fig. 22 illustre les entêtes ajoutés à chaque couche du modèle OSI lors de l'encapsulation des données. La couche liaison de données ajoute également une queue (ou « trailer ») à la fin de la trame, qui contient des informations supplémentaires pour la détection des erreurs de transmission. La couche physique ne modifie pas les données, mais se contente de les transmettre sur le support physique.

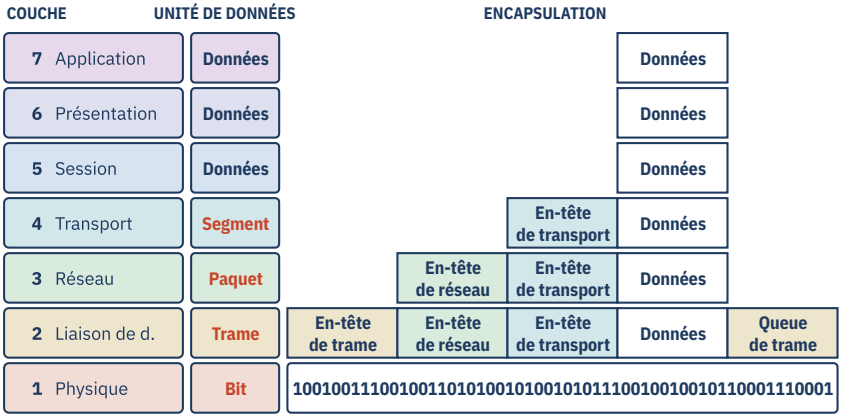


Fig. 22. – Illustration de l'encapsulation des données dans le modèle OSI. Chaque couche ajoute ses propres en-têtes et la couche liaison de données ajoute également une queue.

Prenons une analogie pour illustrer le principe d'encapsulation et de décapsulation des données. Imaginez que vous recevez une lettre par la poste. Cette lettre est transportée par le camion de livraison (L1), qui contient une enveloppe (L2). Sur cette enveloppe, il y a une adresse de destination (L3) et la mention « Urgent » (L4). À l'intérieur de l'enveloppe, il y a une lettre contenant l'objet de la communication (L5). Cette lettre commence par « Chère Madame / Cher Monsieur » (L6). Le contenu de la lettre vous indique que votre inscription à un cours en ligne a été acceptée, il s'agit de la « charge utile » (L7). La Fig. 23 illustre cette analogie.

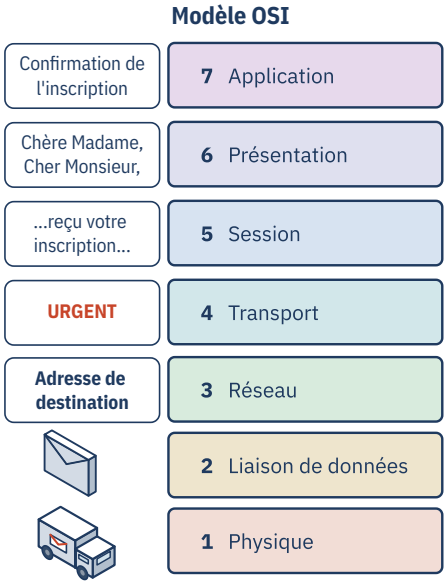


Fig. 23. – Illustration du principe d'encapsulation et de décapsulation des données à travers une analogie avec une lettre envoyée par la poste.

EXERCICE 4.2 · ORDRE D'ENCAPSULATION

Lors de l'envoi d'une requête HTTP, remettez ces PDU dans l'ordre dans lequel elles apparaissent en descendant les couches : trame, message, bits, segment, paquet.

CHAPITRE 5

Matériel

OBJECTIFS DU CHAPITRE

À l'issue de ce chapitre, vous saurez :

- identifier les principaux équipements réseau et leur rôle dans un réseau
- identifier les équipements réseaux associés aux différentes couches du modèle OSI, ainsi que leur symbole dans un schéma réseau
- décrire les différents médiums physiques
- décrire les différents types de câbles et leurs caractéristiques
- identifier le connecteur RJ45
- citer les médiums de transmission sans fil et leurs caractéristiques

Afin de faire fonctionner un réseau informatique, différents équipements sont nécessaires. Du switch au pare-feu, en passant par le routeur, chaque équipement a un rôle précis dans le fonctionnement du réseau. Ce chapitre décrit les principaux équipements réseau, ainsi que les différents médiums physiques et sans fil.

5.1 Équipements réseau

Un équipement réseau agit sur un certain nombre de couches du modèle OSI. La Fig. 24 illustre les principaux équipements réseau et les couches du modèle OSI sur lesquelles ils agissent.

ATTENTION

Bien qu'un équipement réseau n'agisse que sur un certain nombre de couches, certains peuvent être configurés à distance avec des protocoles comme SSH (p. ex. switch, routeur, pare-feu). Dans ce cas-là, ils utilisent les 7 couches du côté « management », mais uniquement les couches logiques associées côté **opérationnel**. Il s'agit bien du côté opérationnel qui est représenté sur la Fig. 24.

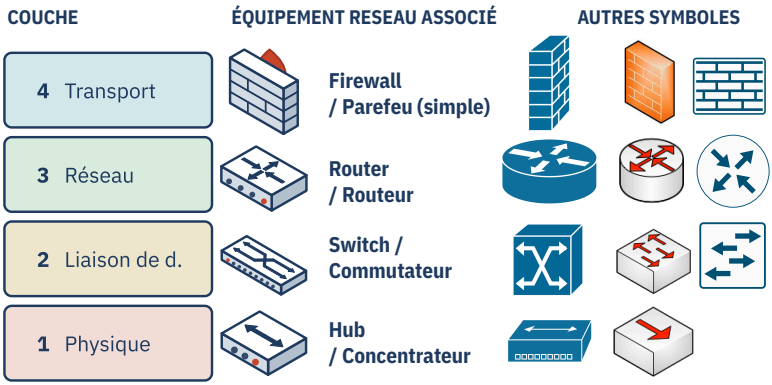


Fig. 24. – Principaux équipements réseau et couches du modèle OSI sur lesquelles ils agissent. Les symboles utilisés dans ce livre sont listés en annexe. La liste des symboles alternatifs est non-exhaustive et peut varier selon les auteurs et les logiciels de dessin.

5.1.1 Hub (Concentrateur)

Le hub (ou « concentrateur » en français) permet de relier plusieurs périphériques réseau entre eux. Il agit uniquement sur la couche physique du modèle OSI. Il ne fait pas de distinction entre les périphériques connectés : lorsqu'il reçoit un signal d'un périphérique, il le retransmet à tous les autres périphériques connectés. Il s'agit du type d'équipement le plus simple et le moins cher, mais il est rarement utilisé dans les réseaux modernes en raison de ses limitations :

- Il ne peut pas gérer le trafic réseau efficacement, ce qui peut entraîner des collisions de données et une baisse des performances.
- Un seul périphérique peut communiquer à la fois avec un autre périphérique, ce qui limite la bande passante disponible pour chaque périphérique.
- Il n'a aucune connaissance des couches supérieures du modèle OSI, ce qui signifie qu'il ne peut pas filtrer ou acheminer les données de manière intelligente. Résultat : tout le monde voit les transmissions de tout le monde.

Le symbole utilisé pour représenter un concentrateur est généralement un rectangle avec une flèche simple ou double à l'intérieur. La Fig. 25 illustre le symbole d'un concentrateur.

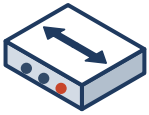


Fig. 25. – Symbole d'un concentrateur (hub).

5.1.2 Switch (Commutateur)

Le switch est la version intelligente du hub. Il agit sur les couches 1 et 2 du modèle OSI. Contrairement au hub, le switch a connaissance des adresses MAC des périphériques connectés (voir le chapitre *Ethernet et IP*) et peut commuter les données uniquement vers le périphérique de destination. Cela permet aux périphériques de communiquer simultanément sans interférer les uns avec les autres, ce qui améliore considérablement les performances du réseau. D'autre part, un périphérique ne reçoit que son propre trafic.

Pour pouvoir savoir à quel périphérique envoyer les données, le switch utilise une table d'adresses MAC, qui est construite dynamiquement en apprenant les adresses MAC des périphériques connectés.

APPROFONDISSEMENT · Switch de niveau 3

Certains switches peuvent également agir sur la couche 3 du modèle OSI, en utilisant des protocoles de routage pour acheminer les données entre différents réseaux. Ces switches sont appelés « switches de niveau 3 » ou « L3 switches ». Ils ne sont pas abordés dans ce cours.

REMARQUE

Un switch à deux ports est appelé un bridge (bien qu'historiquement ce soit l'inverse, un switch est un bridge à plus de 2 ports). À l'instar des hubs, ils ne sont pas beaucoup utilisés, du moins dans leur forme physique. Les bridges logiciels restent en revanche très utilisés dans la virtualisation, par exemple pour relier des machines virtuelles au réseau de l'hôte.

Le symbole du switch est généralement un rectangle avec deux flèches doubles qui s'entrecroisent (ou non) à l'intérieur. La Fig. 26 illustre le symbole d'un switch.

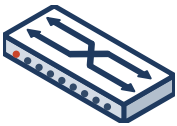


Fig. 26. – Symbole d'un commutateur (switch).

5.1.3 Routeur

Le routeur agit sur les couches 1, 2 et 3 du modèle OSI. Il s'occupe de faire « l'aiguillage » des paquets et de les acheminer vers le réseau de destination. Il utilise une table de routage pour déterminer le meilleur chemin pour chaque paquet. Un routeur est souvent appelé « gateway » (passerelle).

Le symbole du routeur est généralement un cercle (ou un rectangle) avec deux flèches qui pointent à l'intérieur, et deux flèches qui pointent à l'extérieur. La Fig. 27 illustre le symbole d'un routeur.

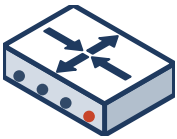


Fig. 27. – Symbole d'un routeur.

> **ATTENTION**
> Une confusion courante est de confondre une « Application Gateway » et un routeur. Une Application Gateway est un type de pare-feu qui agit sur les couches 5 à 7 du modèle OSI, tandis qu'un routeur agit sur les couches 1 à 3. Les deux équipements ont des fonctions différentes et ne doivent pas être confondus.

5.1.4 Pare-feu (Firewall)

Le pare-feu, dans sa version la plus simple, agit sur les couches 1 à 4 du modèle OSI. Il filtre le trafic réseau en fonction de règles prédéfinies, permettant ou bloquant le passage des paquets en fonction de leur adresse IP ou du port utilisé (UDP / TCP). Un pare-feu peut être matériel ou logiciel, et il est souvent utilisé pour protéger les réseaux contre les intrusions et les attaques. Bien souvent, un pare-feu monte jusqu'à la couche 7 du modèle OSI, et ne se limite pas à la couche 4. Il peut alors filtrer le trafic en fonction de l'application utilisée (HTTP, FTP, etc.) ou du contenu des paquets. Pour ce chapitre, la version la plus simple du pare-feu est abordée, c'est-à-dire celle qui agit sur les couches 1 à 4 du modèle OSI.

Le symbole du pare-feu est généralement un mur de brique avec (ou non) une flamme. La Fig. 28 illustre le symbole d'un pare-feu.

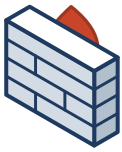


Fig. 28. – Symbole d'un pare-feu (firewall).

5.1.5 Résumé

Chaque équipement réseau agit sur un certain nombre de couches du modèle OSI. Le hub est peu utilisé, contrairement au switch et au routeur. Le pare-feu est un équipement de sécurité qui filtre le trafic réseau en fonction de règles prédéfinies. La Fig. 29 illustre les principaux équipements réseau et les couches du modèle OSI sur lesquelles ils agissent, avec un exemple simple de transmission de données entre un PC et un serveur.

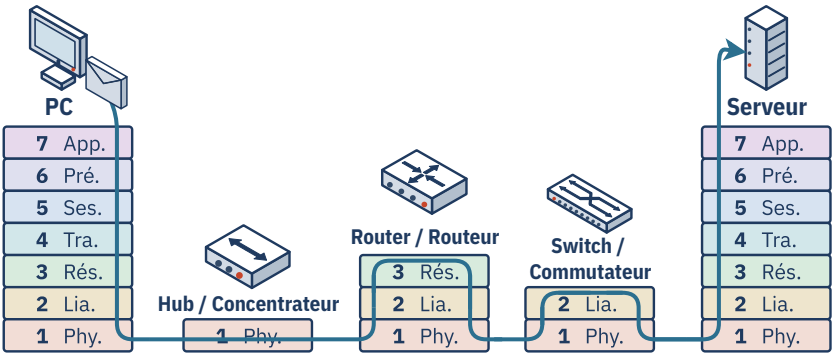


Fig. 29. – Exemple de transmission de données entre un PC et un serveur, avec les principaux équipements réseau et les couches du modèle OSI sur lesquelles ils agissent.

EXERCICE 5.1 · CHOISIR LE BON ÉQUIPEMENT

Pour chaque besoin ci-dessous, indiquez l'équipement approprié : hub, switch, routeur ou pare-feu.

A. Relier les 8 PC d'un bureau au sein d'un même réseau local.

B. Interconnecter le réseau local de l'entreprise avec Internet.

C. Bloquer le trafic entrant sur certains ports.

D. Relier quelques périphériques à moindre coût, en acceptant que chacun voie le trafic de tous les autres.

EXERCICE 5.2 · ÉQUIPEMENTS ET COUCHES OSI

Pour chaque équipement, citez les couches du modèle OSI sur lesquelles il agit (côté opérationnel) : hub, switch, routeur, pare-feu simple.

5.2 Médiums physiques et sans fil

Les médiums physiques sont les supports de transmission des signaux électriques ou optiques dans un réseau. Ils peuvent être classés en deux grandes catégories : les câbles et les médiums sans fil. Chaque support a ses propres caractéristiques, avantages et inconvénients, qui influencent la performance et la fiabilité du réseau. Les principaux médiums physiques sont le cuivre, la fibre optique et les médiums sans fil.

Choisir le bon médium en fonction des besoins et des contraintes fait partie du travail d'un ingénieur réseau.

5.2.1 Cuivre

Les supports de transmission en cuivre sont les plus couramment utilisés dans les réseaux locaux (LAN). Il en existe deux types principaux : les paires torsadées et les câbles coaxiaux. Le cuivre est un bon conducteur électrique, ce qui permet une transmission efficace des signaux électriques.

L'avantage du cuivre est qu'il est économique et facile à installer. Cependant, il est sensible aux interférences électromagnétiques (EMI) et à l'atténuation du signal sur de longues distances. Le cuivre est donc plus adapté aux réseaux locaux (LAN) qu'aux réseaux étendus (WAN).

5.2.1.1 Paires torsadées

Les paires torsadées sont les câbles les plus utilisés dans les réseaux locaux. On les nomme souvent « câble Ethernet » par abus de langage, car ce sont eux qui sont utilisés pour les réseaux Ethernet. Ils sont composés de 4 paires de fils de cuivre torsadés entre eux, ce qui permet de réduire les interférences électromagnétiques. Généralement, la connectique se fait avec des connecteurs RJ45, comme illustré sur la Fig. 30. Les câbles à

paires torsadées peuvent être blindés (STP) ou non blindés (UTP). Le blindage permet de réduire les interférences électromagnétiques, mais il est plus coûteux et moins flexible que les câbles non blindés.

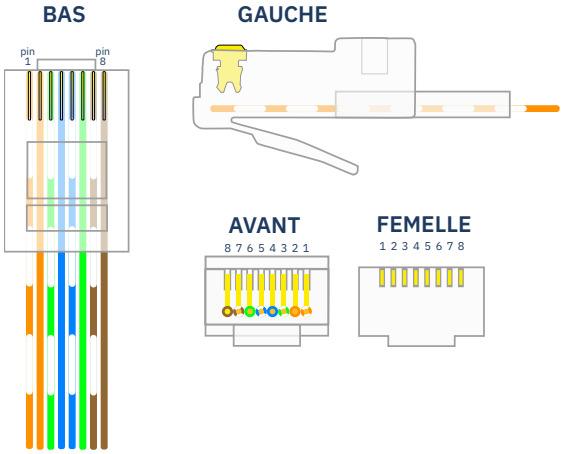


Fig. 30. – Connecteur RJ45 pour câble à paires torsadées.

Il existe différents types de câbles à paires torsadées, classés en fonction de leur catégorie (Cat 5e, Cat 6, Cat 6a, Cat 7, etc.). Chaque catégorie a ses propres caractéristiques de performance, notamment la bande passante et la vitesse de transmission maximale. Le Tableau 11 résume les principales caractéristiques des différentes catégories de câbles à paires torsadées.

Catégorie	Fréquence caractérisée	Débit max (100 m)	Normes Ethernet associées
Cat 5	100 MHz	1 Gbit/s[3]	100BASE-TX, 1000BASE-T
Cat 5e	100 MHz	2.5 Gbit/s	1000BASE-T, 2.5GBASE-T
Cat 6	250 MHz	5 Gbit/s[4]	5GBASE-T
Cat 6a	500 MHz	10 Gbit/s	10GBASE-T
Cat 7	600 MHz	10 Gbit/s	aucune[5]

[3]1000BASE-T a été conçu pour fonctionner sur le parc de câbles Cat 5 existant. En pratique, on installe aujourd'hui du Cat 5e au minimum.

[4]10GBASE-T possible sur Cat 6, mais limité à environ 55 m.

Tableau 11. – Caractéristiques des différentes catégories de câbles à paires torsadées.

APPROFONDISSEMENT · Normes Ethernet associées aux câbles à paires torsadées

La norme Ethernet 802.3 définit les spécifications en termes de débit et de distance pour chaque catégorie de câble. La nomenclature est la suivante:

`xBASE-y`, où `x` est le débit en Mbit/s ou Gbit/s, et `y` est le type de médium utilisé (T pour paires torsadées, S ou L pour fibre optique, etc.). Par exemple, 1000BASE-T correspond à un débit de 1000 Mbit/s (1 Gbit/s) sur un câble à paires torsadées. Les normes Ethernet associées aux câbles à paires torsadées sont listées dans le Tableau 11. Certaines catégories supportent plusieurs normes, cela dépend également du codage utilisé pour la transmission des données.

`BASE` signifie que le signal est transmis en bande de base, c'est-à-dire sans modulation sur une fréquence porteuse. Historiquement on retrouvait aussi le terme `broadband` pour les transmissions modulées sur une fréquence porteuse, mais ce n'est plus utilisé dans les réseaux locaux modernes.

De plus, les anciennes normes comme 10BASE2 et 10BASE5 avaient un digit de fin indiquant la distance maximale en centaines de mètres (2 pour ~200 m, 5 pour ~500 m). Ces normes sont obsolètes et ne sont plus utilisées dans les réseaux locaux modernes.

Deux types de câbles à paires torsadées existent : les câbles droits et les câbles croisés. Entre l'émetteur et le récepteur, les paires doivent être croisées. Il existe deux façons de câbler une interface : MDI (PC, serveurs, routeurs) et MDIX (switches, hubs), qui est câblée de manière inversée. En découle la règle suivante : entre deux équipements câblés de la même manière (deux PC, deux switches, mais aussi un PC et un routeur), on utilise un câble croisé, tandis qu'entre un équipement MDI et un équipement MDIX (par exemple, un ordinateur et un switch), on utilise un câble droit.

[5]Catégorie ISO (classe F) sans norme IEEE dédiée ; supporte 10GBASE-T comme le Cat 6a.

ATTENTION
On entend souvent la règle simplifiée « équipements de même type = câble croisé ». Elle est trompeuse : un PC et un routeur sont des équipements de types différents, mais leurs interfaces sont toutes deux câblées en MDI. Il faut donc un câble croisé entre eux.

La Fig. 31 illustre la différence entre un câble droit et un câble croisé.

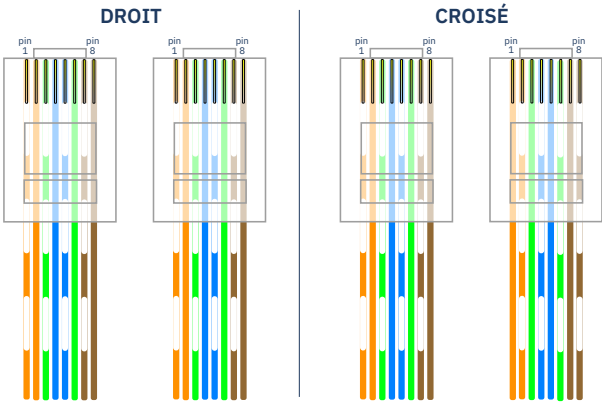


Fig. 31. – Différence entre un câble droit et un câble croisé. Les paires sont croisées entre elles.

Aujourd'hui, l'auto-MDI/MDIX permet de détecter automatiquement le type de câble utilisé et d'adapter la configuration des ports en conséquence. Cependant, il est toujours important de connaître la différence entre un câble droit et un câble croisé, car certains équipements plus anciens ne supportent pas l'auto-MDI/MDIX.

5.2.1.2 Câbles coaxiaux

Les câbles coaxiaux sont composés d'un conducteur central en cuivre, entouré d'un isolant, d'une tresse métallique et d'une gaine extérieure. Ils sont moins utilisés dans les réseaux locaux modernes, mais ils étaient couramment utilisés pour la télévision par câble et les réseaux Ethernet 10BASE2 et 10BASE5. La Fig. 32 illustre un câble coaxial.

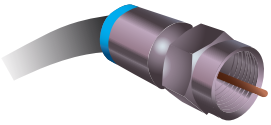


Fig. 32. – Câble coaxial.

5.2.2 Fibre optique

La fibre optique est un médium de transmission qui utilise la lumière pour transmettre les données. Elle est composée d'un coeur en verre ou en plastique, entouré d'une gaine qui réfléchit la lumière et d'une gaine extérieure protectrice. La fibre optique offre des débits très élevés et une grande distance de transmission avec une perte de signal très faible, ce qui la rend idéale pour les réseaux longue distance et les réseaux à haut débit. Elle est également insensible aux interférences électromagnétiques. En revanche, son coût est plus élevé que celui des câbles en cuivre, sa manipulation est plus délicate et elle nécessite des équipements spécifiques pour sa maintenance. La Fig. 33 illustre un câble à fibre optique.

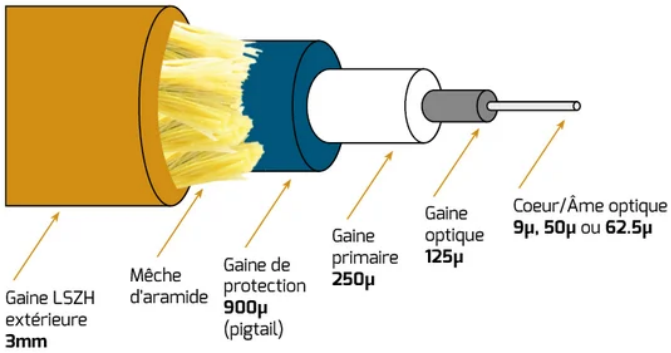


Fig. 33. – Composition d'une fibre optique.[6]

Le débit sur fibre optique peut atteindre plusieurs dizaines de Gbit/s (10, 40, 100 Gbit/s et plus), avec des distances de transmission allant jusqu'à plusieurs dizaines de kilomètres sans répéteur. La fibre optique est donc particulièrement adaptée aux réseaux longue distance et aux réseaux à haut débit. C'est en quelque sorte « l'autoroute de l'information » par rapport aux câbles en cuivre, qui sont plutôt des routes locales.

[6]Source de l'image: https://blog.uniformatic.fr/cable-optique

APPROFONDISSEMENT

Il existe deux types de fibre optique : la fibre monomode et la fibre multimode. La fibre monomode permet une transmission sur de longues distances avec un seul mode de propagation de la lumière, tandis que la fibre multimode permet une transmission sur de courtes distances avec plusieurs modes de propagation. La fibre monomode est généralement utilisée pour les réseaux longue distance, tandis que la fibre multimode est utilisée pour les réseaux locaux et les centres de données. Cette différence n'est pas abordée dans ce cours.

5.2.3 Médiums sans fil

Les médiums sans fil englobent des technologies comme le Wi-Fi, le Bluetooth, la 4G/5G ou encore le LoRa. Toutes ces technologies utilisent des ondes électromagnétiques pour transmettre les données, sur des fréquences radio spécifiques. Les avantages des médiums sans fil sont la mobilité et la facilité d'installation, tandis que les inconvénients incluent la sensibilité aux interférences, aux obstacles physiques ou à la distance, mais aussi la sécurité. En effet, tout périphérique à portée peut potentiellement intercepter les communications, ce qui nécessite des protocoles de sécurité adaptés (WPA2/WPA3 pour le Wi-Fi, chiffrement pour le Bluetooth, etc.).

5.2.3.1 Wi-Fi

Le Wi-Fi est une technologie de réseau local sans fil qui permet aux périphériques de se connecter à un réseau et à Internet sans utiliser de câbles. Il utilise des ondes radio pour transmettre les données entre les périphériques et un point d'accès (AP). Le Wi-Fi est largement utilisé dans les environnements domestiques, les entreprises et les lieux publics. Il existe différentes normes Wi-Fi (802.11a/b/g/n/ac/ax), chacune offrant des débits et des portées différents.

5.2.3.2 Bluetooth

Le Bluetooth est une technologie de communication sans fil à courte portée, utilisée pour connecter des périphériques comme des casques audio, des claviers, des souris ou des smartphones. Il fonctionne sur la bande de fréquence 2,4 GHz et permet des échanges de données à des débits modérés sur des distances généralement inférieures à 100 mètres.

5.2.3.3 4G/5G

La 4G (LTE) et la 5G sont des technologies de communication sans fil à large couverture, utilisées pour connecter des périphériques mobiles à Internet. La 4G offre des débits allant jusqu'à plusieurs centaines de Mbit/s, tandis que la 5G peut atteindre plusieurs Gbit/s et offre une latence très faible. Ces technologies utilisent des bandes de fréquences spécifiques et nécessitent des infrastructures réseau étendues (antennes relais).

5.2.3.4 LoRa

Le LoRa (Long Range) est une technologie de communication sans fil à longue portée et à faible consommation d'énergie, utilisée principalement pour les applications IoT (Internet of Things). Elle permet de connecter des capteurs et des dispositifs sur de grandes distances (jusqu'à plusieurs kilomètres) avec un débit relativement faible. Le LoRa fonctionne sur des bandes de fréquences spécifiques et est particulièrement adapté aux environnements ruraux ou aux applications nécessitant une longue autonomie des dispositifs.

5.2.3.5 Li-Fi

Le Li-Fi est une technologie de communication sans fil qui utilise la lumière visible pour transmettre des données. Elle offre des débits élevés et une faible latence, mais sa portée est limitée et elle nécessite une ligne de vue directe entre l'émetteur et le récepteur. Le Li-Fi est encore en développement et n'est pas largement utilisé dans les réseaux commerciaux.

5.2.4 Exemples d'applications

Un ingénieur réseau doit être capable de choisir le bon médium en fonction des besoins et des contraintes. Ci-dessous, quelques exemples d'applications et de médiums adaptés :

- Réseau local d'entreprise : câbles à paires torsadées
- Réseau longue distance entre deux sites : fibre optique
- Réseau domestique : câbles à paires torsadées ou Wi-Fi

EXERCICE 5.3 · CHOISIR LE BON MÉDIUM

Pour chaque situation, proposez le médium le plus adapté (paires torsadées, fibre optique, Wi-Fi, 4G/5G, LoRa) et justifiez brièvement.

A. Relier deux bâtiments d'un campus distants de 2 km.

B. Connecter le poste de travail fixe d'un développeur.

C. Des capteurs de température répartis dans des champs, envoyant une mesure par heure.

D. L’accès à Internet d’un smartphone en déplacement.

CHAPITRE 6

Accès au médium

OBJECTIFS DU CHAPITRE

À l'issue de ce chapitre, vous saurez :

- décrire les domaines de diffusion et de collision dans un réseau
- décrire les types de transmission (half-duplex, full-duplex) et leurs implications sur l'accès au médium
- expliquer le rôle des commutateurs et des routeurs dans la segmentation des domaines de diffusion et de collision
- expliquer le principe de base du Token Ring et son fonctionnement pour gérer l'accès au médium partagé
- expliquer le protocole CSMA/CD et son rôle dans la gestion de l'accès au médium partagé

Ce chapitre traite de la problématique de l'accès à un médium partagé dans un réseau. Il aborde les concepts de domaines de diffusion et de collision, ainsi que les protocoles et techniques utilisés pour gérer l'accès au médium et ainsi éviter les collisions. L'accès au médium est un aspect de la couche 2 (liaison de données) du modèle OSI.

6.1 Domaines de diffusion et de collision

Avant de traiter les techniques qui permettent d'éviter les collisions sur un médium partagé, il est important de comprendre les concepts de domaines de diffusion et de collision.

Un domaine de diffusion est un segment de réseau dans lequel une trame de diffusion (broadcast) est reçue par tous les périphériques.

Un domaine de collision est un segment de réseau dans lequel les trames de données peuvent entrer en collision lorsqu'ils sont envoyés simultanément par plusieurs périphériques. Dans un domaine de collision, une méthode d'accès au médium (Chapitre 6.3) est nécessaire pour éviter les collisions et garantir que les périphériques puissent communiquer efficacement. La

Fig. 34 illustre une collision sur un médium partagé, au sein d'un domaine de collision.

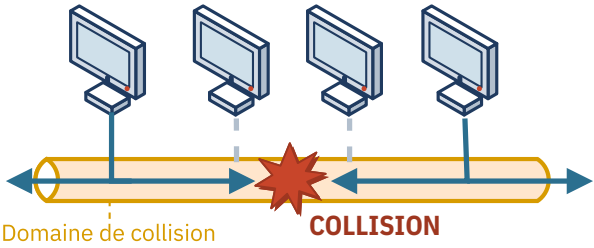


Fig. 34. – Illustration d'une collision sur un médium partagé, au sein d'un domaine de collision. Dans cet exemple, deux périphériques tentent d'envoyer des données en même temps, ce qui entraîne une collision et la perte des trames.

Les domaines de diffusion et de collision sont définis par la topologie du réseau et les équipements utilisés. Les switches séparent les domaines de collision : un domaine de collision par port du switch. Les routeurs séparent les domaines de diffusion : un domaine de diffusion par interface du routeur. Un hub quant à lui ne sépare aucun des domaines. La Fig. 35 illustre les domaines de diffusion et de collision dans un réseau simple.

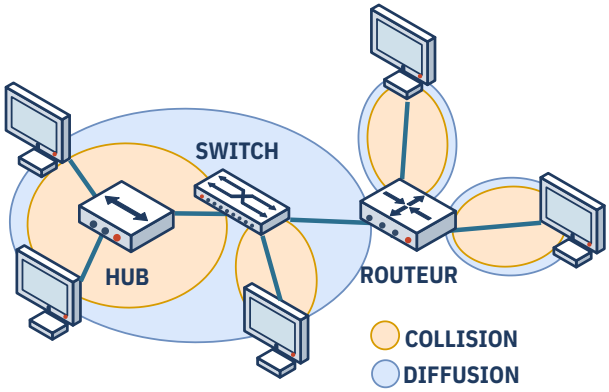


Fig. 35. – Illustration des domaines de diffusion et de collision dans un réseau.

EXERCICE 6.1 · COMPTER LES DOMAINES DE COLLISION ET DE DIFFUSION

Un réseau est construit comme illustré sur la Fig. 36.

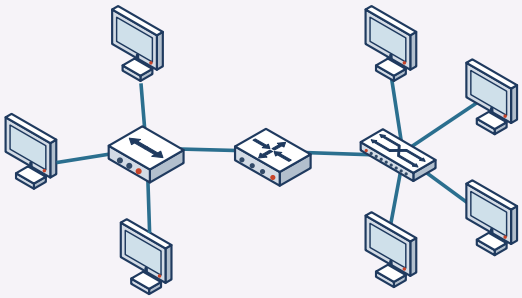


Fig. 36. – Réseau pour l'exercice sur les domaines de diffusion et de collision.

Combien ce réseau compte-t-il de domaines de collision et de domaines de diffusion ?

EXERCICE 6.2 · VRAI OU FAUX : HUB, SWITCH ET ROUTEUR

Pour chaque affirmation, indiquez si elle est vraie ou fausse. Justifiez.

A. Un switch sépare les domaines de diffusion.

B. Un hub sépare les domaines de collision.

C. Chaque interface d'un routeur constitue un domaine de diffusion distinct.

D. Tous les périphériques connectés à un hub appartiennent au même domaine de collision.

6.2 Types de transmission

Dans un réseau, on distingue trois types de transmission : simplex, half-duplex et full-duplex. La Fig. 37 illustre la transmission simplex. Dans ce cas-ci, un seul périphérique peut émettre des données, tandis que l'autre périphérique ne peut que recevoir. Un exemple typique de transmission

simplex est la communication unidirectionnelle, comme la diffusion radio ou la télévision.



Fig. 37. – Transmission simplex : un périphérique émet, l'autre reçoit.

La transmission half-duplex permet aux périphériques d'émettre et de recevoir des données, mais pas simultanément. La Fig. 38 illustre la transmission half-duplex. Un exemple typique de transmission half-duplex est la communication par talkie-walkie.



Fig. 38. – Transmission half-duplex : les périphériques peuvent émettre et recevoir, mais pas simultanément.

La transmission full-duplex permet aux périphériques d'émettre et de recevoir des données simultanément. La Fig. 39 illustre la transmission full-duplex. Un exemple typique de transmission full-duplex est la communication téléphonique moderne, où les deux parties peuvent parler et écouter en même temps. C'est le type de transmission qui est utilisé dans les réseaux Ethernet modernes.



Fig. 39. – Transmission full-duplex : les périphériques peuvent émettre et recevoir simultanément.

Le type de transmission a une conséquence directe sur l'accès au médium : en half-duplex, les deux sens partagent le même canal, des collisions sont possibles et une méthode d'accès au médium (Chapitre 6.3) est indispensable. En full-duplex, chaque sens de transmission dispose de son propre canal (par exemple des paires de cuivre distinctes pour l'émission et la

réception en Ethernet) : il n'y a plus de médium partagé, donc plus de collisions possibles. C'est pourquoi l'Ethernet commuté moderne, full-duplex, n'a plus besoin de CSMA/CD, alors que le Wi-Fi, dont le canal radio reste half-duplex et partagé, utilise toujours CSMA/CA.

ATTENTION
Il existe parfois la nécessité d'utiliser des méthodes d'accès au médium partagé en full-duplex. Cela est typiquement nécessaire pour des réseaux point-à-multipoint (fibre optique partagée par exemple). On peut résumer la nécessité à la phrase suivante : « si le médium possède plusieurs émetteurs potentiels, il est partagé et nécessite une méthode d'accès au médium ».

EXERCICE 6.3 · DUPLEX ET MÉTHODES D'ACCÈS

Expliquez pourquoi l'Ethernet commuté moderne n'a plus besoin de CSMA/CD, alors que le Wi-Fi utilise toujours une méthode d'accès au médium (CSMA/CA).

6.3 Méthodes d'accès au médium

Pour pouvoir gérer l'accès au médium partagé dans les domaines de collision, il existe plusieurs types de méthodes d'accès au médium : par multiplexage, par compétition et par consultation. Ces méthodes permettent de réguler l'accès au médium et d'éviter les collisions entre les périphériques.

6.3.1 Par consultation

Avec les méthodes par consultation, les périphériques se mettent d'accord sur qui utilise le médium à un moment donné. Un exemple de méthode par consultation est le Token Ring, où un jeton circule dans le réseau et permet au périphérique qui le possède d'émettre des données. La Fig. 40 illustre le principe du Token Ring.

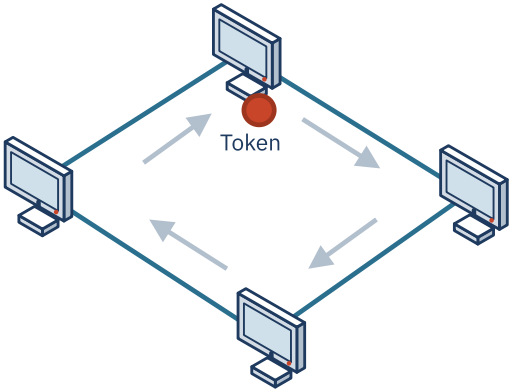


Fig. 40. – Illustration du principe du Token Ring : un jeton circule dans le réseau et permet au périphérique qui le possède d'émettre des données.

Les méthodes par consultation ont l'avantage d'éviter les collisions et d'être déterministes (le temps d'attente maximum pour émettre est connu). Il y a également une équité dans l'accès au médium, car chaque périphérique a la possibilité d'émettre à tour de rôle. Lors de charges très élevées, les méthodes par consultation permettent de garder une performance stable. En revanche, de telles méthodes créent un surcoût en termes de complexité et de latence, car il faut gérer le jeton et la circulation dans le réseau. De plus, si un périphérique tombe en panne ou ne libère pas le jeton, cela peut bloquer l'accès au médium pour tous les autres périphériques.

6.3.2 Par compétition

Les méthodes par compétition permettent aux périphériques de tenter d'accéder au médium en même temps, ce qui peut entraîner des collisions. Le protocole CSMA/CD (Carrier Sense Multiple Access with Collision Detection) est un exemple de méthode par compétition. Il existe également d'autres algorithmes comme « ALOHA » ou CSMA/CA (« équivalent » CSMA/CD pour le Wi-Fi, avec un fonctionnement légèrement différent) qui ne sont pas abordés dans le cours. CSMA/CD était historiquement utilisé pour Ethernet, et fonctionne en détectant si le médium est libre avant d'émettre et en détectant les collisions lorsqu'elles se produisent. La Fig. 41 illustre le principe du CSMA/CD.

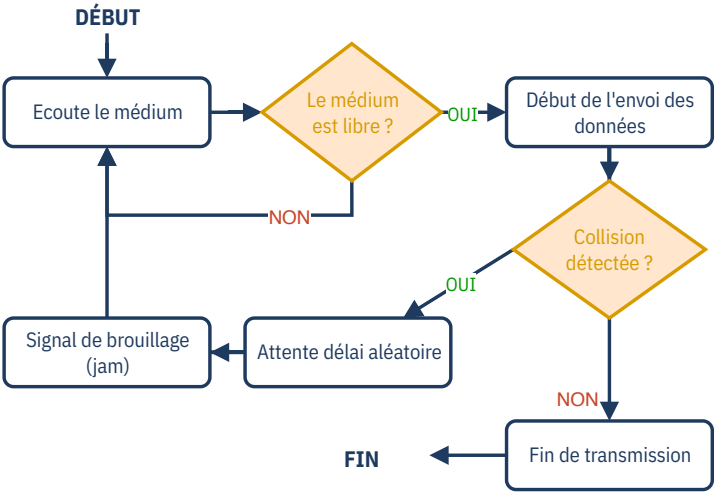


Fig. 41. – Illustration du principe du CSMA/CD : les périphériques écoutent le médium avant d'émettre et détectent les collisions lorsqu'elles se produisent.

Lorsqu'une collision est détectée, les périphériques impliqués attendent un temps aléatoire avant de réessayer d'émettre, ce qui réduit la probabilité de collisions répétées. L'attente aléatoire est gérée par un algorithme appelé « Binary Exponential Backoff », qui augmente le temps d'attente après chaque collision successive.

Les méthodes d'accès par compétition sont simples à mettre en oeuvre, aucun système de gestion centralisé n'est nécessaire. La latence pour émettre est quasi-nulle lorsque le médium est libre. En revanche, ces méthodes sont non déterministes : le temps d'attente pour émettre peut varier considérablement en fonction de la charge du réseau et du nombre de collisions. De plus, elles peuvent entraîner une baisse de performance lors de charges élevées, car les collisions deviennent plus fréquentes et le temps d'attente augmente.

EXERCICE 6.4 · DÉROULER CSMA/CD PAS À PAS

Trois stations A, B et C partagent un médium géré par CSMA/CD. A est en train d'émettre. B et C veulent chacune envoyer une trame. Décrivez, étape par étape, ce qui se passe entre le moment où B et C veulent émettre et le moment où leurs trames sont transmises avec succès.

6.3.3 Par multiplexage

Les méthodes par multiplexage permettent de diviser le médium en plusieurs canaux, chacun pouvant être utilisé par un périphérique différent. Il existe deux types principaux de multiplexage : le multiplexage temporel (TDMA) et le multiplexage fréquentiel (FDMA). La Fig. 42 illustre la différence entre TDMA et FDMA.

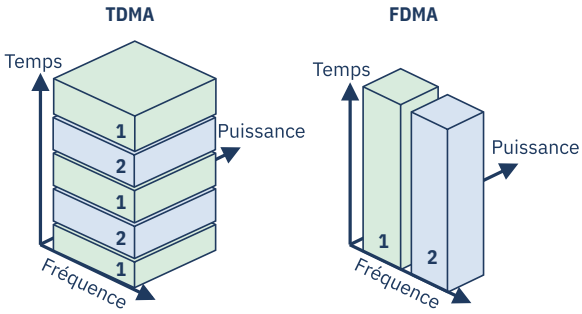


Fig. 42. – Illustration de la différence entre le multiplexage temporel (TDMA) et le multiplexage fréquentiel (FDMA) : dans TDMA, chaque périphérique utilise le médium à tour de rôle dans des intervalles de temps distincts, tandis que dans FDMA, chaque périphérique utilise une bande de fréquence distincte pour transmettre ses données.

Les méthodes par multiplexage ont l'avantage d'éviter les collisions, d'avoir un débit et une latence déterministes, et de permettre une utilisation efficace du médium. Cependant, elles nécessitent une coordination et une planification plus complexes. Si un canal est défini mais jamais utilisé, il est perdu. C'est un type de méthode d'accès au médium qui n'est pas adapté aux communications sporadiques.

6.3.4 Comparaison des méthodes d'accès au médium

Le Tableau 12 compare les différentes méthodes d'accès au médium en termes de complexité, de latence, de débit et de tolérance aux collisions.

Méthode d'accès	Complexité	Latence	Débit	Tolérance aux collisions
Consultation	Élevée	Modérée, bornée (déterministe)	Stable, même en forte charge	Aucune collision
Compétition	Faible	Quasi-nulle à faible charge, imprévisible en forte charge	Se dégrade en forte charge (non déterministe)	Collisions possibles, gérées par backoff
Multiplexage	Moyenne à élevée	Faible, bornée (déterministe)	Garanti par canal, mais capacité perdue si un canal est inutilisé	Aucune collision

Tableau 12. – Comparaison des différentes méthodes d'accès au médium en termes de complexité, de latence, de débit et de tolérance aux collisions.

ANNEXE

Corrigés des exercices

Solutions de tous les exercices, classées par chapitre.

Chapitre 1 · Introduction à la téléinformatique

Exercice 1.1 · Chronologie de la téléinformatique

1. Télégraphe électrique (1837)
2. ARPANET (1969)
3. Adoption de TCP/IP (1983)
4. Le Web (1991)
5. iPhone (2007)

Exercice 1.2 · Nommer des périphériques

- Terminaux:
  - Ordinateur
  - Smartphone
  - Console de jeu
  - Smartwatch
  - Tablette
  - Caméra IP
  - Imprimante réseau
  - Capteur IoT
- Intermédiaires:
  - Routeur
  - Switch
  - Pare-feu (Firewall)
  - Point d'accès Wi-Fi
- Et bien d'autres !

Exercice 1.3 · Identifier les éléments d'un réseau

- Périphériques terminaux : la tablette d'Alice, le serveur de streaming
- Périphériques intermédiaires : le routeur de la maison (et tous les équipements de l'opérateur et d'Internet entre les deux)

- Médiums : les ondes radio (Wi-Fi) entre la tablette et le routeur, la fibre optique vers Internet
- Message : le flux vidéo

Exercice 1.4 · Fiabilité, débit et latence selon l'application

1. Pour un email, la **fiabilité** est primordiale : il est essentiel que le message arrive intact et complet.
2. Pour le streaming vidéo, le **débit** est crucial : une bande passante suffisante est nécessaire pour assurer une lecture fluide sans interruptions. La latence est également importante, mais moins critique que le débit pour ce type d'application, sauf si l'on parle de streaming en direct, où la latence peut affecter l'expérience utilisateur.
3. Pour les jeux en ligne, la **latence** est l'aspect le plus important : une faible latence (communément appelée « ping » dans le jargon des joueurs) est essentielle pour une expérience de jeu réactive et compétitive. Un débit suffisant est également nécessaire, mais la latence est souvent le facteur déterminant pour la jouabilité.

Chapitre 2 · Signaux, topologies et classifications des réseaux

Exercice 2.1 · Identifier les éléments d'une chaîne de transmission

- Émetteur : Alice
- Canal : Le facteur et le transport de la lettre
- Récepteur : Bob
- Sources potentielles de bruit : Conditions météorologiques défavorables (pluie, vent), mauvaise écriture d'Alice, etc.

Exercice 2.2 · Analogique ou numérique ?

- A. Analogique, la voix humaine est un signal continu qui peut prendre une infinité de valeurs.
- B. Numérique, un fichier MP3 est un signal discret qui ne peut prendre qu'un nombre limité de valeurs. Dès le moment où il tient sur un ordinateur, il est numérique.
- C. Analogique, un disque vinyle est un support analogique qui reproduit un signal continu.
- D. Numérique, un SMS est un signal discret qui ne peut prendre qu'un nombre limité de valeurs.

- E. Analogique, la température affichée par un thermomètre à mercure est un signal continu qui peut prendre une infinité de valeurs.

Exercice 2.3 · Identifier le mode de transmission

- A. Unicast
- B. Multicast (seuls les abonnés qui regardent le flux reçoivent le signal)
- C. Broadcast
- D. Unicast

Exercice 2.4 · Nombre de liens d'un maillage complet

A. Chaque périphérique est relié aux 5 autres :

$$\frac{6 \times 5}{2} = 15 \text{ liens}$$

(on divise par 2 car chaque lien relie deux périphériques).

B.

$$\frac{n(n-1)}{2}$$

C. Le coût : le nombre de liens croît quadratiquement avec le nombre de périphériques, ce qui rend le maillage complet très coûteux à grande échelle. Par exemple, pour 100 périphériques, il faudrait déjà $\frac{100 \times 99}{2} = 4950$ liens.

Exercice 2.5 · Identifier la classe de réseau

A. LAN (Local Area Network) - Réseau domestique

B. MAN (Metropolitan Area Network) - Réseau d'entreprise dans une ville

C. PAN (Personal Area Network) - Connexion Bluetooth entre la manette et la console

D. GAN (Global Area Network) - Les satellites Galileo permettent la communication à l'échelle mondiale

Chapitre 3 · Binaire, hexadécimal et opérations logiques

Exercice 3.1 · Conversions

A. Comme 1 « B » = 8 « b » :

$$10 \text{ MB} = 10 \times 8 \text{ Mb} = 80 \text{ Mb}$$

B. Comme 1000 « kB » = 1 « MB » et 1000 « MB » = 1 « GB » :

$$1000 \text{ kB} = 1 \text{ MB} = \frac{1}{1000} \text{ GB} = 0.001 \text{ GB}$$

C. Comme 1 « o » = 8 « b » :

$$250 \text{ o} = 250 \times 8 \text{ b} = 2000 \text{ b}$$

D. Comme 1 « Gb » = 1/8 « GB » :

$$1 \text{ Gb} = \frac{1}{8} \text{ GB} = 0.125 \text{ GB}$$

E. Ici on passe d'une unité en base 10 (ko) à une unité en base 2 (KiB). Comme 1 « ko » = 1000 « o » et 1 « KiB » = 1024 « o » :

$$500 \text{ ko} = 500 \times 1000 \text{ o} = 500000 \text{ o}$$

$$500000 \text{ o} = \frac{500000}{1024} \text{ KiB} \approx 488.28 \text{ KiB}$$

Exercice 3.2 · Calcul du temps de téléchargement: modem 56k

Tout d'abord, convertissons 5 Mo en bits. Comme 1 Mo = 8 Mb (mégaoctets en mégabits) :

$$5 \text{ Mo} = 5 \times 8 \text{ Mb} = 40 \text{ Mb}$$

Ensuite, convertissons les mégabits en kilobits :

$$40 \text{ Mb} = 40 \times 1000 \text{ kb} = 40000 \text{ kb}$$

Maintenant, avec un débit de 56 kbps, le temps nécessaire pour télécharger le fichier est :

$$t = \frac{40000 \text{ kb}}{56 \text{ kb/s}} \approx 714.29 \text{ s}$$

Convertissons les secondes en minutes :

$$t \approx \frac{714.29}{60} \approx 11.9 \text{ minutes}$$

Donc, il faudrait environ 12 minutes pour télécharger un PDF de 5 Mo à un débit de 56 kbps ! Rien que ça.

Exercice 3.3 · Calcul du temps de téléchargement: fibre optique

Tout d'abord, convertissons 5 Mo en bits. Comme 1 Mo = 8 Mb (mégaoctets en mégabits) :

$$5 \text{ Mo} = 5 \times 8 \text{ Mb} = 40 \text{ Mb}$$

Ensuite, convertissons les mégabits en gigabits :

$$40 \text{ Mb} = \frac{40}{1000} \text{ Gb} = 0.04 \text{ Gb}$$

Maintenant, avec un débit de 1 Gbps, le temps nécessaire pour télécharger le fichier est :

$$t = \frac{0.04 \text{ Gb}}{1 \text{ Gb/s}} = 0.04 \text{ s}$$

Donc, il faudrait environ 0.04 secondes pour télécharger un PDF de 5 Mo à un débit de 1 Gbps ! C'est légèrement plus rapide que le modem 56k, n'est-ce pas ?

Exercice 3.4 · Conversion de la base 2 à la base 10

A. $1011_2 = 1 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 1 \times 2^0 = 8 + 0 + 2 + 1 = 11_{10}$

B. $1101_2 = 1 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0 = 8 + 4 + 0 + 1 = 13_{10}$

C. $10010_2 = 1 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 0 \times 2^0 = 16 + 0 + 0 + 2 + 0 = 18_{10}$

D. $111111_2 = 1 \times 2^5 + 1 \times 2^4 + 1 \times 2^3 + 1 \times 2^2 + 1 \times 2^1 + 1 \times 2^0 = 32 + 16 + 8 + 4 + 2 + 1 = 63_{10}$

Exercice 3.5 · Valeurs maximales sur n bits

A. Sur n bits, la plus grande valeur représentable est $2^n - 1$: soit $2^8 - 1 = 255$ sur 8 bits et $2^{16} - 1 = 65535$ sur 16 bits.

B. Avec 9 bits, on peut représenter au maximum $2^9 - 1 = 511 < 1000$. Avec 10 bits, on monte à $2^{10} - 1 = 1023 \geq 1000$. Il faut donc 10 bits.

Exercice 3.6 · Conversion de la base 16 aux bases 10 et 2

A. $1\text{A}_{16} = 1 \times 16^1 + A \times 16^0 = 1 \times 16 + 10 \times 1 = 16 + 10 = 26_{10}$ En binaire : $1\text{A}_{16} = 00011010_2$

B. $\text{FF}_{16} = F \times 16^1 + F \times 16^0 = 15 \times 16 + 15 \times 1 = 240 + 15 = 255_{10}$ En binaire : $\text{FF}_{16} = 11111111_2$

C. $2\text{B}_{16} = 2 \times 16^1 + B \times 16^0 = 2 \times 16 + 11 \times 1 = 32 + 11 = 43_{10}$ En binaire : $2\text{B}_{16} = 00101011_2$

D. $\text{C3}_{16} = C \times 16^1 + 3 \times 16^0 = 12 \times 16 + 3 \times 1 = 192 + 3 = 195_{10}$ En binaire : $\text{C3}_{16} = 11000011_2$

Exercice 3.7 · Conversion de la base 10 aux bases 2 et 16

A. $100 = 64 + 32 + 4$, donc $100_{10} = 1100100_2$

B. $173 = 128 + 32 + 8 + 4 + 1$, donc $173_{10} = 10101101_2$

C. $255 = 128 + 64 + 32 + 16 + 8 + 4 + 2 + 1$, donc $255_{10} = 11111111_2$ (la valeur maximale sur 8 bits !)

D. $300 = 1 \times 256 + 2 \times 16 + 12$, donc $300_{10} = 12\text{C}_{16}$

E. $4096 = 16^3$, donc $4096_{10} = 1000_{16}$

Exercice 3.8 · Opérateurs logiques fondamentaux

A. $0 \text{ AND } 1 = 0$

B. $1 \text{ XOR } 0 = 1$

C. D'abord, calculons les deux parties de l'expression :

- $0 \text{ AND } 1 = 0$
- $1 \text{ XOR } 0 = 1$

Ensuite, nous combinons les résultats avec l'opérateur OR :

- $0 \text{ OR } 1 = 1$

Le résultat final est donc 1.

D. D'abord, calculons la partie entre parenthèses :

- $0 \text{ OR } 1 = 1$

Ensuite, nous combinons le résultat avec l'opérateur AND :

- $1 \text{ AND } 1 = 1$

Le résultat final est donc 1.

E. D'abord, calculons les deux parties de l'expression :

- $1 \text{ XOR } 1 = 0$
- $0 \text{ AND } 1 = 0$

Ensuite, nous combinons les résultats avec l'opérateur OR :

- $0 \text{ OR } 0 = 0$

Le résultat final est donc 0.

Exercice 3.9 · Opérateurs logiques sur des mots binaires

A.

```
    1 0 1 0
AND 1 1 0 0
    -------
    1 0 0 0
```

B.

$$\begin{array}{rcccc} & 1 & 0 & 1 & 0 \\ \textbf{XOR} & 0 & 1 & 1 & 0 \\ \hline & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} \end{array}$$

C. D'abord, calculons la partie entre parenthèses :

- $A \text{ OR } B = 1110$

$$\begin{array}{rcccc} & 1 & 0 & 1 & 0 \\ \textbf{OR} & 1 & 1 & 0 & 0 \\ \hline & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} \end{array}$$

Ensuite, nous combinons le résultat avec l'opérateur AND :

- $1110 \text{ AND } C = 0110$

$$\begin{array}{rcccc} & 1 & 1 & 1 & 0 \\ \textbf{AND} & 0 & 1 & 1 & 0 \\ \hline & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} \end{array}$$

Le résultat final est donc 0110_2.

D. D'abord, calculons les deux parties de l'expression :

- $A \text{ XOR } B = 0110$

$$\begin{array}{rcccc} & 1 & 0 & 1 & 0 \\ \textbf{XOR} & 1 & 1 & 0 & 0 \\ \hline & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} \end{array}$$

- $B \text{ AND } C = 0100$

$$\begin{array}{rcccc} & 1 & 1 & 0 & 0 \\ \textbf{AND} & 0 & 1 & 1 & 0 \\ \hline & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} \end{array}$$

Ensuite, nous combinons les résultats avec l'opérateur OR :

- $0110 \text{ OR } 0100 = 0110$

$$\begin{array}{rcccc} & 0 & 1 & 1 & 0 \\ \textbf{OR} & 0 & 1 & 0 & 0 \\ \hline & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} \end{array}$$

Le résultat final est donc 0110_2.

E. D'abord, calculons les deux parties de l'expression :

- $A \text{ AND } C = 0010$

```
  1 0 1 0
AND 0 1 1 0
  ---------
  0 0 1 0
```

- $B \text{ OR } C = 1110$

```
  1 1 0 0
OR 0 1 1 0
  ---------
  1 1 1 0
```

Ensuite, nous combinons les résultats avec l'opérateur XOR :

- $0010 \text{ XOR } 1110 = 1100$

```
  0 0 1 0
XOR 1 1 1 0
  ---------
  1 1 0 0
```

Le résultat final est donc 1100_2.

Exercice 3.10 · Décodage d'un message binaire en ASCII

B (0x42), r (0x72), a (0x61), v (0x76), o (0x6F), ! (0x21)

Bravo!

Exercice 3.11 · Encodage d'un message en ASCII

- O (79, 0x4F) : 01001111
- k (107, 0x6B) : 01101011
- ! (33, 0x21) : 00100001

Soit : 01001111 01101011 00100001

Chapitre 4 · Protocoles et modèles en couches

Exercice 4.1 · Associer les éléments aux couches OSI

- A. Couche 7 (application)
- B. Couche 2 (liaison de données)
- C. Couche 4 (transport)
- D. Couche 1 (physique)
- E. Couche 3 (réseau)

- F. Couche 6 (présentation)
- G. Couche 4 (transport)

Exercice 4.2 · Ordre d'encapsulation

1. Message (couches 7 à 5)
2. Segment (couche 4)
3. Paquet (couche 3)
4. Trame (couche 2)
5. Bits (couche 1)

À la réception, l'ordre est inversé (décapsulation).

Chapitre 5 · Matériel

Exercice 5.1 · Choisir le bon équipement

- A. Switch
- B. Routeur
- C. Pare-feu
- D. Hub (solution historique ; aujourd'hui, un switch d'entrée de gamme fait mieux pour un prix comparable)

Exercice 5.2 · Équipements et couches OSI

- Hub : couche 1
- Switch : couches 1 et 2
- Routeur : couches 1 à 3
- Pare-feu simple : couches 1 à 4 (les pare-feu applicatifs montent jusqu'à la couche 7)

Exercice 5.3 · Choisir le bon médium

A. Fibre optique : distance trop grande pour le cuivre (100 m au maximum), débit élevé, insensible aux interférences électromagnétiques.

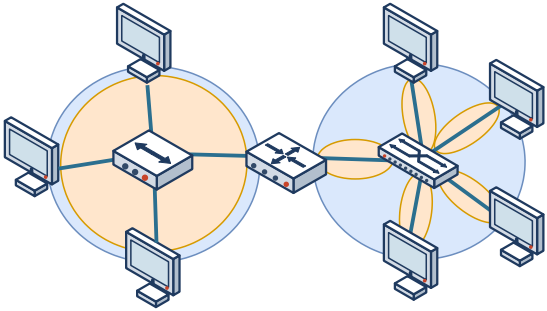
B. Paires torsadées : fiable, économique, débit largement suffisant.

C. LoRa : très faible débit, mais longue portée et faible consommation, idéal pour ce cas d'usage IoT.

D. 4G/5G : mobilité et couverture étendue.

Chapitre 6 · Accès au médium

Exercice 6.1 · Compter les domaines de collision et de diffusion



- Domaines de collision : 6. Chaque port actif du switch forme un domaine de collision : 4 pour les PC et 1 pour le lien switch-routeur, soit 5. Le hub ne sépare pas les domaines de collision : le hub, ses 3 PC et l'interface du routeur forment un seul domaine, soit 1 de plus.
- Domaines de diffusion : 2. Le routeur sépare les domaines de diffusion : un par interface.

Exercice 6.2 · Vrai ou faux : hub, switch et routeur

- A. Faux : un switch sépare les domaines de collision (un par port), mais tous ses ports appartiennent au même domaine de diffusion.
- B. Faux : un hub ne sépare ni les domaines de collision, ni les domaines de diffusion ; il répète le signal sur tous ses ports.
- C. Vrai : les routeurs ne transmettent pas les trames de diffusion d'une interface à l'autre.
- D. Vrai : le hub répète tout signal reçu sur tous ses autres ports, les collisions y sont donc possibles entre tous les périphériques.

Exercice 6.3 · Duplex et méthodes d'accès

Sur un lien Ethernet commuté moderne, chaque périphérique est relié à son propre port de switch par un lien point-à-point full-duplex : chaque sens de transmission dispose de son propre canal, sur lequel il n'y a qu'un seul émetteur possible. Le médium n'est donc plus partagé et aucune collision n'est possible : CSMA/CD devient inutile. En Wi-Fi au contraire, tous les périphériques émettent sur le même canal radio, qui est half-duplex et

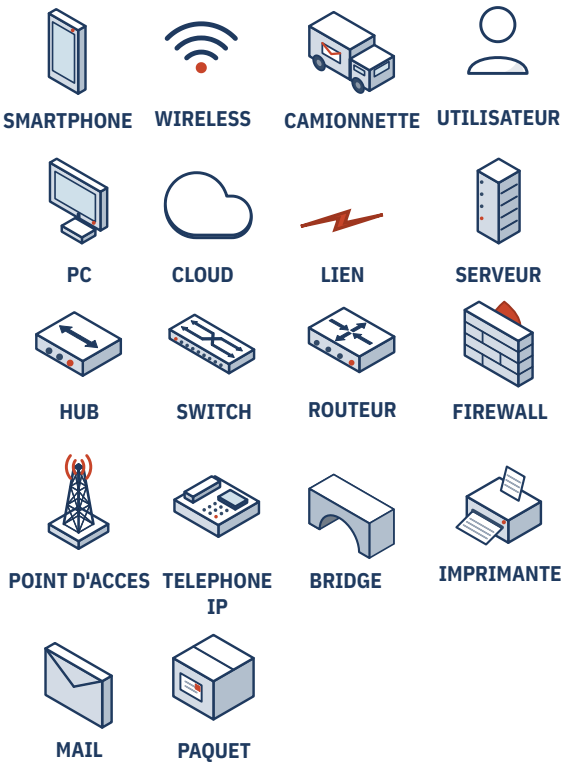
partagé : il y a plusieurs émetteurs potentiels sur le même médium, une méthode d'accès reste donc indispensable.

Exercice 6.4 · Dérouler CSMA/CD pas à pas

1. B et C écoutent le médium (carrier sense) : il est occupé par A, elles attendent donc sans émettre.
2. Lorsque A termine sa transmission, le médium devient libre. B et C le détectent et commencent toutes deux à émettre en même temps.
3. Une collision se produit. B et C la détectent (collision detection) et interrompent immédiatement leur transmission.
4. B et C attendent chacune un temps aléatoire différent, déterminé par l'algorithme de Binary Exponential Backoff.
5. La station dont le temps d'attente est le plus court (par exemple B) réessaie la première : le médium est libre, sa trame est transmise avec succès.
6. Lorsque C réessaie à son tour, elle écoute le médium : si B émet encore, elle attend la fin de la transmission, puis émet sa trame.

ANNEXE

Symboles réseau



ANNEXE

Glossaire

Termes et acronymes employés dans l'ouvrage, classés par ordre alphabétique.

A

ARP Address Resolution Protocol : protocole utilisé pour résoudre les adresses IP en adresses MAC sur un réseau local.

ASCII American Standard Code for Information Interchange : encodage de caractères sur 7 bits, permettant 128 caractères.

B

Bash Un shell populaire pour les systèmes Linux, qui offre des fonctionnalités avancées pour l'interprétation des commandes et la programmation de scripts.

Binaire Système de numération en base 2, utilisant les symboles 0 et 1.

Bit Binary digit : unité fondamentale de l'information, valant 0 ou 1.

Bitwise Se dit d'une opération logique appliquée bit par bit sur des mots binaires.

Bridge Pont : commutateur à deux ports reliant deux segments de réseau.

Broadcast Mode de transmission d'un émetteur vers tous les hôtes du domaine de diffusion.

Bruit Perturbation qui altère le signal pendant sa transmission et peut provoquer des erreurs de communication.

C

Canal Support par lequel le signal transite entre l'émetteur et le récepteur.

CRC Cyclic Redundancy Check : un algorithme utilisé pour détecter les erreurs de transmission dans une trame Ethernet.

CSMA/CA Carrier Sense Multiple Access with Collision Avoidance : protocole d'accès au média utilisé dans les réseaux sans fil pour gérer l'accès au support physique partagé et éviter les collisions de données.

CSMA/CD Carrier Sense Multiple Access with Collision Detection : protocole d'accès au média utilisé dans les réseaux Ethernet pour gérer l'accès au support physique partagé et détecter les collisions de données.

Câble coaxial Câble à conducteur central en cuivre entouré d'une tresse métallique, utilisé historiquement (10BASE2, 10BASE5, télévision par câble).

D

Débit Quantité d'information transmise par unité de temps, exprimée en bits par seconde.

Décapsulation Retrait, par chaque couche, de l'en-tête correspondant lors de la remontée du modèle en couches.

E

EMI ElectroMagnetic Interference : interférences électromagnétiques, auxquelles le cuivre est sensible, contrairement à la fibre optique.

En-tête (header) Informations de contrôle ajoutées par une couche devant les données ; la couche liaison de données ajoute aussi une queue (trailer).

Encapsulation Ajout, par chaque couche, d'un en-tête aux données reçues de la couche supérieure lors de la descente du modèle en couches.

EtherType Un champ de 2 octets dans l'en-tête d'une trame Ethernet de type II qui indique le protocole de la couche supérieure (L3, réseau) utilisé pour traiter les données contenues dans la trame.

F

FCS Frame Check Sequence : un champ de 4 octets dans une trame Ethernet utilisé pour détecter les erreurs de transmission.

Fibre monomode Fibre optique à un seul mode de propagation de la lumière, utilisée pour les longues distances.

Fibre multimode Fibre optique à plusieurs modes de propagation, utilisée pour les courtes distances (réseaux locaux, centres de données).

Fibre optique Médium transmettant les données par la lumière, offrant de très hauts débits et une très faible atténuation.

G

GAN Global Area Network : réseau à l'échelle mondiale, p. ex. réseaux satellitaires.

GNU Un projet de logiciels libres qui fournit de nombreux outils et utilitaires pour les systèmes d'exploitation de type Unix, souvent utilisés avec le noyau Linux.

H

Hexadécimal Système de numération en base 16, utilisant les symboles 0 à 9 et A à F.

Hub Concentrateur : équipement de couche 1 qui retransmet chaque signal reçu à tous les autres ports.

Hôte (host) Noeud d'un réseau, qu'il soit terminal (ordinateur, smartphone) ou intermédiaire (routeur, switch).

I

ICMP Internet Control Message Protocol : protocole de la couche réseau utilisé pour envoyer des messages de contrôle et de diagnostic, comme les messages d'erreur et les requêtes de ping.

ICMPv6 Internet Control Message Protocol version 6 : version d'ICMP utilisée dans les réseaux IPv6 pour envoyer des messages de contrôle et de diagnostic.

IEEE Institute of Electrical and Electronics Engineers : organisme de normalisation, notamment des réseaux locaux (famille 802.x).

IETF Internet Engineering Task Force : organisme qui normalise les protocoles d'Internet à travers les RFC.

IoT Internet of Things : Internet des objets, désigne l'ensemble des objets connectés à Internet et capables de communiquer entre eux ou avec des serveurs.

IP Internet Protocol : protocole de la couche réseau responsable de l'adressage logique et du routage des paquets de données sur Internet.

IPv4 Internet Protocol version 4 : version du protocole IP utilisant des adresses sur 32 bits, permettant d'adresser environ 4,3 milliards d'hôtes.

IPv6 Internet Protocol version 6 : version du protocole IP utilisant des adresses sur 128 bits, permettant d'adresser un nombre quasi infini d'hôtes et de résoudre le problème de pénurie d'adresses IPv4.

ISO International Organization for Standardization : organisme international de normalisation, à l'origine du modèle OSI.

L

LAN Local Area Network : réseau local à l'échelle d'un bâtiment ou d'un site.

Latence Temps nécessaire à un signal pour parcourir le canal de l'émetteur au récepteur, généralement exprimé en millisecondes.

Linux Un système d'exploitation de type Unix, open-source et basé sur le noyau Linux. Il est utilisé sur une variété de dispositifs, allant des serveurs aux ordinateurs personnels et aux appareils embarqués.

M

MAC Media Access Control : sous-couche de la couche liaison de données responsable de la gestion des adresses physiques et de l'accès au support physique partagé.

MAN Metropolitan Area Network : réseau métropolitain à l'échelle d'une ville ou d'un campus.

MDI Medium Dependent Interface : câblage d'interface Ethernet des équipements terminaux et des routeurs.

MDIX MDI crossover : câblage d'interface inversé, utilisé par les switches et les hubs ; l'auto-MDI/MDIX rend le choix du câble droit ou croisé transparent.

MTU Maximum Transmission Unit : la taille maximale d'un paquet qui peut être transmis sur un réseau. Pour Ethernet, la MTU est généralement de 1500 octets, ce qui correspond à la taille maximale d'un payload de trame Ethernet II.

Multicast Mode de transmission d'un émetteur vers un groupe de récepteurs.

Médium Support de transmission (câble, fibre optique, ondes radio) permettant la circulation des données entre les périphériques.

N

NDP Neighbor Discovery Protocol : protocole utilisé dans les réseaux IPv6 pour la découverte des voisins et la résolution d'adresses, remplaçant ARP.

Nibble Groupe de 4 bits, correspondant à un chiffre hexadécimal.

O

Octet Groupe de 8 bits, unité usuelle de quantification des données (byte en anglais).

OSI Open Systems Interconnection : modèle de référence en sept couches pour la communication entre systèmes informatiques.

OSPF Open Shortest Path First : protocole de routage de la couche réseau utilisé pour échanger des informations de routage entre les périphériques d'un réseau, basé sur l'algorithme du plus court chemin.

OUI Organizationally Unique Identifier : les trois premiers octets d'une adresse MAC, identifiant le fabricant.

P

PAN Personal Area Network : réseau personnel de très courte portée (quelques mètres), p. ex. Bluetooth.

Pare-feu Firewall : équipement de sécurité filtrant le trafic réseau selon des règles prédéfinies (adresses IP, ports, voire contenu applicatif).

Passerelle (gateway) Équipement d'interconnexion entre réseaux ; désigne couramment le routeur de sortie d'un réseau local.

PDU Protocol Data Unit : unité de données utilisée par une couche du modèle OSI pour communiquer avec les autres couches.

Port Identifiant de la couche transport permettant de distinguer les applications s'exécutant sur un même hôte.

Protocole Ensemble de règles et de conventions régissant la communication entre les périphériques d'un réseau.

R

RFC Request for Comments : document publié par l'IETF définissant les protocoles et normes d'Internet.

RIP Routing Information Protocol : protocole de routage de la couche réseau utilisé pour échanger des informations de routage entre les périphériques d'un réseau.

RJ45 Connecteur standard des câbles à paires torsadées (nom technique : 8P8C).

Routeur Équipement de couches 1 à 3 qui achemine les paquets entre réseaux à l'aide d'une table de routage.

Réseau informatique Mise en relation d'au moins deux systèmes informatiques au moyen d'un médium de communication.

S

Shell Un programme qui interprète les commandes de l'utilisateur et les exécute. Il fournit une interface en ligne de commande pour interagir avec le système d'exploitation.

Signal Grandeur physique porteuse d'information, transmise d'un émetteur à un récepteur à travers un canal.

Signal analogique Signal continu pouvant prendre une infinité de valeurs.

Signal numérique Signal discret ne pouvant prendre qu'un nombre fini de valeurs.

SPOF Single Point of Failure : élément dont la panne entraîne l'arrêt de l'ensemble du système.

STP Shielded Twisted Pair : câble à paires torsadées blindées, plus résistant aux interférences.

Switch Commutateur : équipement de couches 1 et 2 qui commute les trames vers le port du destinataire grâce à sa table d'adresses MAC.

T

Table de routage Table utilisée par un routeur pour déterminer le chemin des paquets vers leur réseau de destination.

Table de vérité Tableau énumérant les sorties d'un opérateur logique pour toutes les combinaisons d'entrées possibles.

TCP Transmission Control Protocol : protocole de la couche transport assurant une communication fiable, orientée connexion, avec contrôle de flux et retransmission des segments perdus.

TCP/IP Transmission Control Protocol/Internet Protocol : ensemble de protocoles utilisés pour la communication sur Internet.

Topologie Forme d'organisation des liens d'un réseau : bus, anneau, étoile, maillée ou arbre.

Téléinformatique Association des techniques des télécommunications et de l'informatique pour réaliser l'échange de données à distance.

U

UDP User Datagram Protocol : protocole de la couche transport assurant une communication non fiable, sans connexion, avec un faible overhead et une faible latence.

Unicast Mode de transmission d'un émetteur vers un récepteur unique (point à point).

UTF-8 Encodage de caractères à longueur variable, compatible ASCII, couvrant l'ensemble des langues.

UTP Unshielded Twisted Pair : câble à paires torsadées non blindées.

W

WAN Wide Area Network : réseau étendu couvrant de grandes zones géographiques et interconnectant plusieurs LAN.

WLAN Wireless Local Area Network : réseau local utilisant des technologies sans fil.

ANNEXE

Bibliographie

[1] International Telecommunication Union, « Measuring Digital Development: Facts and Figures 2025 », technical report, 2025. Consulté le: 10 juillet 2026. [En ligne]. Disponible sur: https://www.itu.int/itu-d/reports/statistics/facts-figures-2025/

[2] C. Külling, G. Waller, L. Suter, I. Willemse, J. Bernath, et D. Süss, « JAMES — Jeunes, activités, médias : enquête Suisse 2024 », technical report, 2024. Consulté le: 10 juillet 2026. [En ligne]. Disponible sur: https://www.zhaw.ch/storage/psychologie/upload/forschung/medienpsychologie/james/2018/JAMES_2024_FR.pdf

[3] UNESCO, « Global Education Monitoring Report 2023. Technology in education: A tool on whose terms? », technical report, 2023. Consulté le: 10 juillet 2026. [En ligne]. Disponible sur: https://www.unesco.org/gem-report/en/technology

[4] G. Flodgren, A. Rachas, A. J. Farmer, M. Inzitari, et S. Shepperd, « Interactive telemedicine: effects on professional practice and health care outcomes », *Cochrane Database of Systematic Reviews*, nº 9, p. CD002098, 2015, doi: 10.1002/14651858.CD002098.pub2.

[5] Office fédéral de la statistique, « Enquête sur l'utilisation d'internet 2025 », technical report, 2025. Consulté le: 10 juillet 2026. [En ligne]. Disponible sur: https://www.bfs.admin.ch/bfs/fr/home/statistiques/culture-medias-societe-information-sport/societe-information/indicateurs-generaux/menages-population/utilisation-internet.html

[6] International Energy Agency, « Energy and AI », technical report, 2025. Consulté le: 10 juillet 2026. [En ligne]. Disponible sur: https://www.iea.org/reports/energy-and-ai

[7] C. Freitag, M. Berners-Lee, K. Widdicks, B. Knowles, G. S. Blair, et A. Friday, « The real climate and transformative impact of ICT: A critique

of estimates, trends, and regulations », *Patterns*, vol. 2, nº 9, p. 100340, 2021, doi: 10.1016/j.patter.2021.100340.

[8] Cambridge Centre for Alternative Finance, « Cambridge Bitcoin Electricity Consumption Index (CBECI) ». Consulté le: 10 juillet 2026. [En ligne]. Disponible sur: https://ccaf.io/cbnsi/cbeci

ANNEXE

Index

A
ARP —
ASCII 24, 44

B
Bash —
Binaire 23
Bit 23, 42
Bitwise 35
Bridge 57
Broadcast 11, 69
Bruit 11

C
Canal 11, 26, 72
CRC —
CSMA/CA 42, 73
CSMA/CD 42, 69
Câble coaxial 64

D
Débit 9, 21, 25, 62, 76
Décapsulation 39

E
EMI 60
En-tête (header) 20, 25, 46, 62, 77
Encapsulation 39
EtherType —

F
FCS —
Fibre monomode 65
Fibre multimode 65
Fibre optique 6, 26, 42, 60, 73

G
GAN 20
GNU —

H
Hexadécimal 23
Hub 56, 70
Hôte (host) 57

I
ICMP 43
ICMPv6 —
IEEE 42, 62
IETF 50
IoT 8, 66
IP 4, 39, 59
IPv4 43
IPv6 43
ISO 40, 62

L
LAN 20, 60
Latence 4, 26, 43, 66, 74
Linux 30

M
MAC 42, 57
MAN 20
MDI 63
MDIX 63
MTU —
Multicast 11
Médium 6, 47, 60, 69

N
NDP —
Nibble 28

O
Octet 23
OSI 39, 55, 69
OSPF 43
OUI —

P
PAN 20
Pare-feu 8, 55
Passerelle (gateway) 58
PDU 42
Port 43, 59, 70
Protocole 4, 17, 39, 69

R

RFC 50
RIP 43
RJ45 55
Routeur 7, 55, 70
Réseau informatique 6, 40, 55

S

Shell ..... —
Signal 4, 11, 26, 56, 71
Signal analogique 11
Signal numérique 11
SPOF 18
STP 61
Switch 7, 55, 70

T

Table de routage 58
Table de vérité 32
TCP 4, 39, 59
TCP/IP 4, 39
Topologie 16, 70
Téléinformatique 1, 11, 23, 39

U

UDP 43, 59
Unicast 11
UTF-8 37
UTP 61

W

WAN 20, 60
WLAN 21