

République Algérienne Démocratique et Populaire  
Ministère de L'enseignement Supérieur et de la Recherche Scientifique  
Centre Universitaire NOUR el Bachir EL BAYADH  
Institut des Technologie  
Département de Génie Electrique



## *Polycopie de Cours*

*1ère Année Master  
Réseaux et Télécommunications (Semestre 01)*

# *Normes et Protocoles*



### Informations sur Auteur :

Nom et Prénom : MENEZLA Fayssal  
Grade : Maitre Conférence Classe A -MCA-  
Etablissement : Centre Universitaire NOUR Bachir - EL BAYADH-  
Email : [f.menezla@cu-elbayadh.dz](mailto:f.menezla@cu-elbayadh.dz)

Année Universitaire : 2024/2025

## AVANT PROPOS

Dans un monde où les technologies de l'information et de la communication évoluent à un rythme soutenu, la maîtrise des **normes** et **protocoles** de communication devient un pilier fondamental pour tout ingénieur ou spécialiste des réseaux. La diversité des environnements de communication – qu'ils soient filaires, sans fil, fixes ou mobiles – impose une compréhension rigoureuse des mécanismes de normalisation, des structures protocolaires et de leur rôle dans l'interopérabilité des systèmes.

Ce cours intitulé « **Normes et Protocoles** » a été conçu pour fournir à l'étudiant une base solide dans le domaine des standards de télécommunication, en lui permettant d'acquérir une vision claire et hiérarchisée des différents protocoles utilisés à travers les couches des modèles OSI et TCP/IP. Il permet également de comprendre le rôle stratégique des institutions de normalisation (telles que l'ITU, l'IEEE ou l'ISO) dans le développement et la diffusion des standards internationaux.

Cette polycopie présente le cours de Normes et Protocoles est adressé particulièrement aux étudiants de la 1<sup>ère</sup> Année Master Réseaux et Télécommunications (Semestre 01).

Les enseignements dispensés couvrent à la fois les aspects **historiques**, **techniques** et **pratiques** des normes liées aux réseaux numériques, aux transmissions audiovisuelles, aux réseaux sans fil, ainsi qu'à l'écosystème Internet. L'objectif est de former des étudiants capables non seulement de comprendre les protocoles existants, mais également d'analyser et de spécifier des solutions de communication adaptées aux besoins modernes.

Cet avant-propos vise ainsi à contextualiser les enjeux du cours et à motiver l'étudiant à approfondir ses connaissances dans un domaine aussi transversal que stratégique pour les métiers de l'ingénierie des télécommunications.

## Plan du Cours

### Chapitre 1 : Notions fondamentales

- Définitions : standard, norme, recommandation, protocole
- Rôle des protocoles dans les systèmes de communication
- Institutions de normalisation (ITU, ISO, IEC, IEEE, ETSI, etc.)
- Historique et évolution des processus de normalisation

### Chapitre 2 : Normes associées à la diffusion analogique et numérique

- Normes audio/vidéo analogiques : CCIR, NTSC, PAL, SECAM
- Normes audio/vidéo numériques : DVB, ATSC, ISDB, NICAM
- Transition de l'analogique vers le numérique

### Chapitre 3 : Normes des réseaux de communication numérique

- Classification des réseaux (LAN, MAN, WAN, etc.)
- Évolution historique des réseaux et de leur normalisation
- Modèles de référence OSI et TCP/IP : rappels et correspondances
- Protocoles des niveaux trame (Ethernet, PPP) et paquet (IP)
- Protocoles de niveau segment/message (TCP, UDP)
- Protocoles liés à l'ADSL et aux accès haut débit

### Chapitre 4 : Protocoles des réseaux sans fil et mobiles

- Protocoles IEEE 802.11 (Wi-Fi), 802.15 (Bluetooth), 802.16 (WiMAX)
- Protocoles de téléphonie mobile : GSM, GPRS, EDGE
- Protocoles 3G (UMTS), 4G (LTE), et introduction à la 5G

### Chapitre 5 : Protocoles Internet

- Historique et architecture de l'Internet
- Classification fonctionnelle des protocoles Internet
- Protocoles de messagerie : SMTP, POP3, IMAP
- Protocoles de transfert de fichiers et d'information : HTTP, FTP, DNS, Telnet
- Protocoles d'application et sécurité (notions de base)

*Introduction*

*Générale*

## ***Introduction Générale***

Dans le domaine des télécommunications et des technologies de l'information, les normes et protocoles jouent un rôle fondamental dans l'interopérabilité, la fiabilité et la sécurité des systèmes de communication. Sans un langage commun et des règles bien établies, il serait impossible pour les équipements, les applications et les réseaux de communiquer efficacement. Ainsi, comprendre les normes et les protocoles revient à comprendre les fondations mêmes de la communication numérique moderne.

Le cours intitulé « Normes et Protocoles » s'inscrit dans une logique de consolidation des acquis fondamentaux des étudiants en réseaux et télécommunications. Il vise à doter les apprenants des compétences théoriques et pratiques nécessaires à la compréhension, à l'analyse et à la mise en œuvre des différents protocoles utilisés dans les systèmes de communication actuels, qu'ils soient filaires ou sans fil, locaux ou étendus, analogiques ou numériques.

### **Objectifs pédagogiques**

Les objectifs principaux de ce cours sont les suivants :

- Familiariser l'étudiant avec les protocoles de communication les plus couramment utilisés dans l'industrie.
- Apprendre à identifier et classifier les protocoles selon les couches des modèles OSI et TCP/IP.
- Comprendre les principes de la normalisation, le rôle des organismes internationaux et le processus de développement des standards.
- Acquérir des connaissances pratiques sur les normes liées à la diffusion audiovisuelle, aux réseaux numériques, aux communications mobiles et à l'Internet.
- Développer une capacité à spécifier, analyser et choisir des protocoles selon le contexte applicatif et les exigences du système.

## **Connaissances préalables**

Pour tirer pleinement profit de ce cours, l'étudiant doit avoir acquis certaines connaissances de base, notamment :

- ❖ Les principes de la théorie de l'information, incluant les notions d'entropie, de débit binaire et de capacité de canal.
- ❖ La structure d'un réseau informatique, avec ses composants fondamentaux (nœuds, liaisons, routeurs, etc.).
- ❖ Ces prérequis permettront une meilleure assimilation des mécanismes protocolaires et de leur rôle fonctionnel dans un réseau.

## **Contenu du cours**

Le contenu du cours est organisé de manière progressive à travers cinq chapitres complémentaires, répartis sur un semestre :

- ***Chapitre 1 : Notions fondamentales***
- ***Chapitre 2 : Normes de diffusion analogique et numérique***
- ***Chapitre 3 : Normes des réseaux de communication numérique***
- ***Chapitre 4 : Protocoles des réseaux sans fil et mobiles***
- ***Chapitre 5 : Protocoles Internet***

## **Méthodologie pédagogique**

Le cours sera dispensé à travers des exposés magistraux, accompagnés de supports visuels, d'études de cas et d'exemples concrets tirés du monde industriel. Des séances de discussion permettront également d'explorer l'actualité des normes émergentes (comme la 5G ou les protocoles IoT).

## **Évaluation**

L'évaluation repose exclusivement sur un examen final noté sur 100%. Il portera sur l'ensemble des chapitres et visera à tester la compréhension des concepts, la capacité d'analyse des protocoles et la maîtrise des structures normatives.

# *Chapitre I*

# Normes et Protocoles

## Chapitre 1

### Notions fondamentales

- INSTITUTIONS DE NORMALISATION EN TÉLÉCOMMUNICATION
- HISTORIQUE ET ÉVOLUTION.
- STANDARDS, RECOMMANDATIONS, NORMES ET PROTOCOLES (DÉFINITIONS ET DIFFÉRENCES).
- RÔLE D'UN PROTOCOLE.

# Organisation internationale de normalisation

**Organisation Internationale de Normalisation**

**ISO International Organization for Standardization**

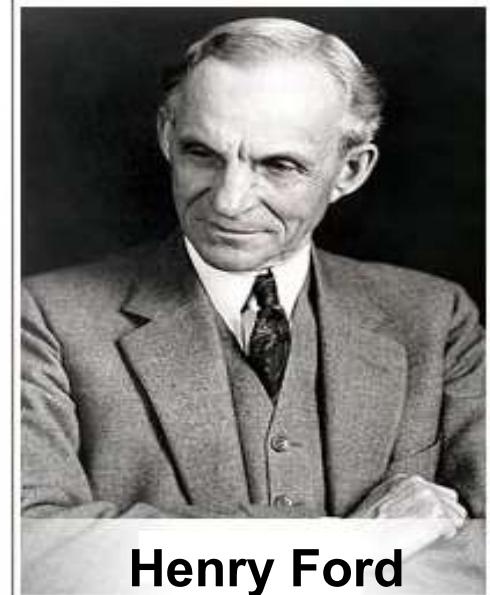
- Organisation composé de représentants d'organisations nationales de normalisation de 165 pays.
- Crée en 1947 a pour but de produire des normes internationales dans les domaines industriels et commerciaux appelées normes ISO.
- Le secrétariat central de l'ISO est situé à Genève, en Suisse.
- L'ISO est le plus grand organisme de normalisation au monde. C'est une organisation non gouvernementale représentant un réseau d'instituts nationaux de 165 pays, selon le principe d'un membre par pays.

# Histoire des Normes



Egypte, environ 7000 ans av. J.-C. : Une pièce cylindrique normalisée était utilisée comme unité de poids

# Histoire des normes



**Henry Ford**

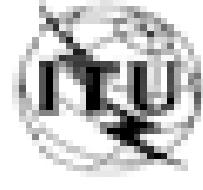
**Henry Ford** : La normalisation des composants a permis la production en série des automobiles

# Histoire des normes



Les normes dans le monde contemporain : Windows, lecteurs DVD, communications et téléphonie mobiles, etc.

# Qui élabore les normes?

- Organisations formelles traditionnelles, notamment :
  - **Organismes internationaux de normalisation**  
par ex. ISO, CEI et UIT
  - **Organismes nationaux et régionaux de normalisation**  
par ex. BSI, KATS, CEN
  - Organisations gouvernementales, par ex. Codex, OMI, CEE/ONU :
  - ASTM, ASME, IEEE, API
- Consortiums industriels  
par ex. W3C, UDDI, etc. (environ 400, selon les statistiques européennes)
- Normalisation *de facto*, par ex. MS Windows, VHS, etc.
- Normes privées pour usage interne

# Définition d'une norme

## Qu'est-ce qu'une norme?

- Une norme est un document établi par voie de consensus entre experts du sujet et approuvé par un organisme reconnu, qui fournit des lignes directrices sur la conception, l'utilisation ou la performance des matériaux, produits, processus, services, systèmes ou personnes.

## Définition formelle de la norme (ISO/CEI : Guide 2)

- Document, établi par consensus et approuvé par un organisme reconnu, qui fournit, pour des usages communs et répétés, des règles, des lignes directrices ou des caractéristiques, pour des activités ou leurs résultats, garantissant un niveau d'ordre optimal dans un contexte donné .

# Parties prenantes à la normalisation

Toutes les parties prenantes peuvent contribuer  
à la normalisation et en bénéficier



# Avantages des normes

- Assurer la cohérence d'aspects essentiels des biens et services, par ex. la sécurité ou l'interopérabilité
- Codifier les technologies les plus récentes et faciliter leur transfert
- Aider à améliorer l'efficacité, la sécurité et la propreté du développement, de la fabrication et de la fourniture de produits et de services.
- Faciliter le commerce entre les pays et le rendre plus équitable
- Les Normes internationales sont cohérentes au sein d'un système global
- **Protéger les utilisateurs et les consommateurs**

# Réglementation technique: avantages du recours aux normes

- ***Les normes sont d'application volontaire; les règlements sont obligatoires***
- Les normes citées en référence dans la réglementation deviennent obligatoires
- **Avantages** : utilisation des compétences techniques existantes, commerce amélioré  
exemple : la législation européenne fait référence aux normes européennes
- Différents modes de référence aux normes :
  - Référence directe : Numéro et titre de la norme, dans le texte de la loi
  - Référence indirecte: norme enregistrée sur une liste publique officielle
- **Publication** : « *Utilisation des normes ISO et CEI et de la référence à celles-ci dans la réglementation technique* »

Téléchargeable sur les sites Web de l'ISO et de la CEI : [www.iso.org](http://www.iso.org) ou [www.iec.ch](http://www.iec.ch)

# Qu'attendent les consommateurs des produits et services?

Les consommateurs veulent :

- les MEILLEURS produits et services
- au MOINDRE coût
- disponible au PLUS GRAND NOMBRE



Qu'entend-on par « MEILLEURS » produits et services et comment les normes peuvent-elles y contribuer?

# Les principes de Consumers International concernant les consommateurs : Droits et responsabilités

## Le droit à :

- La satisfaction des besoins de base
- La sécurité
- L'information
- La possibilité de choisir
- Etre entendu
- La réparation
- L'éducation du consommateur
- Un environnement sain et propre



# Questions relatives aux consommateurs traditionnellement abordées par les normes

- Spécification des performances
- Réduction des dangers au minimum
- Définition de l'information et des instructions sur les produits et services
- Spécification des avis de sécurité
- Garantie de l'uniformité ou de la compatibilité
- Spécification de la composition ou des matériaux
- Définition de la qualité

# Nouvelles questions relatives aux consommateurs au 21<sup>e</sup> siècle

- Réduire au minimum l'impact environnemental
- Durabilité de l'environnement et du tissu social
- Consommation d'énergie
- Aborder le problème de l'exploitation
- Comportement/ valeurs/ éthique des entreprises
- Conception inclusive/disponibilité
- Questions de sécurité

**Les normes ont un rôle à jouer pour traiter toutes ces questions**

# Certaines récentes initiatives de normalisation des consommateurs

- Protection contre les UV dans les vêtements (GB & Australie)
- Sécurité des piscines d'hôtel (UE)
- Protection de l'information personnelle (Canada)
- Berceaux (USA)
- Couches jetables (Corée)
- Facturation des services publics (COPOLCO)
- Gestion des réclamations (COPOLCO)
- Résolution externe de conflits (COPOLCO)
- Articles d'occasion (COPOLCO)
- Sécurité de l'image (IWA, avec conseils du COPOLCO)

## **Le cadre général – Comment les consommateurs peuvent contribuer à l'élaboration de normes**

- Influer sur le « domaine d'application» de la norme
- Fournir des données sur les dangers
- Aborder les questions de sécurité, de commodité et de durabilité
- Fournir des informations sur le mode d'utilisation des produits dans la pratique et les usages abusifs courants
- Garantir que les marquages et modes d'emploi sont adaptés
- Vérifier que les méthodes d'essai et spécifications de performance correspondent à l'usage dans la pratique
- Remettre en question les idées reçues

# Quelques exemples de normes où les consommateurs ont « fait la différence »

- Gilets de sauvetage
- Tondeuses à gazon
- Contraception
- Sécurité de l'eau
- Cars scolaires



- Llandaus et poussettes
- Etiquetage environnemental
- Normes pour la plongée
- Guide ISO/CEI 71 (sur les besoins des personnes âgées & des handicapés)

# Priorités émergentes des consommateurs dans la normalisation internationale

- Sécurité publique, confidentialité et sécurité
- Articles d'occasion
- Normes pour les services (jusqu'à présent : tourisme et services financiers)
- Autres questions liées au marché mondial, par ex.
  - Achats en ligne
  - Responsabilité sociétale (RS) et de l'environnement

**Les nouvelles questions intéressant les consommateurs et le rôle des normes sont examinés tous les ans par le COPOLCO**

# Influencer les priorités des consommateurs en matière de normes dans votre pays ou votre région

Les questions relatives aux consommateurs ont plus de chance d'être traitées dans les normes si les consommateurs sont impliqués dans l'élaboration :

- d'une politique et de priorités pour les consommateurs au sein de l'organisme national de normalisation
- de normes au niveau technique



**Vos initiatives possibles seront examinées ultérieurement dans ce cours.**

# Protocoles

- Un protocole est une série d'étapes à suivre pour permettre une communication harmonieuse entre plusieurs ordinateurs ou périphériques reliés en réseau.

# Protocoles

- Les protocoles sont classés en deux catégories :
- Les protocoles où les machines s'envoient des accusés de réception (pour permettre une gestion des erreurs). Ce sont les protocoles dits **orientés connexion**.
- Les autres protocoles qui n'avertissent pas la machine qui va recevoir les données sont les protocoles dits **non orientés connexion**.

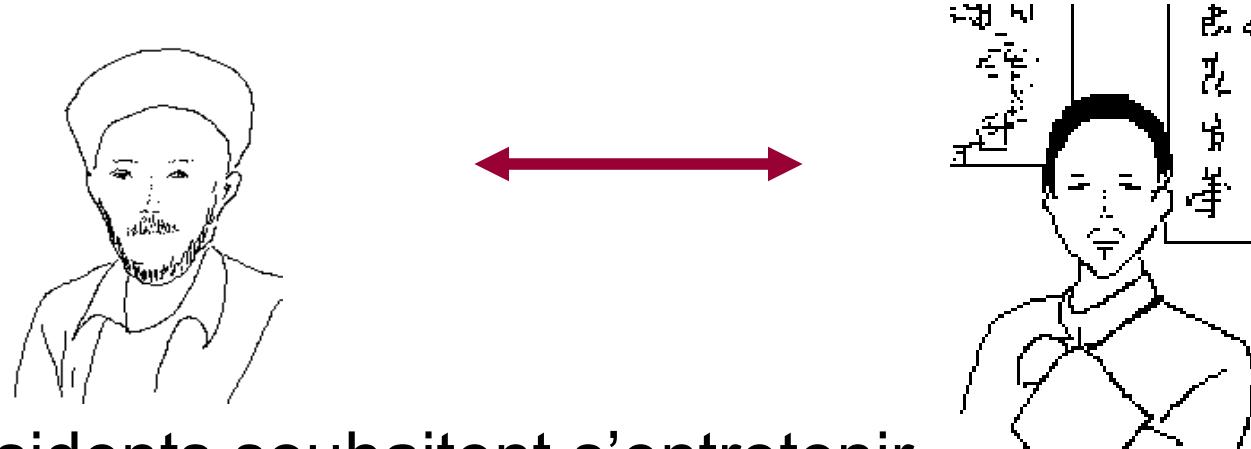
# Rôles des protocoles

- Identification du début et de la fin de chaque élément d'un bloc
- Fonctions de commandes telles que l'initialisation, l'interrogation, l'identification des équipements
- Détection des erreurs de transmission

# Couches de protocoles

- Les protocoles sont hiérarchisés en quatre couches dans le modèle TCP/IP (Transmission Control Protocol / Internet Protocol), ou en sept couches dans le modèle OSI (Open Standard Interconnection).
- Chaque couche s'occupe d'apporter un plus permettant la transmission de données, et de fournir des éléments avec les couches de niveau supérieur.

# Communication en couches

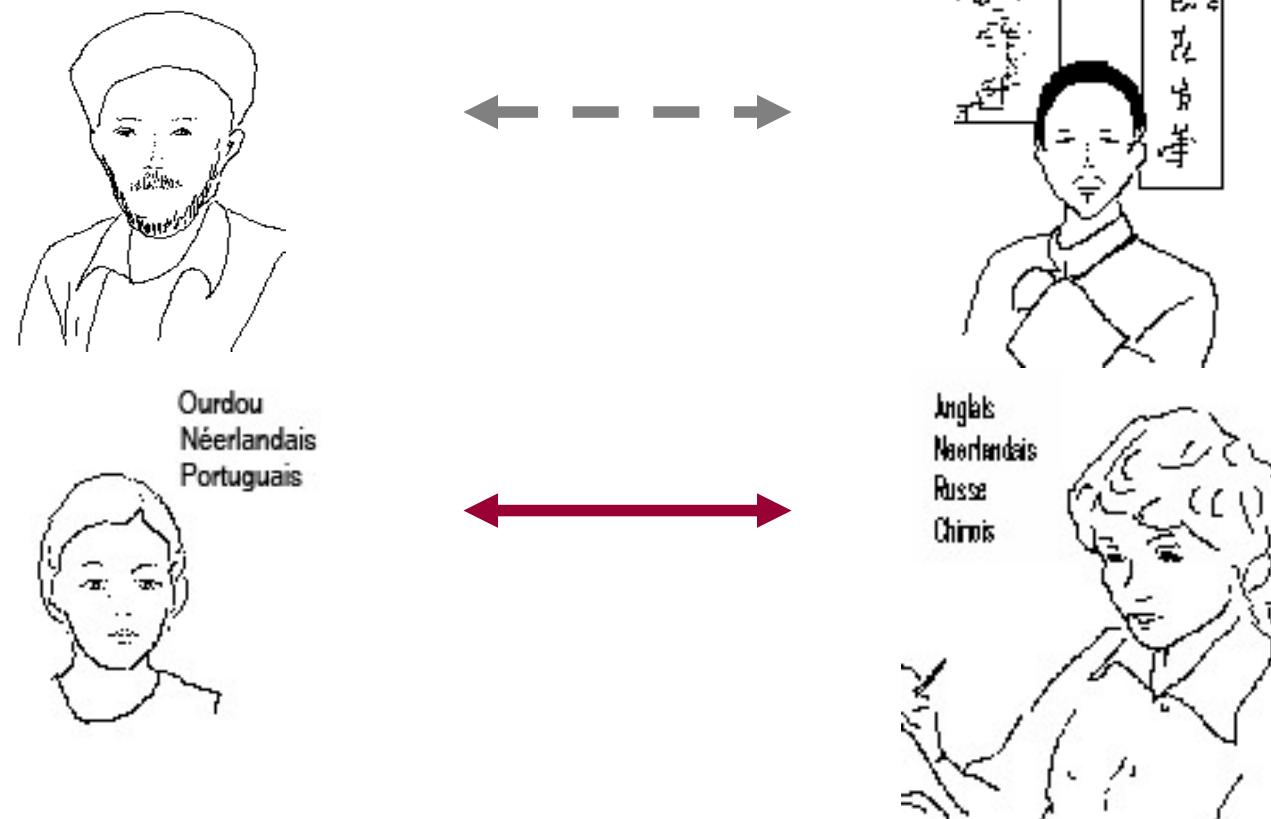


Deux présidents souhaitent s'entretenir

- L'un ne parle que ourdou et anglais
- L'autre ne parle que chinois et français

Faute de partager une langue commune,  
ils engagent chacun un traducteur.

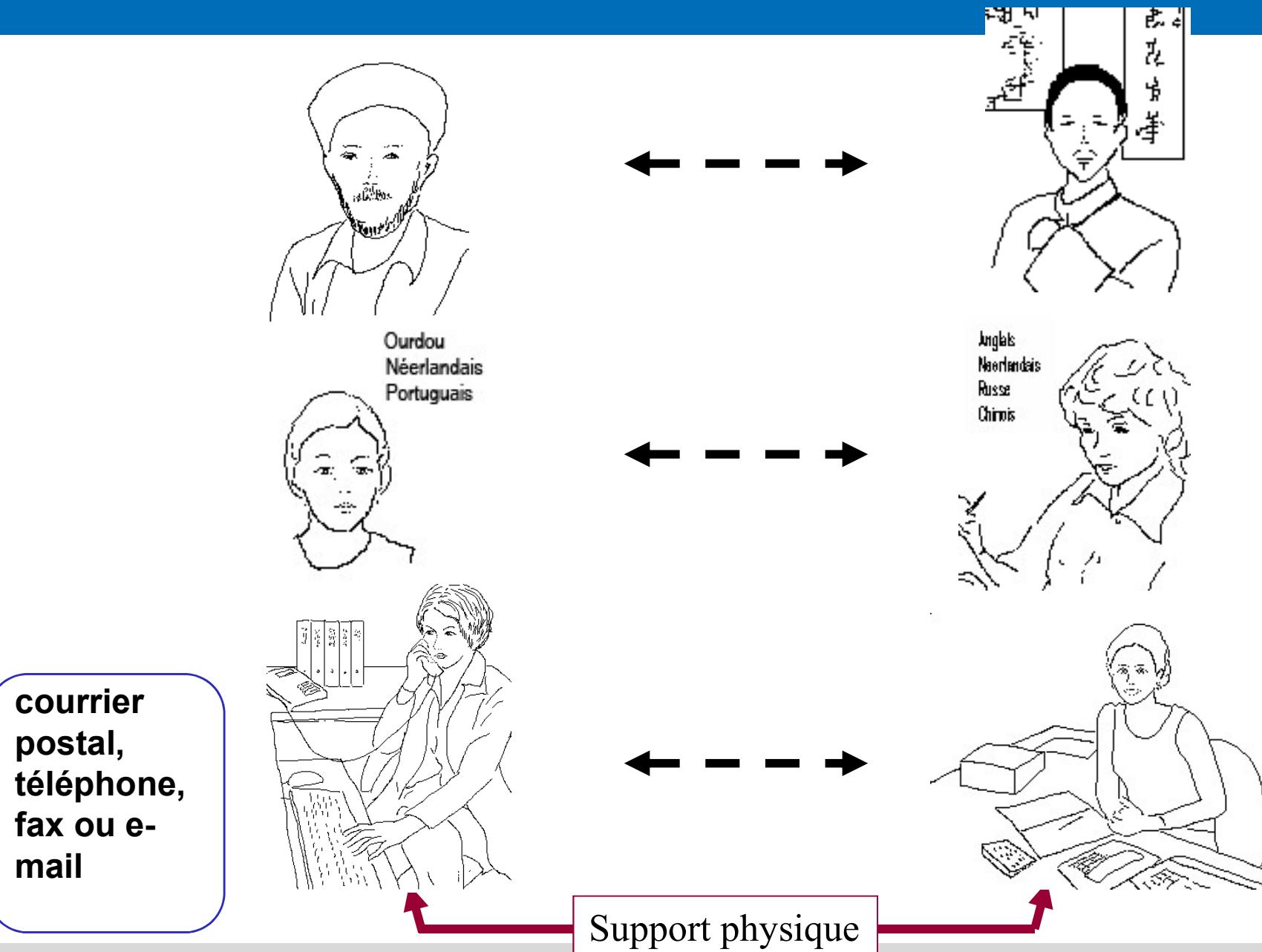
# Communication en couches



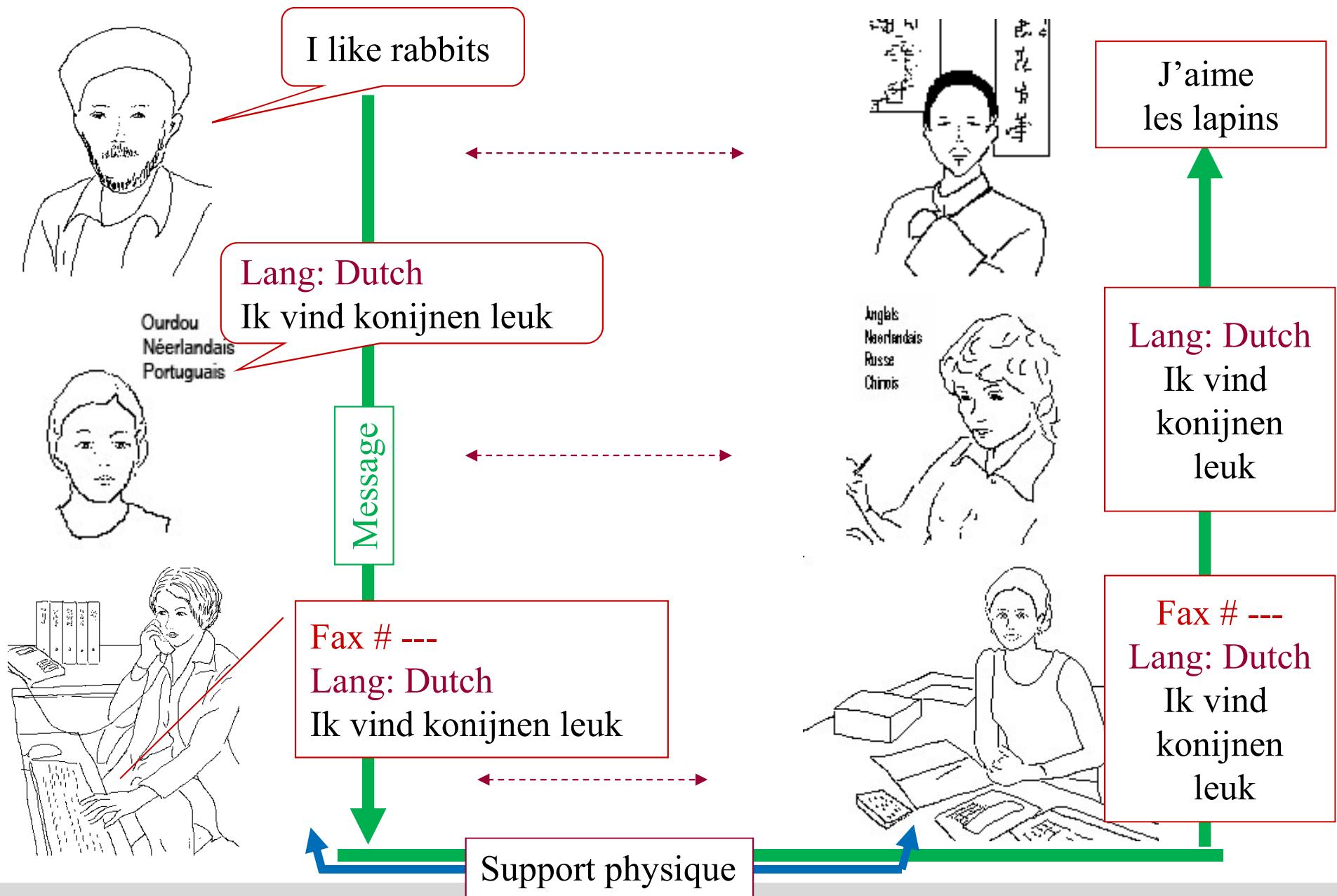
Chaque président a engagé une traductrice

Qui a son tour fait appel à une secrétaire

# Communication en couches



# Communication en couches

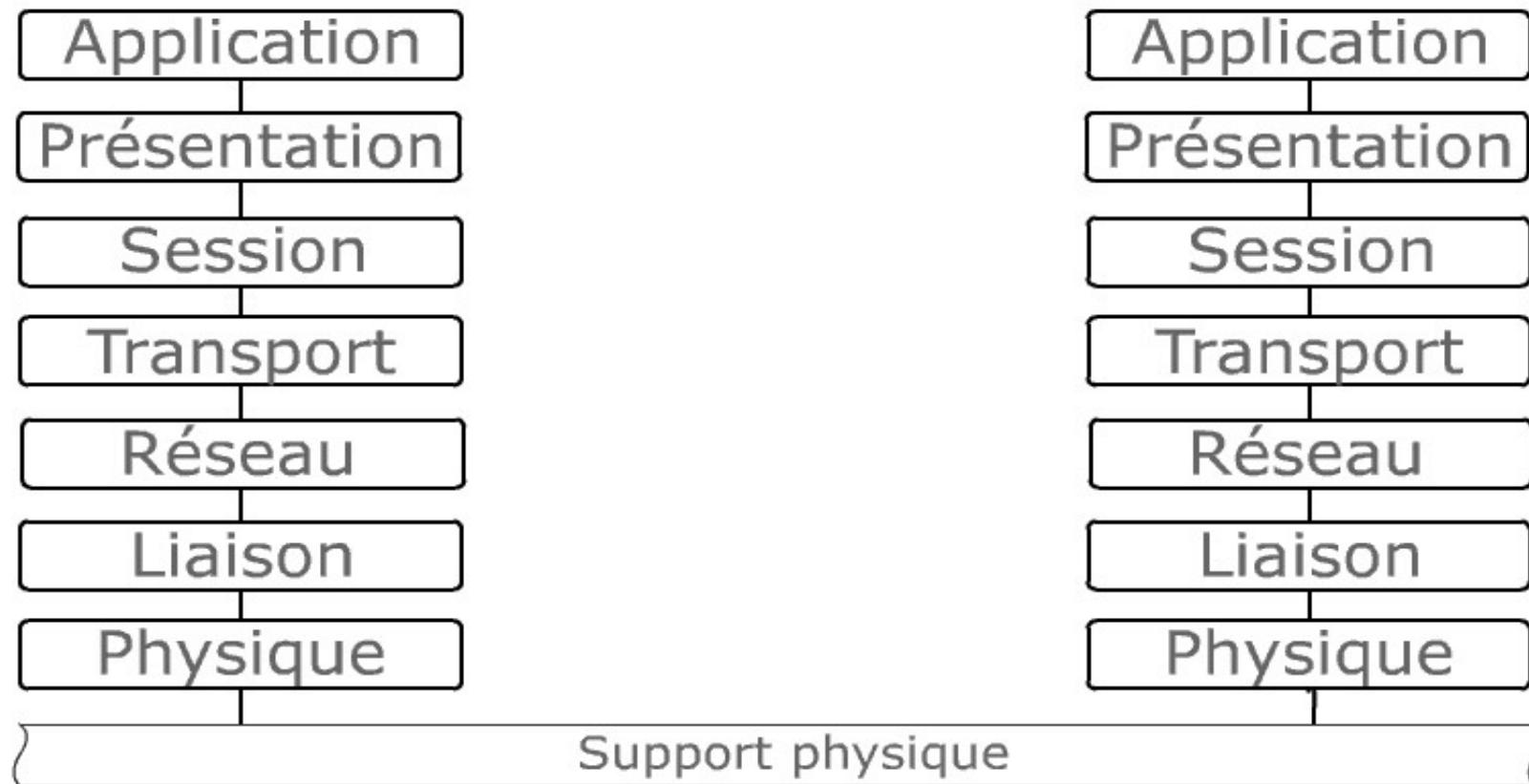


# Le modèle de référence OSI

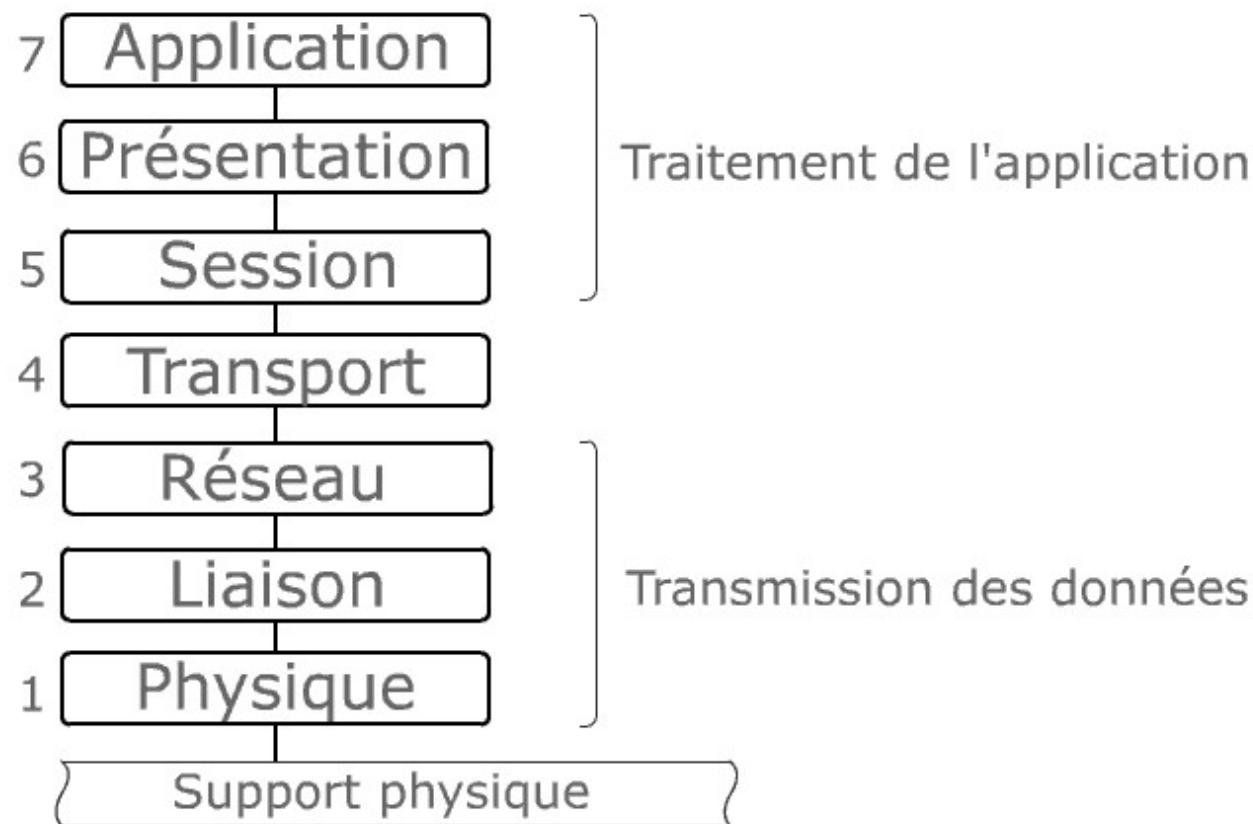
# Le modèle OSI

- *Open Systems Interconnection*  
= Interconnexion de Systèmes Ouverts
- Tentative de standardisation publiée en 1984 et revisité en 1995
- Réalisée par l'ISO  
*International Standards Organization*  
= Organisation Internationale de Normalisation
- C'est un modèle de référence en 7 couches

# Les 7 couches du modèle OSI



# Les 7 couches du modèle OSI



# Les couches...

Les données utilisateurs



# Les couches...

Les données utilisateurs



7 Application



Service

# Les couches...

Les données utilisateurs



7 Application



Service

6 Présentation



Forme

# Les couches...

Les données utilisateurs



7 Application



Service

6 Présentation



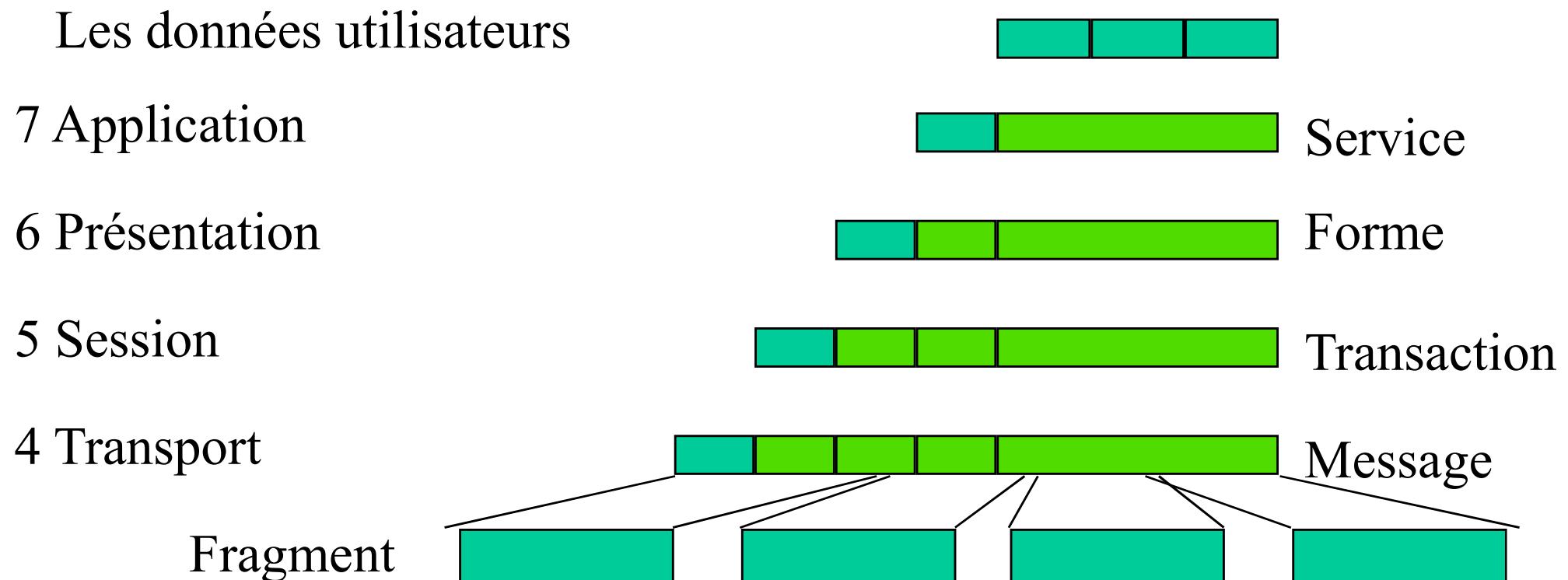
Forme

5 Session

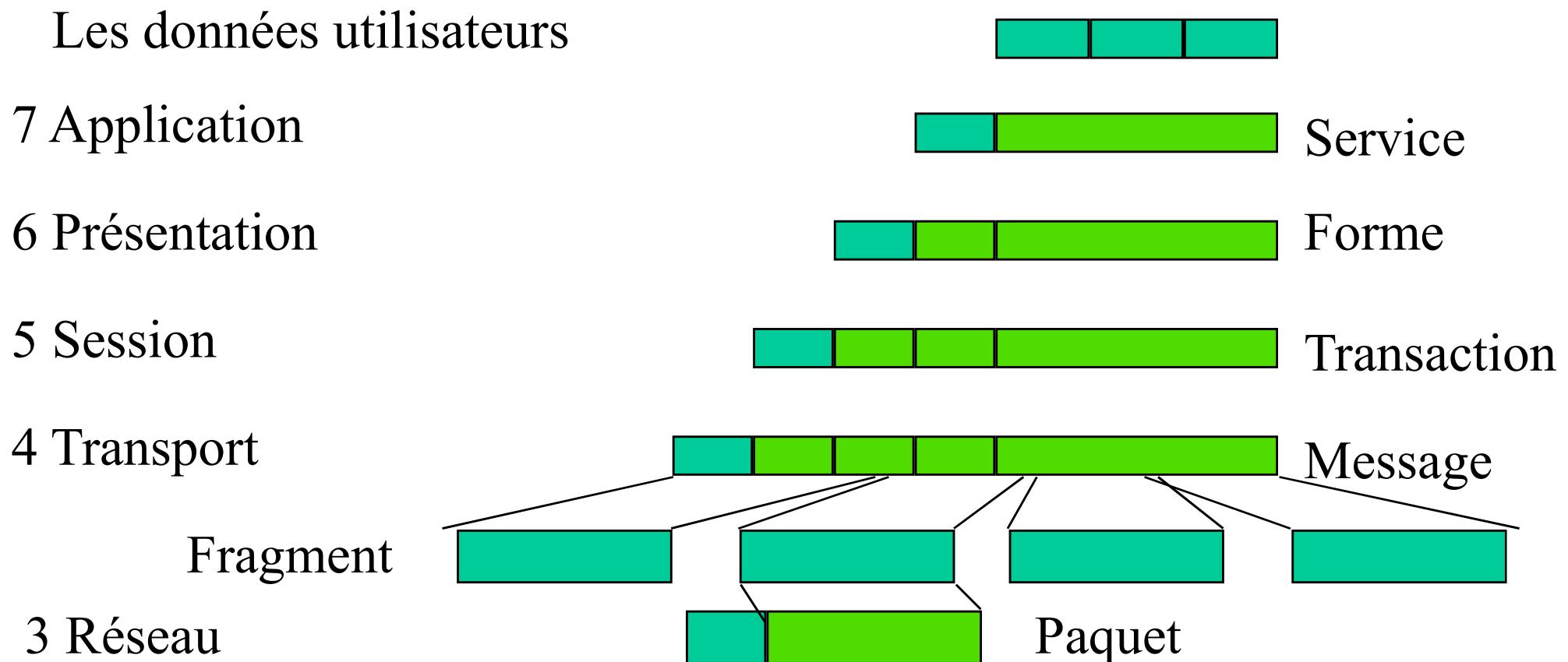


Transaction

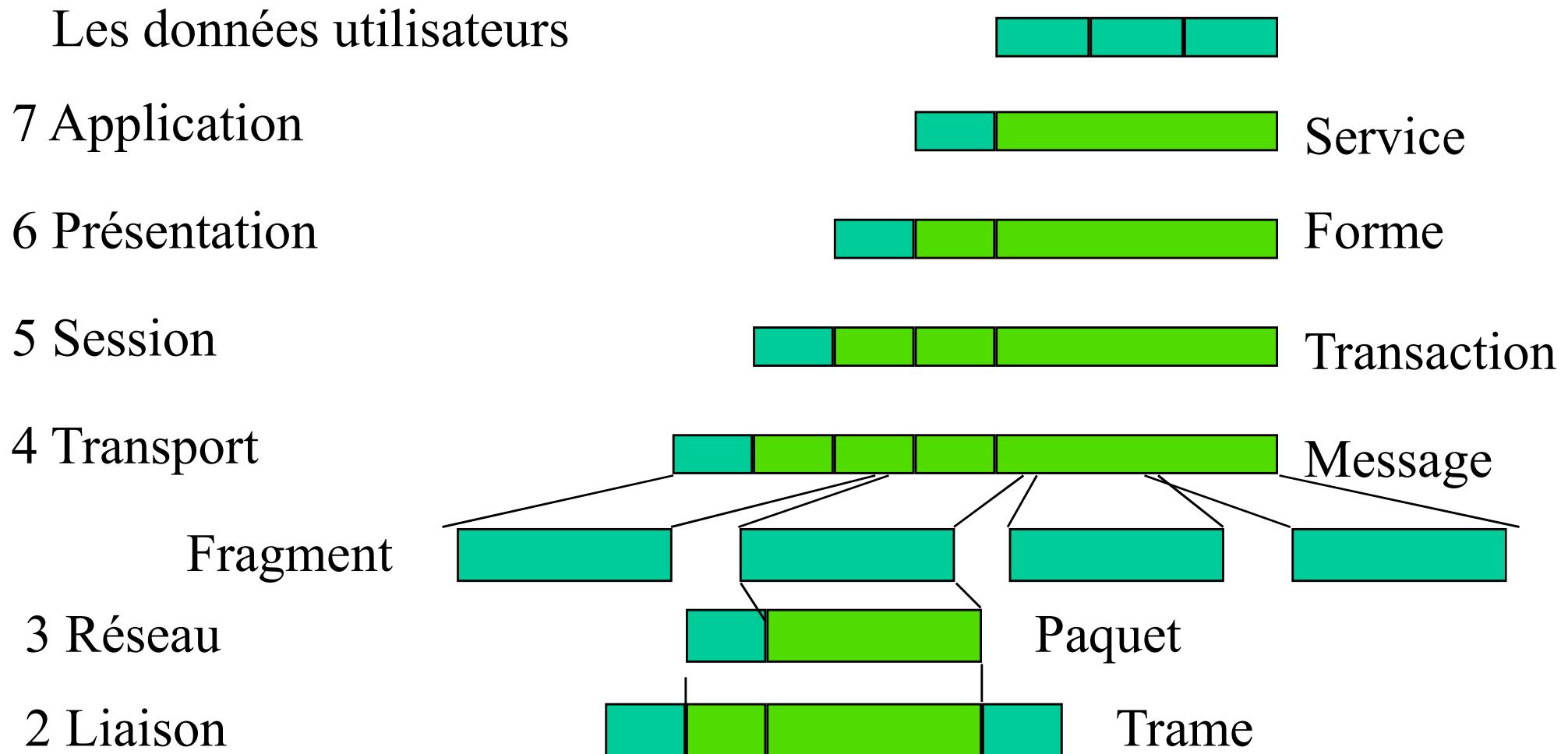
# Les couches...



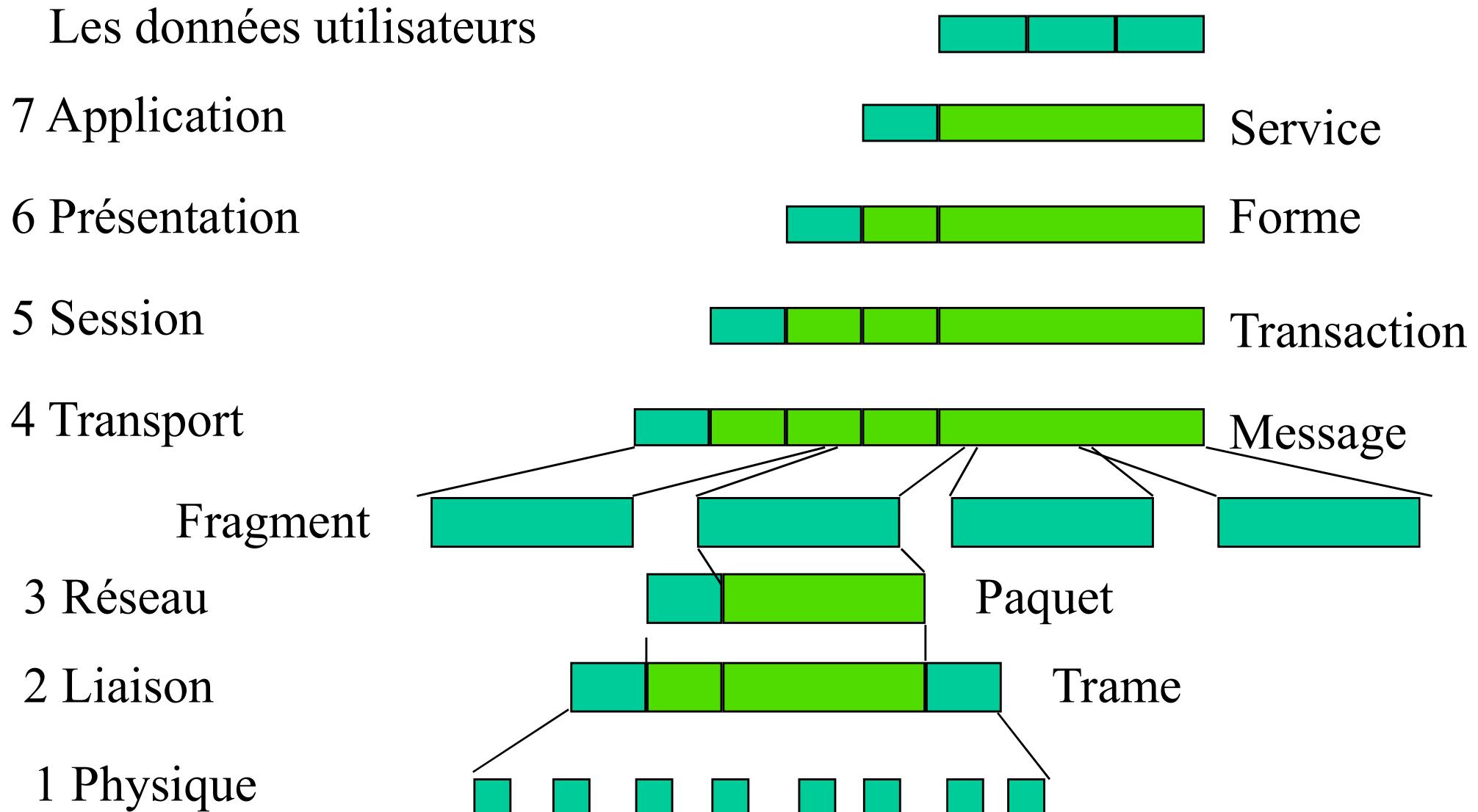
# Les couches...



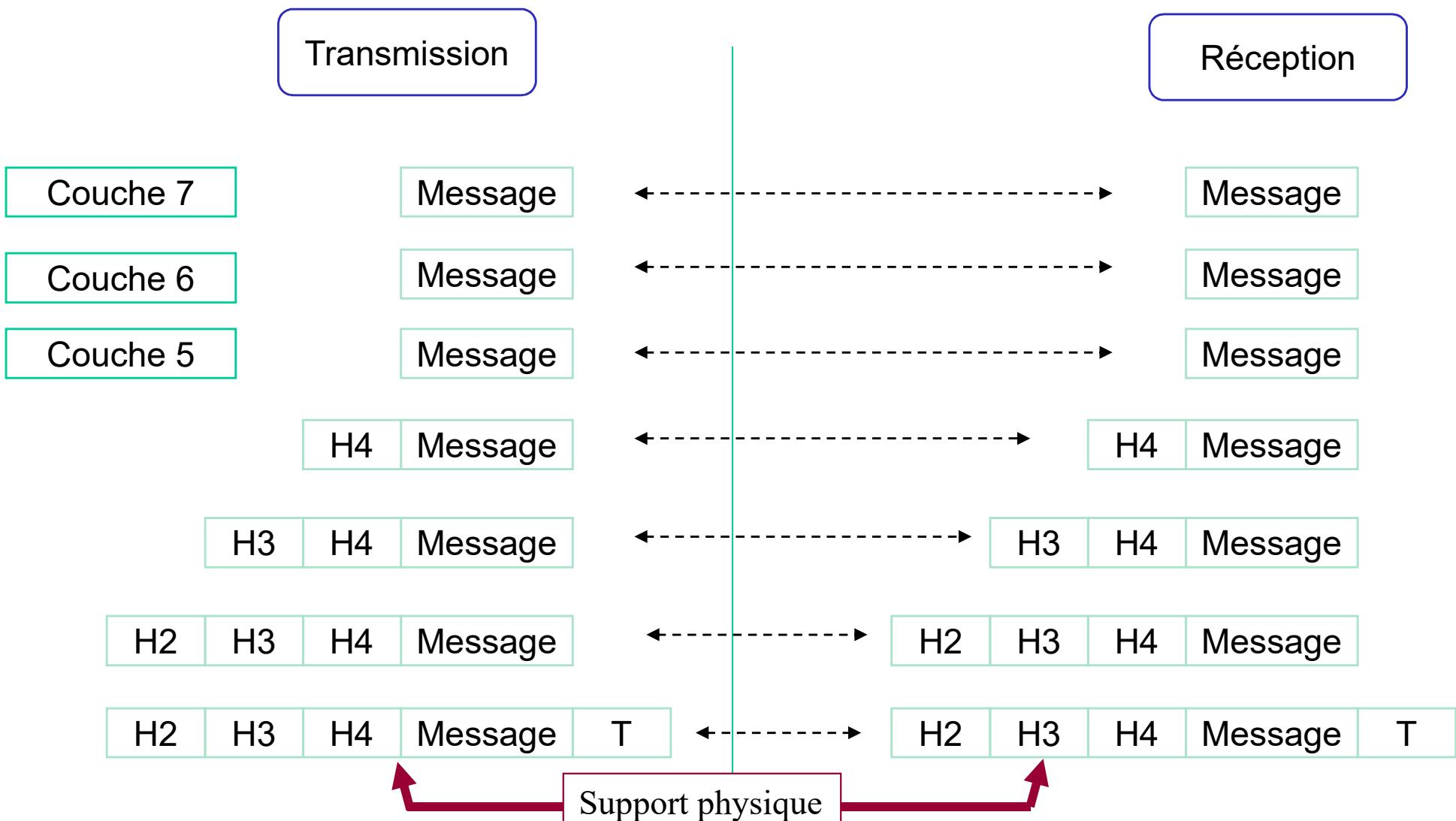
# Les couches...



# Les couches...

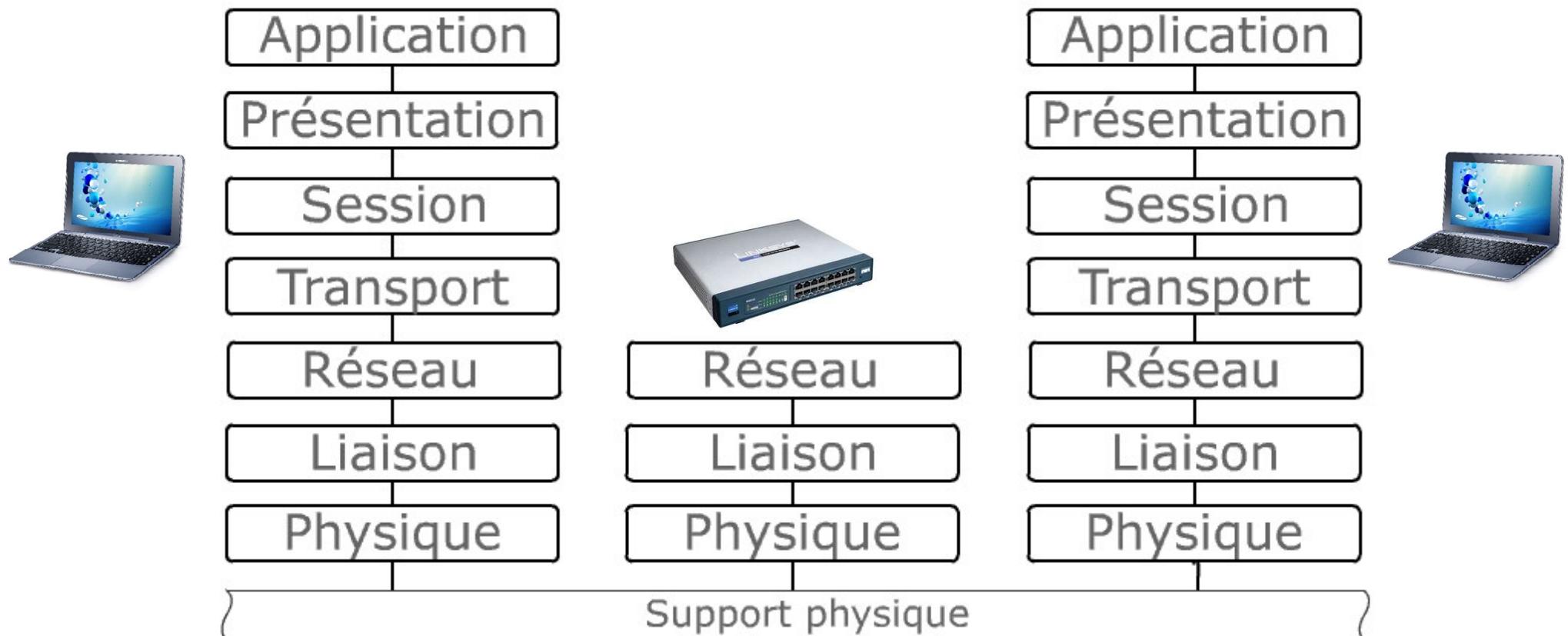


# Les 7 couches du modèle OSI

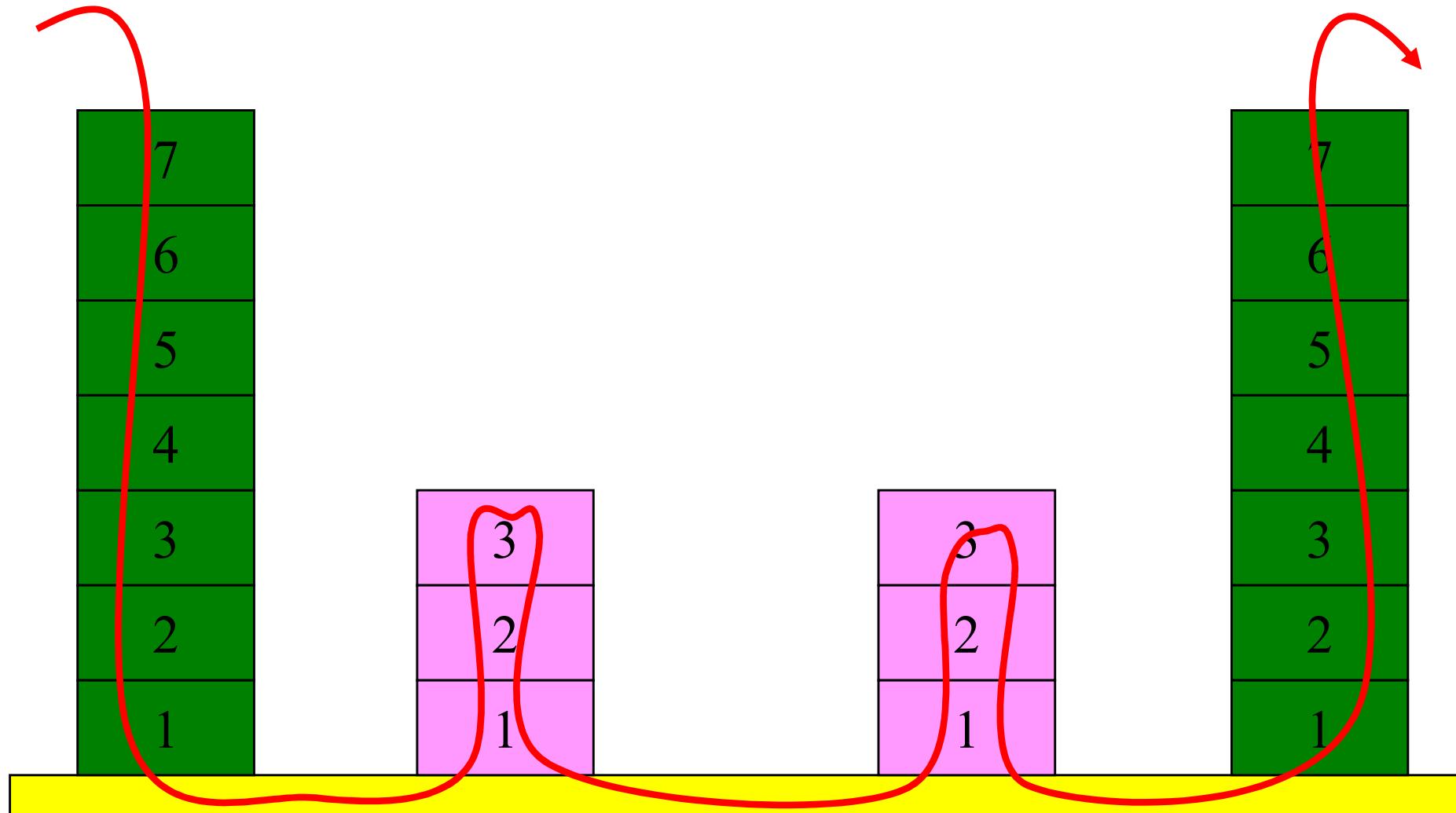


# Les 7 couches du modèle OSI

Communication **de proche en proche** pour les couches basses  
**de bout en bout** pour les 4 couches supérieures



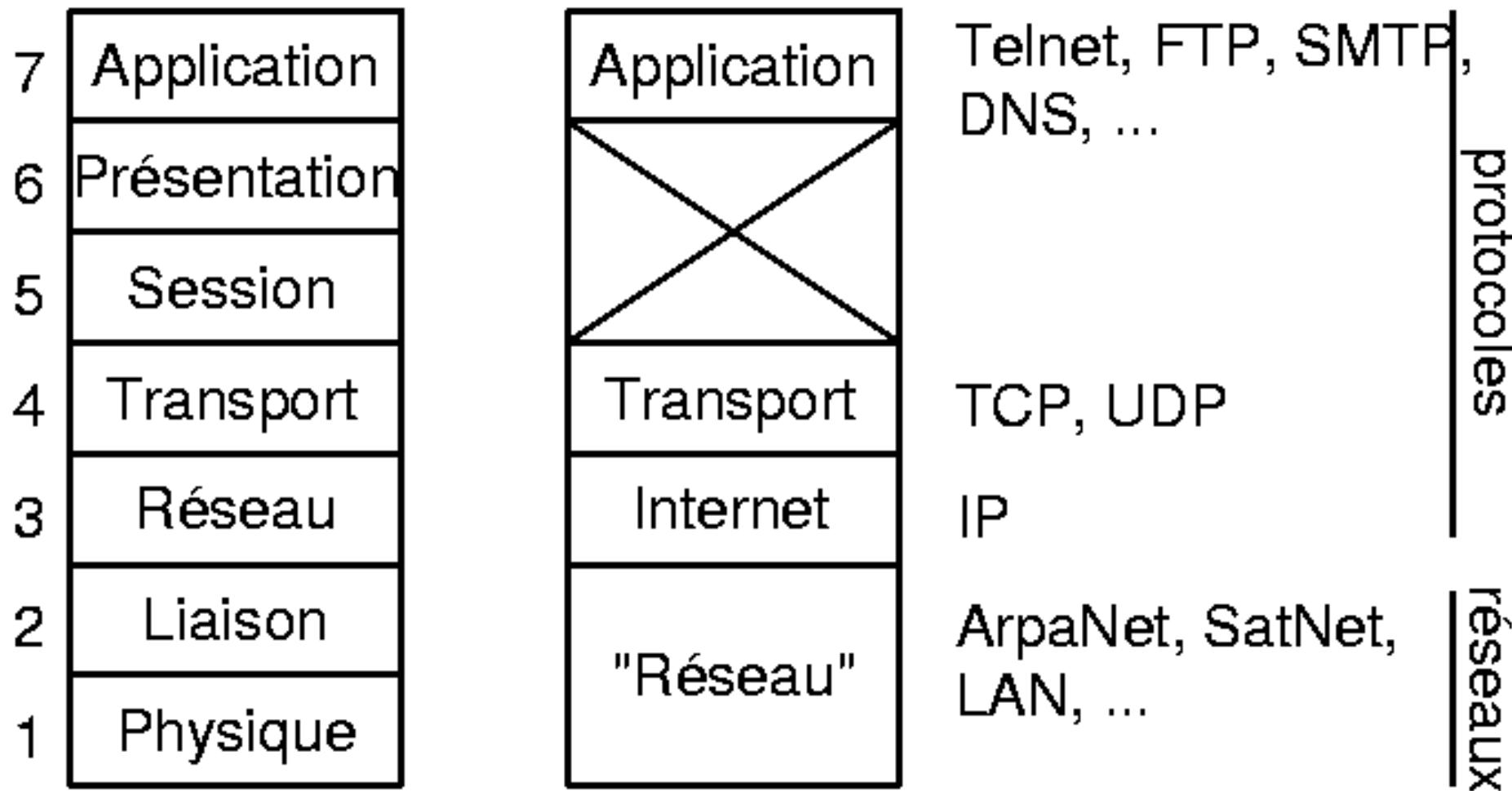
# Le découpage en couches OSI de la norme ISO



# Architecture

## TCP/IP

# Architecture de pile TCP/IP



Et protocoles de contrôle : ICMP, ARP, RARP, BOOTP.

# Et Internet dans tout ça ?

Internet est un ensemble de protocoles regroupés sous le terme "TCP-IP" (**T**ransmission **C**ontrol **P**rotocol/**I**nternet**P**rotocol).

Voici une liste non exhaustive des différents protocoles qui peuvent être utilisés :

- **HTTP:** (Hyper Texte Transfert Protocol): c'est celui que l'on utilise pour consulter les pages web.
- **FTP:** (File Transfert Protocol): C'est un protocole utilisé pour transférer des fichiers.
- **SMTP:** (Simple Mail Transfert Protocol): c'est le protocole utilisé pour envoyer des mails.
- **POP:** C'est le protocole utilisé pour recevoir des mails.
- **Telnet:** utilisé surtout pour commander des applications côté serveur en lignes de commande
- **IP** (internet Protocol): L'adresse IP vous attribue une adresse lors de votre connexion à un serveur.

# *Chapitre II*

# Normes et protocoles

## Chapitre II

### Normes associées à la diffusion analogique et Numérique

- NORMES AUDIO ET VIDÉO ANALOGIQUES (CCIR ET NTSC ...ETC)
- NORMES AUDIO ET VIDÉO NUMÉRIQUE (DVB, ATSC, ISDB, NICAM ...)

# Norme et standard vidéo

Une série de **normes et standards de télévision** a été développée pour simplifier l'industrialisation et la diffusion commerciale des téléviseurs puis des appareils vidéo et informatiques; ces accords internationaux définissent les spécifications de compatibilité entre les systèmes et équipements exploités.

# Norme et standard vidéo

- La **norme** concerne principalement le mode de télédiffusion. Elle définit le type de modulation.
- Le **standard** concerne le signal vidéo, lequel doit être modulé (émis) conformément à la norme. Il définit plus particulièrement le système couleurs.

# Technologie de transmission

Les standards vidéo se différencient notamment sur leur fréquence image (trames), laquelle a été déterminée conformément à celle des fréquence du réseau électrique nationaux, principalement pour minimiser certaines interférences et réduire les coûts de fabrication industrielle.

« La **vidéo** \* regroupe  
l'ensemble des techniques permettant  
l'**enregistrement** ainsi que la **restitution**  
**d'images animées**,  
accompagnées ou non de **son**,  
sur un **support électronique** et non photochimique. »

\* **vidéo**phonie ou **vidéogramme**, du **latin** «video» («je vois»)



## Film = succession d'images animées

Plus les images s'enchaînent vite, plus le film est **fluide**.

Normes héritées des **formats de diffusion** télévision :

25 images / seconde en **PAL/SECAM**

30 images / seconde en **NTSC**

(**fps**: frames per seconds)

Possibilité de recourir à d'autres fréquences d'enregistrement au détriment de la fluidité (ex : **films d'animation, webcams**).

# Formats et standards vidéo

Standards d'enregistrement vidéo	Analogique	Numériques
PAL	VHS	Digital 8
SECAM	VHS-C	DV ou Digital Video
NTSC	S-VHS	DVCAM
HD TV	8mm ou Video 8	Betacam SX
MAC	Hi-8	Digital-S
	Betacam / Betacam SP	IMX
	U-matic / U-MATIC SP	XDCAM
	Betamax	DVCPRO
	V2000	Betacam numérique
	Bande 1 pouce	HDV
	Bande 2 pouces	XDCAM HD
	BVU / BVU SP	DVCPRO-HD
		HDCam
		DVD
		AVCHD
		D1
		HDCAM SR

# Standards d'enregistrement vidéo

# NTSC : National Television System Committee

Développé aux États-Unis, il est le premier standard de télévision national en couleurs commercialisé. Les retransmissions publiques débutent officiellement en 1954 (téléviseur couleurs mécaniques de type RCA).



# NTSC : National Television System Committee

lignes/nombre de trames	525/60
fréquence horizontale	15.734 kHz
fréquence verticale	60 Hz
fréquence porteuse couleur	3.579545 MHz
largeur de bande vidéo	4.2 MHz
porteuse audio	4.5 MHz (FM)

## PAL : Phase Alternation Line

Développé en Allemagne, il exploite plusieurs brevets du NTSC, dont il réduit la distorsion de phase des couleurs. Les retransmissions commencent en 1967.

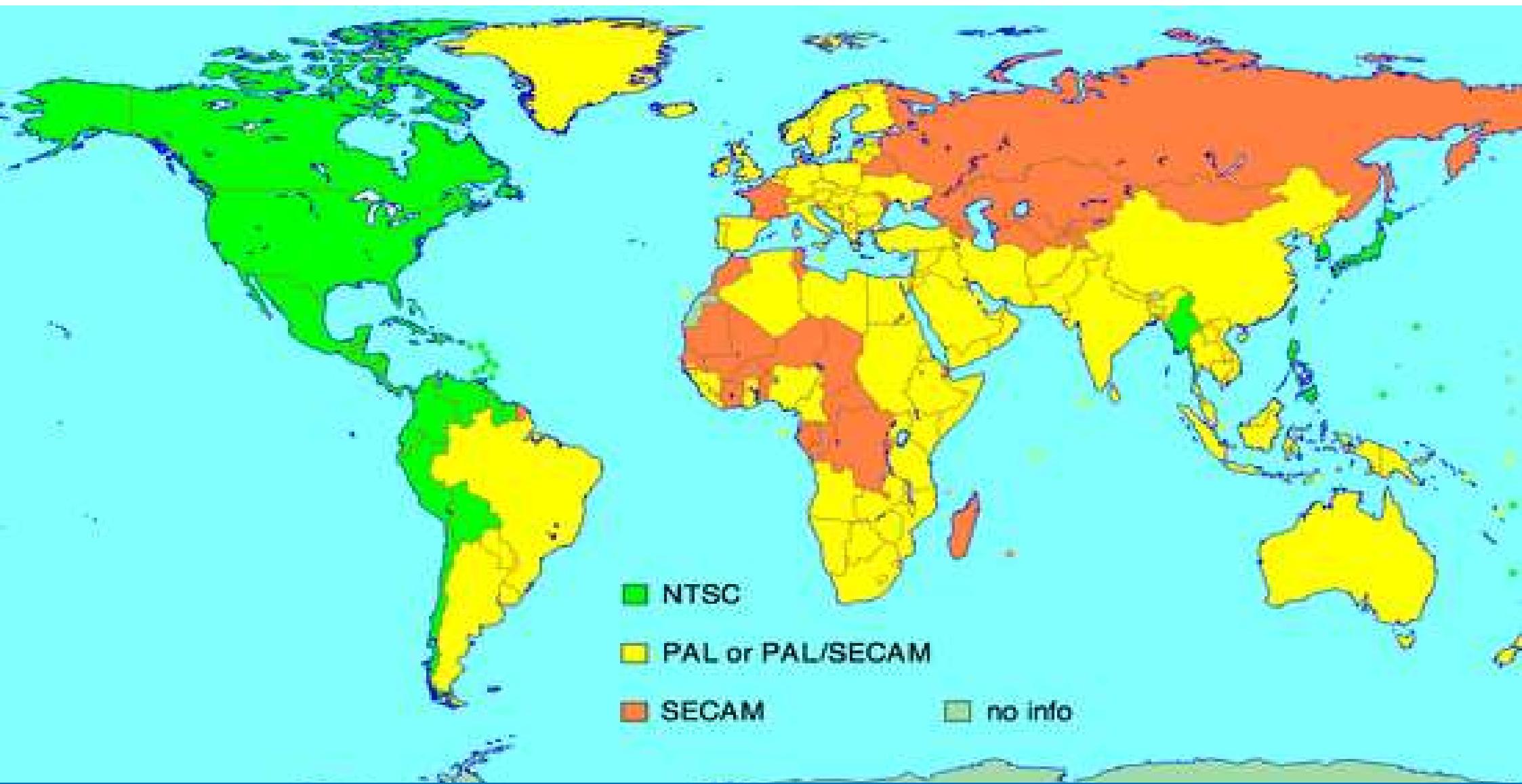
# PAL : Phase Alternation Line

PAL B-G-H	PAL I	PAL D	PAL N	PAL M	
lignes/ trames	625/ 50	625/ 50	625/ 50	625/ 50	525/ 60
fréquence horizontale	15.625 kHz	15.625 kHz	15.625 kHz	15.625 kHz	15.734 kHz
fréquence verticale	50 Hz	50 Hz	50 Hz	50 Hz	60 Hz
fréquence porteuse vidéo couleurs	4.433618 MHz	4.433618 MHz	4.433618 MHz	3.582056 MHz	3.575611 MHz
largeur de bande vidéo	5.0 MHz	5.5 MHz	6.0 MHz	4.2 MHz	4.2 MHz.
porteuse audio	5.5 MHz (FM)	6.0 MHz	6.5 MHz	4.5 MHz	4.5 MHz

# SÉCAM : Séquentiel couleur à mémoire

Développé en France. Début de la diffusion commerciale en 1967.

	SECAM B-G-H	SECAM D	SECAM K-K1	SECAM L
lignes/nombre de trames	625/50	625/50	625/50	625/50
fréquence horizontale	15.625 kHz.	15.625 kHz.	15.625 kHz.	15.625 kHz.
fréquence verticale	50 Hz	50 Hz	50 Hz	50 Hz
largeur de bande vidéo	5.0 MHz	6.0 MHz	6.0 MHz	6.0 MHz
porteuse audio	5.5 MHz (FM)	6.5 MHz (FM)	6.5 MHz (FM)	6.5 MHz (AM)



Distribution géographique

1,33:1  
(4/3)

1,66:1

1,77:1  
(16/9)

1,85:1

2,35:1  
(Cinémascope)

2,55:1  
(Cinémascope original)

**Résolution** = Largeur x Hauteur de l'image  
(en pixels)

→ **Qualité** de l'image

(plus de précision = plus de netteté)

→ **Poids** du fichier

(plus d'informations = fichier plus « lourd »)

→ **Aspect (Ratio largeur/hauteur) de l'image:**

. 1,33:1 (**4/3**) ex: 720x480 (NTSC), 768x576 (PAL/SECAM),  
800x600, 2048x1536

. 1,78:1 (**16/9**) ex: 1280x720 («720»), 1920x1080 («1080»)

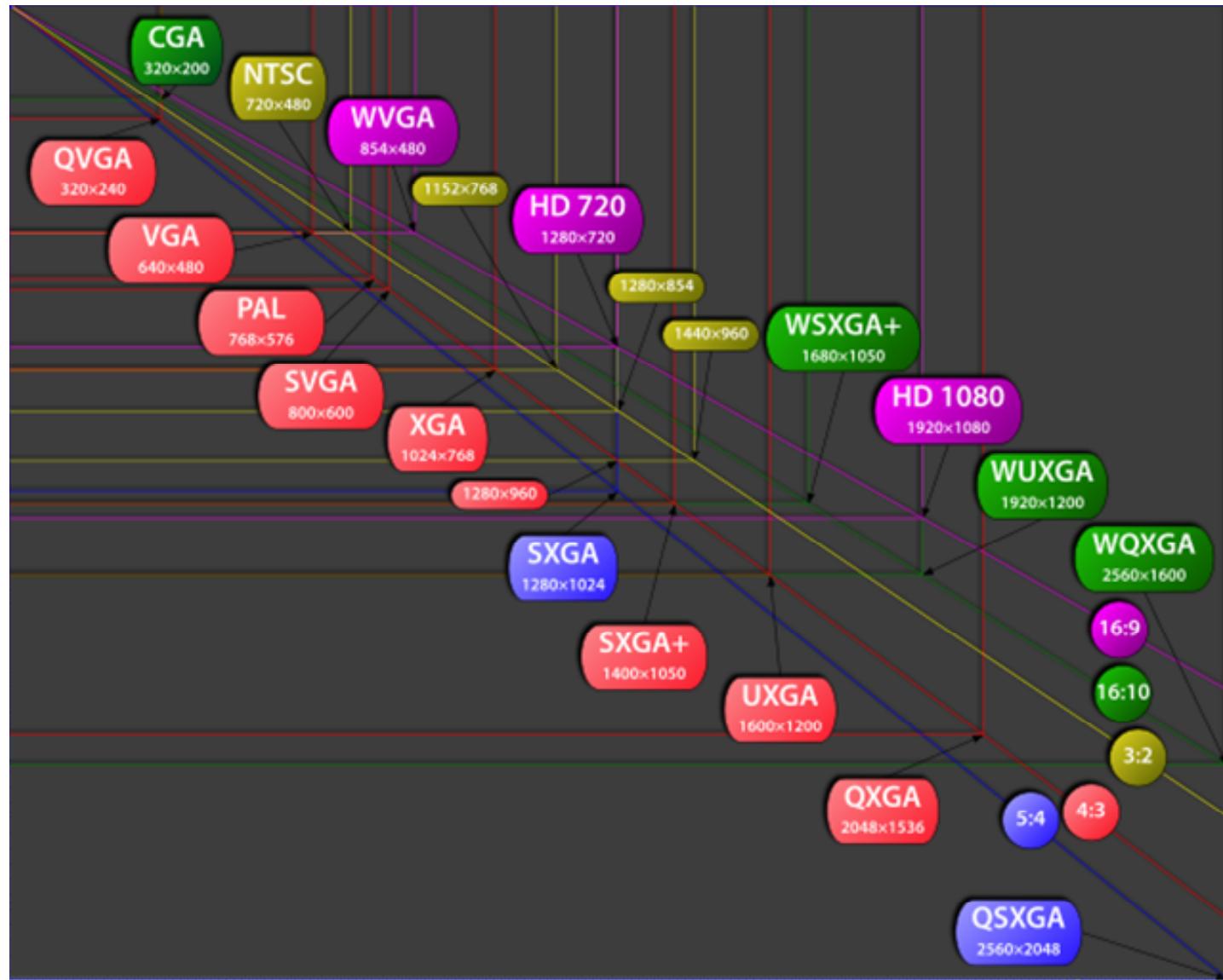
. 2,35:1 (**Cinemascope**)

**Haute-Définition:** Téléviseur **HD Ready**: peut afficher HD 720 // **Full HD**: peut afficher HD 1080

720i → affichage **entrelacé** (*interlace*): écrans **cathodiques** // 1080p → affichage progressif: écrans **LCD**

# Cadrage vidéo

Standard	Images par seconde
NTSC	29,97
PAL/SECAM	25
Cinéma	24 ou 25



# Normes audio et vidéo analogiques

# VHS (Video Home System)

système vidéo domestique, mieux connue sous le sigle **VHS**, désigne une norme d'enregistrement de signaux vidéos sur bande magnétique de 1/2 pouce mis au point par la marque japonaise JVC à la fin des années 1970.



## Video 8 (8mm)

- Le format ***Video 8***, ***V8*** ou encore ***8mm*** est développé par le japonais Sony en 1985 ainsi que plusieurs autres marques.



# Betamax

**Betamax** est un format de cassette à ruban vidéo de 1/2 pouce, soit 12,7 mm. Format créé par Sony en 1975, il est destiné aux enregistrements de télévision grand public.



# Normes audio et vidéo numériques

# Digital Video

- Le format **Digital Video**, ou **DV**, est un format vidéo qui date de 1996 et qui permet d'enregistrer des vidéos sur des cassettes en numérique avec une relativement faible compression pour chaque image.
- Ceci facilite le transfert direct de la vidéo vers un ordinateur.

# DVCAM

- Le **DVCAM** est un format vidéo numérique de la firme Sony. Il s'agit de la version « professionnelle » du Digital Video (DV).

# Digital8

Le **Digital8 - D8** est un format vidéo numérique grand public de Sony, exploitant un signal vidéo DV et le format de vidéocassettes 8mm et Hi-8.

# Digital-S

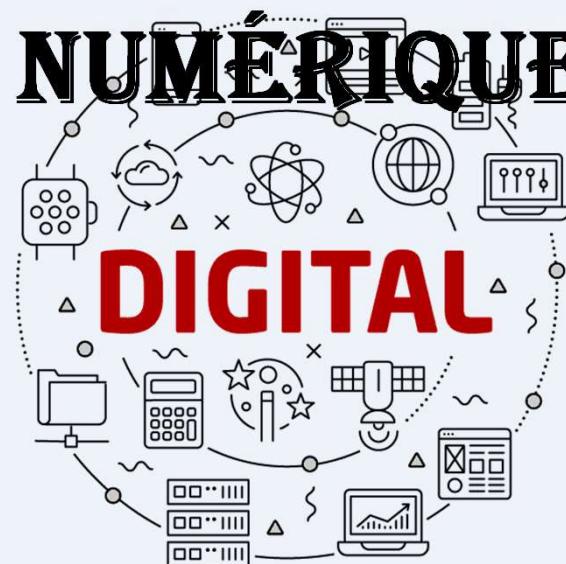
- Le **Digital-S** ou **D9** est un format vidéo présenté par JVC en 1995, pour concurrencer le format Betacam numérique de Sony. Enregistré sur une bande magnétique « métal particule » de 1/2 pouce de large

# *Chapitre III*

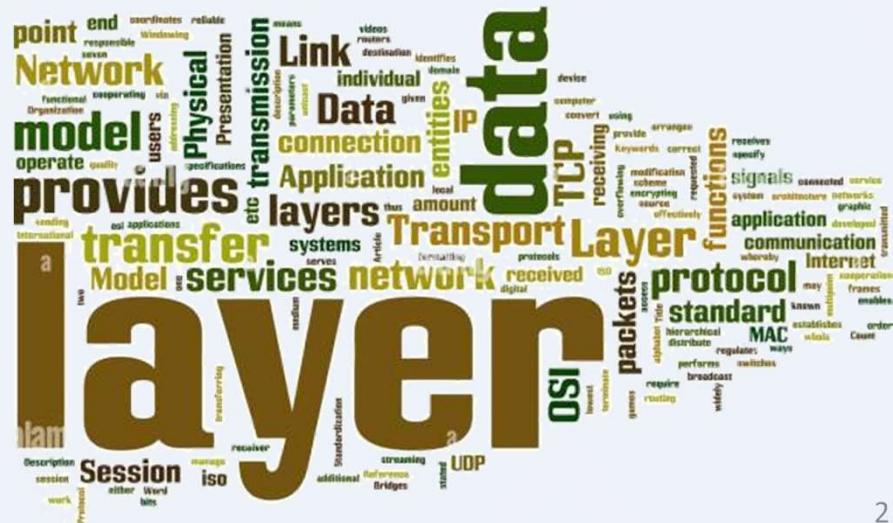
# Normes et Protocoles

## CHAPITRE 03

### NORMES ASSOCIÉES AUX RÉSEAUX DE COMMUNICATION NUMÉRIQUE



# Rappels sur les modèles OSI et TCP/IP



## Protocoles Propriétaires

- Les constructeurs informatiques ont proposé des architectures réseaux propres à leurs équipements. Par exemple :
  - ✓ IBM a proposé SNA (System Network Architecture)
  - ✓ DEC a proposé DNA (Digital Network Architecture)
- Ces architectures ont toutes le même défaut : du fait de leur caractère propriétaire, il n'est pas facile des les interconnecter, à moins d'un accord entre constructeurs.
- Il faut trouver une norme permettant à différents systèmes informatiques de communiquer entre eux...

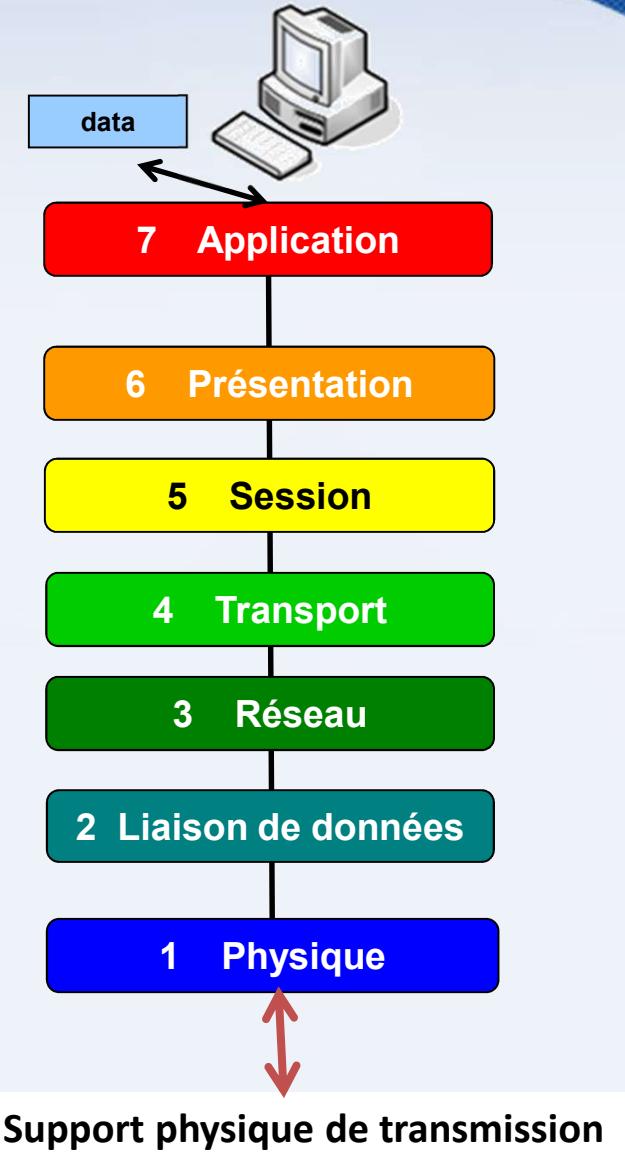
## Standardisation et modélisation des réseaux

- La modélisation des réseaux permet de comparer les différents protocoles entre eux en plaçant des points de repère et une séparation claire des différentes tâches présentent lors d'une communication.
- Cette séparation en tâche, appelées couches, permet également d'obtenir une modularité importante, qui a permis le développement rapide des réseaux et leur inter-opérabilité.
- Il existe deux principaux modèles :
  - Le modèle OSI: *Open Systems Interconnection*,
  - Le modèle Internet TCP/IP ...

# Le Modèle OSI

Le modèle OSI a été proposé en 1977 par l'*International Organization for Standardization*. Dans ce modèle, un système en réseau utilise une pile constituée de **7 couches**. Le modèle OSI a été créé pour la standardisation des divers protocoles employés dans les réseaux d'ordinateurs "ouverts".

Ce modèle d'organisation est un **modèle de référence** "papier" et ne correspond pas réellement à une technologie réseau "réelle".



# Le Modèle OSI (2)

La couche **Application** : gère les échanges entre les programmes et les Utilisateurs (service de SGDB, d'impression, navigation Internet...)

La couche **Présentation** : met en forme les informations de telle sorte qu'elles soient exploitable par les applications logicielles.( cryptage, compression)

La couche **Session** : gère la communication entre les ordinateurs (identification, test de connexion)

La couche **Transport** : Décompose l'information en paquets numérotés (segments) et vérifie l'acheminement des informations vers le destinataire (erreurs, réexpédition)

La couche **Réseau** : identifie les ordinateurs connectés et détermine l'acheminement des données (adresses, routes).

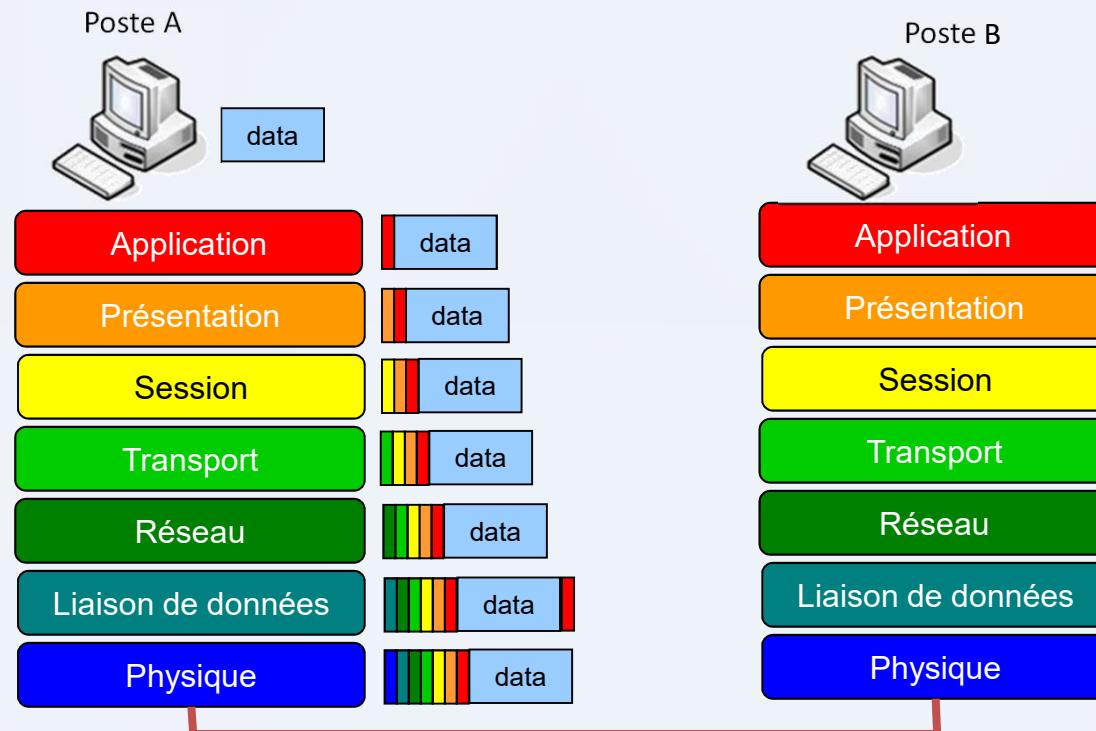
La couche **Liaison de Données** : assure que les données (trames) sont correctement véhiculés par le media physique (méthode d'accès, correction d'erreurs de transmission)

La couche **Physique** : gère la transmission de bits (0,1) sur le média utilisé (support physique, vitesse de transmission)



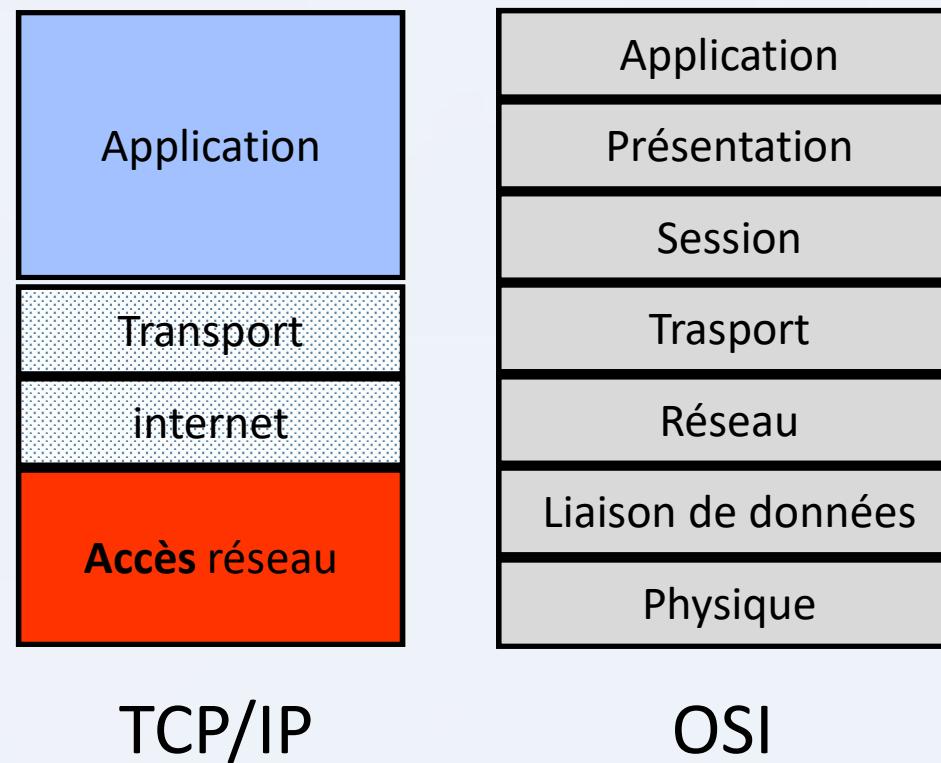
# Le Modèle OSI (notion d'encapsulation)

Chaque couche a un rôle unique et indépendant dans le transfert d'une information :



# Le modèle Internet TCP/IP

Modèle plus simple (en nombre de couches) que le modèle OSI.  
C'est le modèle de référence pour les applications sur Internet.



# Le modèle Internet TCP/IP

**Couche Application :** Elle est la couche de communication qui s'interface avec les utilisateurs. Exemples de protocoles : HTTP, DNS, SMTP , FTP, ...

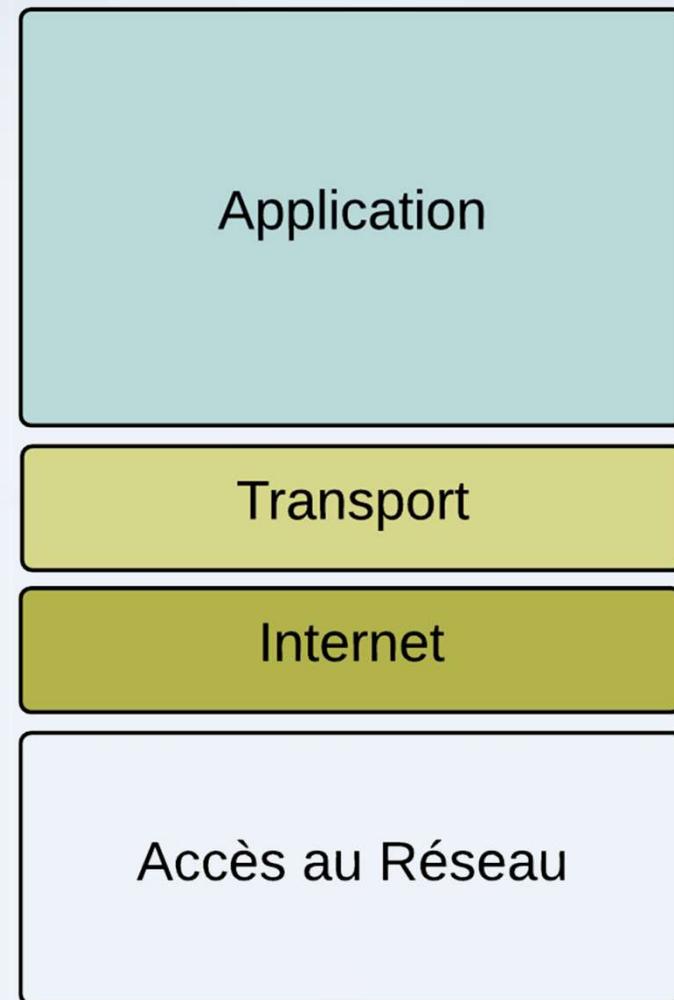
**Couche Transport :** TCP Elle est responsable du dialogue entre les hôtes terminaux d'une communication.

Les applications utiliseront TCP pour un transport fiable et UDP sans ce service.

**Couche Internet :** IP Elle permet de déterminer les meilleurs chemins à travers les réseaux en fonction des adresses IPv4 ou IPv6.

**Couche Accès Réseau :** Au sens du modèle TCP/IP est vide, car la pile des protocoles Internet (TCP/IP) est censée "inter-opérer" avec les différentes technologies qui offrent un accès au réseau...

## Modèle TCP/IP



# Le modèle Internet TCP/IP

Couche	Identifiant	Exemple
Couche Application	Un protocole et un nom de domaine	<b>http:// www.cisco.com</b>
Couche Transport	Port TCP ou UDP	<b>80</b> comme port par défaut pour HTTP
Couche Internet	Adresse IPv4 et/ou IPv6	<b>192.168.150.252/24</b> ou <b>2001:db8::1/64</b>
Couche Accès	adresse physique (MAC 802)	<b>70:56:81:bf:7c:37</b>

# Tableau de synthèse

TCP/IP	OSI	Rôles	PDU	Protocoles	Matériel
Application	7 Application	Services au plus proche des utilisateurs	Données	HTTP, DNS, DHCP	Ordinateurs
Application	6 Présentation	encode, chiffre, compresse les données utiles	<i>Idem</i>	<i>idem</i>	<i>Idem</i>
Application	5 Session	établit des sessions entre des applications	<i>Idem</i>	<i>idem</i>	<i>Idem</i>
Transport	4 Transport	établit, maintient, termine des sessions entre des hôtes d'extrémité.	Segment	TCP ou UDP	Ordinateurs, routeurs NAT, pare-feux
Internet	3 Réseau	Identifie les hôtes et assure leur connectivité	Datagramme ou paquet	IPv4 ou IPv6	Routeurs

# Tableau de synthèse

Accès Réseau	2 Liaison de Données	Détermine la méthode d'accès au support, organise les bits de données	Trame	Ethernet IEEE 802.3, Wi-Fi IEEE 802.11, pontage 802.1	Commutateurs , cartes d'interface réseau
Accès Réseau	1 Physique	s'occupe du placement physique du signal	bits	Normes physiques : xDSL (WAN), 1000-BASE-TX	Câblage (UTP CAT 6) et connecteurs (RJ-45), bande fréquences (2.4 GHz, 5 GHz)

...

# Les technologies xDSL



## La technologie DSL

- La ligne d'abonné numérique (DSL, *Digital Subscriber Line*) est une technologie d'accès à large bande qui permet des transmissions de données à haut débit sur les fils téléphoniques en cuivre existants (paires torsadées)
- Ces lignes téléphoniques sont déjà installées dans la plupart des bâtiments, ce qui ne nécessite aucun travail particulier, donc aucun frais de ce point de vue pour l'utilisateur .
- la technologie DSL est capable d'atteindre des débits de transmission de données jusqu'à 52 Mb/s en utilisant des technologies de modulation de signal avancées,
- L'intervalle de fréquence du canal est allant de 25 kHz à une limite supérieure.

## La technologie DSL

Le terme xDSL regroupe l'ensemble des technologies mises en place pour ce type de transport numérique de l'information. Ces technologies sont différenciées par :

- La manière de l'exploitation de la bande passante
- La vitesse de transmission
- La distance maximale de transmission
- La variation de débit entre le flux montant et le flux descendant
- Le caractère symétrique ou non de la liaison

# Types de technologies xDSL

En gros, les normes xDSL peuvent être divisées en trois groupes:

- 1. DSL Symétrique:** fournit le même débit de données pour les transmissions en amont et en aval, il comprend les types suivants:

DSL Variant	Débit montant/descendant	Distance max
HDSL - <b>High data rate</b> DSL	1.5Mbps/1.5Mbps	3.7 km
SDSL - <b>Symmetric</b> DSL	2.3Mbps/2.3Mbps	3 km
SHDSL - <b>Symmetric High bit rate</b> DSL	4.6Mbps/4.6Mbps	5 km

## Types de technologies xDSL

**2. DSL asymétrique:** Fournit des taux de transmission de données en aval, plus élevé, et en amont, comprend les types suivants:

DSL Variant	Débit montant/descendant	Distance max
ADSL, <b>Asymmetric</b> DSL	1Mbps/10Mbps	5.5km
ADSL Lite	384Kbps/1.5Mbps	5.5km
ADSL 2 -	1Mbps/12Mbps	5.5km
ADSL 2+	1Mbps/20Mbps	5.5km

## Types de technologies xDSL

**3. DSL symétrique et asymétrique:** peut transmettre des données à la fois symétriquement et asymétriquement et comprend les types suivants:

DSL Variant	Débit montant/descendant	Distance max
VDSL, Very High bit rate DSL	10Mbps/10Mbps; 1.5Mbps/52Mbps	0.3km -1.3km
VDSL 2 , Very High bit rate DSL	100Mbps/ 100Mbps	0.5 km

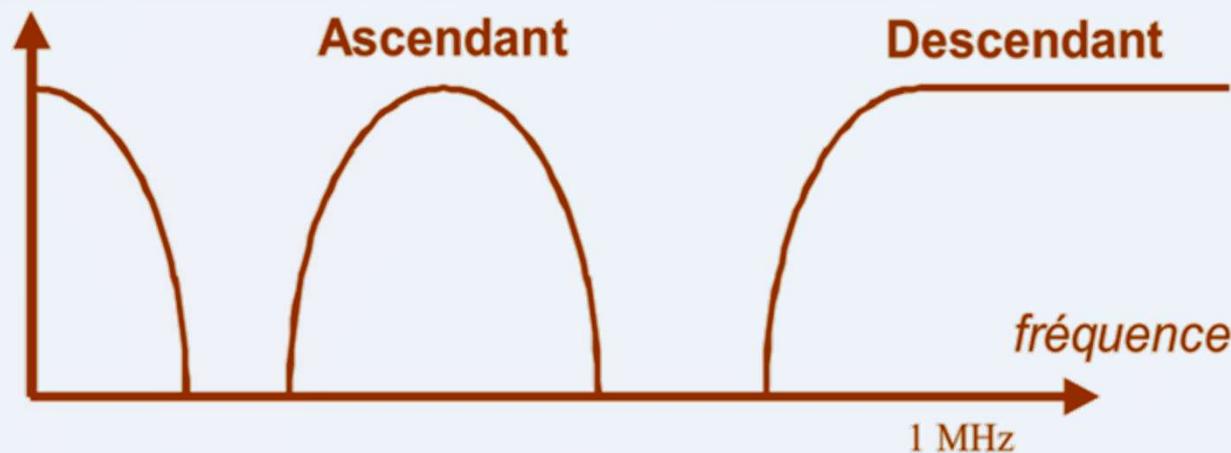
- Les données fournies dans ces tableaux sont théoriques et peuvent donc, dans la pratique, varier sensiblement,
- Les variantes ADSL sont les implémentations DSL les plus populaires, principalement en raison de leur adéquation aux applications de navigation Internet qui sont fortement axées sur la transmission de données en aval (téléchargement)...

## La technologie ADSL

- *Asymmetric DSL*, c'est la première version déployée dans le début des années 2000, elle offre un assez bon compromis entre les performances et le coût, et elle est bien adaptée à une clientèle grand public.
- Il utilise le multiplexage en *FDM (Frequency Division Multiplexing)*,
- Il est basée sur une modulation *DMT (Discrete Multi Tone)* utilisant 256 sous-canaux, modulés indépendamment en *QAM (Quadrature Amplitude Modulation)* pour accélérer le débit
- et avec une bande passante de 1,1 MHz.

## Multiplexage en fréquence (FDM)

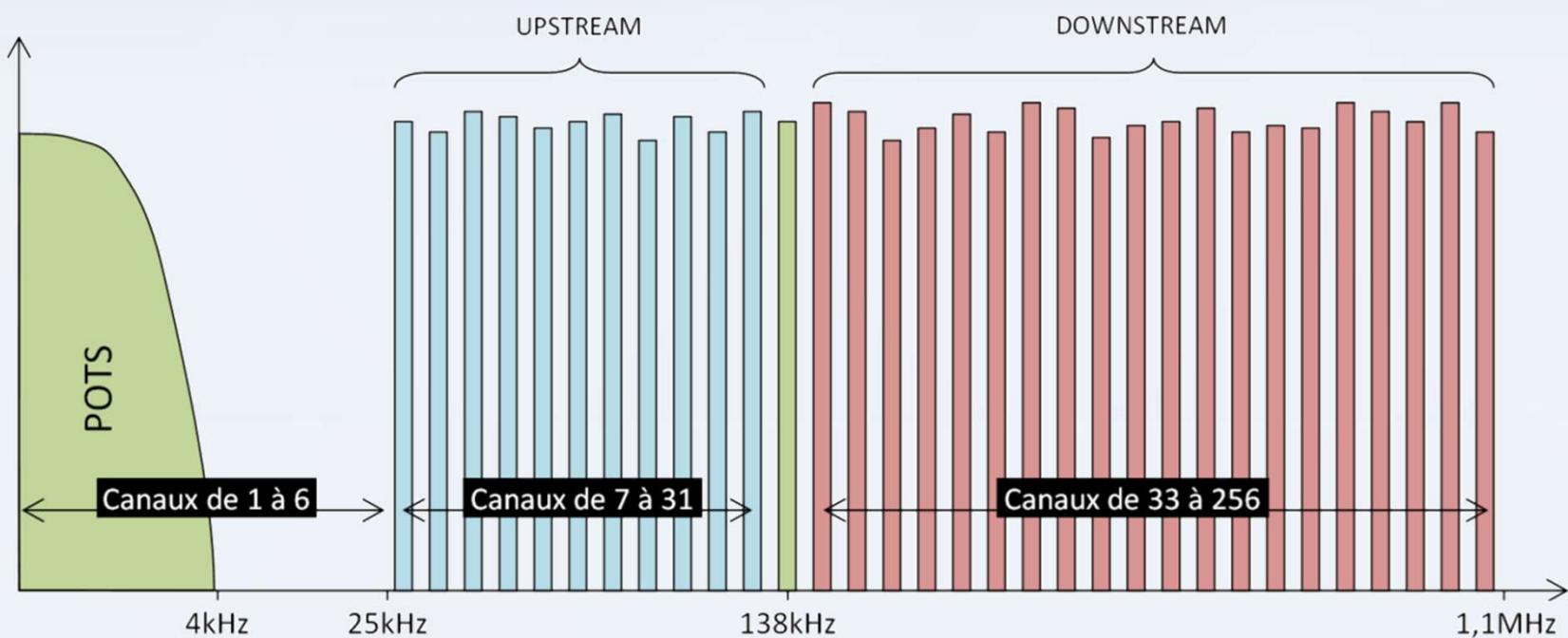
- L'ADSL fonctionne en full duplex grâce à FDM, permettant de faire transiter simultanément et séparément les signaux montants et descendants accompagnés également des signaux portant la voix téléphonique.
- Les bandes [25 kHz, 140 kHz] et [150 kHz, 1 100 kHz] sont respectivement utilisées pour les flux de données montants et descendants.



## Modulation DMT (*Discret Multi Tone*)

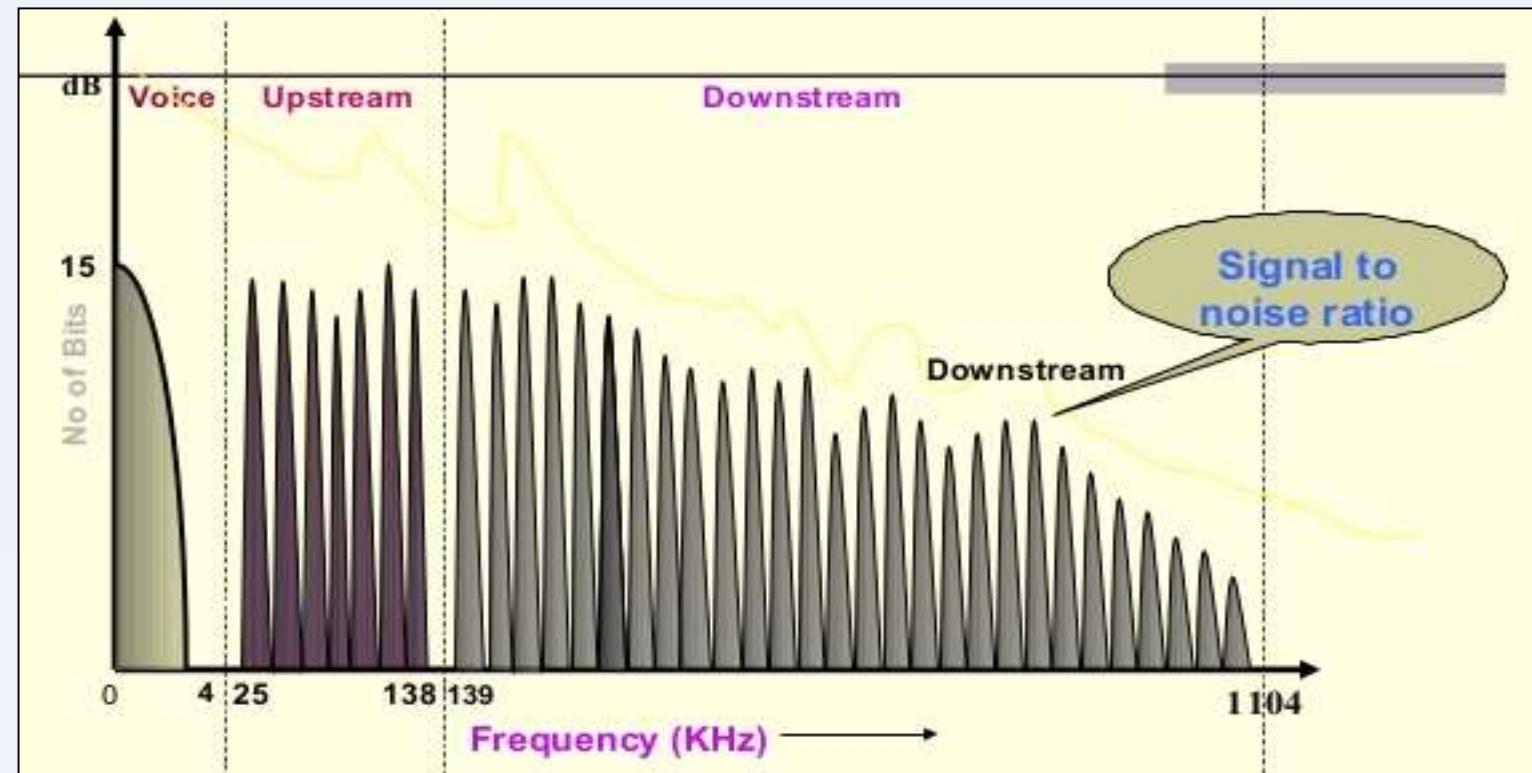
- Le principe de cette technique de modulation repose sur l'utilisation d'un grand nombre de sous-porteuses réparties sur la bande de fréquence utilisée par le système.
- Pour son application à l'ADSL, le spectre de fréquence compris entre 0 Hz et 1,104 MHz est divisé en 256 sous-canaux distincts espacés de 4,3125 kHz, et de largeur de 4KHz.
  - Les sous-canaux 1 à 6 sont utilisés pour la téléphonie,
  - les sous-canaux 7 à 31 pour le flux montant,
  - le sous-canal 32 est réservé,
  - les sous-canaux 33 à 256 sont utilisés pour les flux descendant.

# Modulation DMT (*Discret Multi Tone*)



# Modulation des sous-porteuse

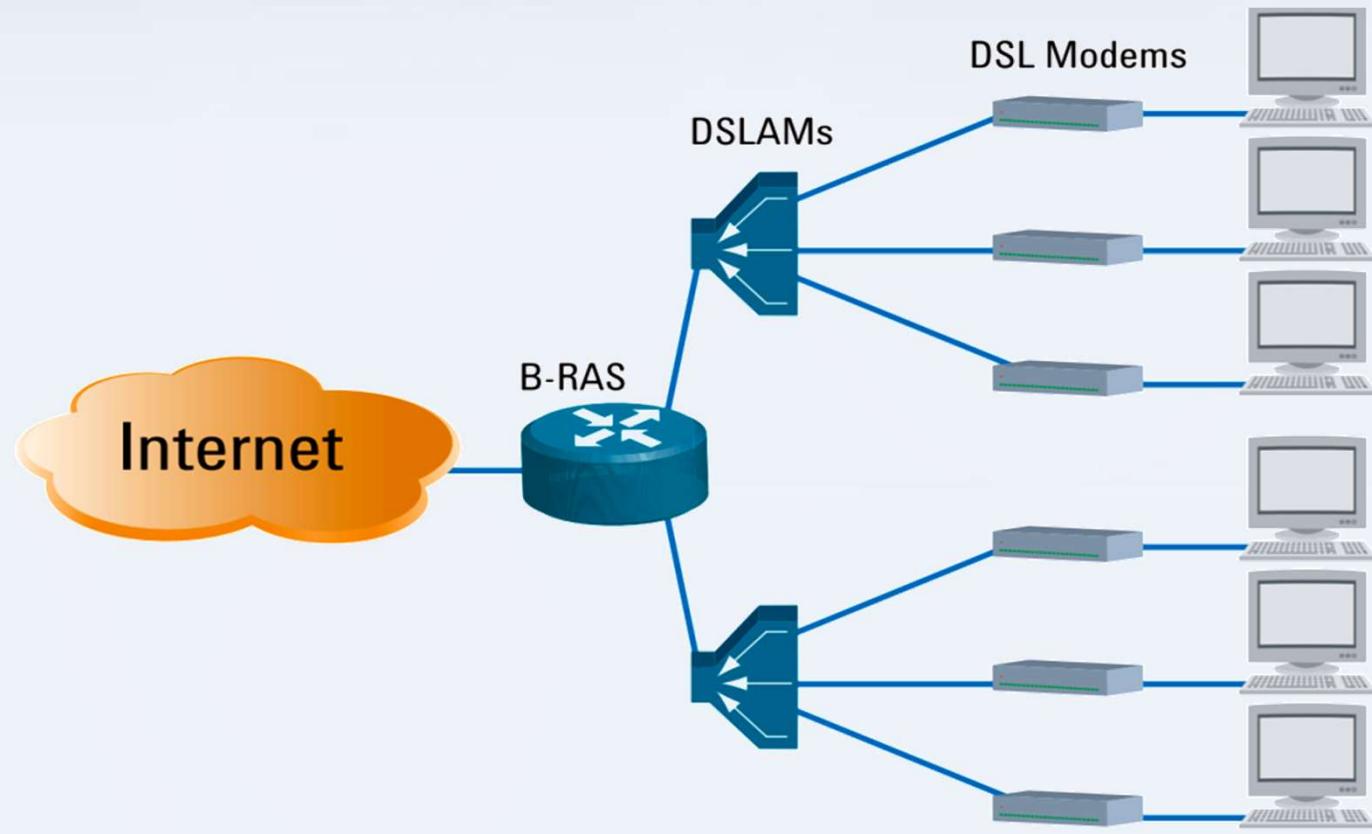
La modulation en QAM de chacun des canaux est automatiquement réglée de 0 à 15 bits par symbole et ce en fonction de la qualité du canal,



## Modulation des sous-porteuse

- Chacun des canaux de la ligne est testé dans une négociation préalable et périodique pour déterminer l'atténuation de ligne et le degré de perturbation à ce point-là de la bande passante.
- Si la ligne est perturbée ou l'atténuation forte sur l'étendue d'un canal, celui-ci se voit attribuer une modulation à faible nombre de bits par symbole. Cela peut aller jusqu'à la suppression du canal ( 0 bits par symbole ).
- Ainsi, la qualité de la ligne influe sur la vitesse de transmission, mais pas sur le taux d'erreurs.
- Si tous les canaux sont excellents, le débit maximum théorique d'un tel système est donc de  $15 \text{ bits} \times 4000 \text{ Hz} = 60 \text{ kbit/s}$  par canal.

# Infrastructure classique ADSL



# Infrastructure classique ADSL

## 1. Partie Utilisateur

On trouve un modem-routeur et d'un splitter qui assure la séparation des canaux, voies et données. Le Modem-routeur ADSL contient les éléments suivants :

- Un modem ADSL pour la connexion à Internet.
- Un Routeur pour gérer la translation d'adresse entre l'adresse publique et les adresses privées, assurant ainsi la fonction NAT (*Network Adress Translation*)
- Un Firewall pour sécuriser la connexion avec Internet.
- Un switch pour gérer les communications entre les appareils du réseau (ordinateurs, modem)
- Eventuellement un point d'accès WI-FI,
- Offre un accès de type Ethernet et USB .

# Infrastructure classique ADSL

## 2. Partie Réseau

- Les données numériques envoyées par le modem sont reçues par le **DSLAM** (*Digital Subscriber Line Access Multiplexer*). Le DSLAM regroupe les flux de données numériques provenant d'un certain nombre d'abonnés sur une seule liaison montante haute capacité (ATM ou liaison Gigabit Ethernet) au fournisseur de services Internet.
- Chez le fournisseur d'accès (FAI), les données agrégées de plusieurs abonnés sont traitées par le serveur **B-RAS** (*Broadband Remote Access Server*) qui authentifie les informations d'identification de l'abonné, valide les politiques d'accès des utilisateurs et achemine les données vers leurs destinations respectives sur Internet.

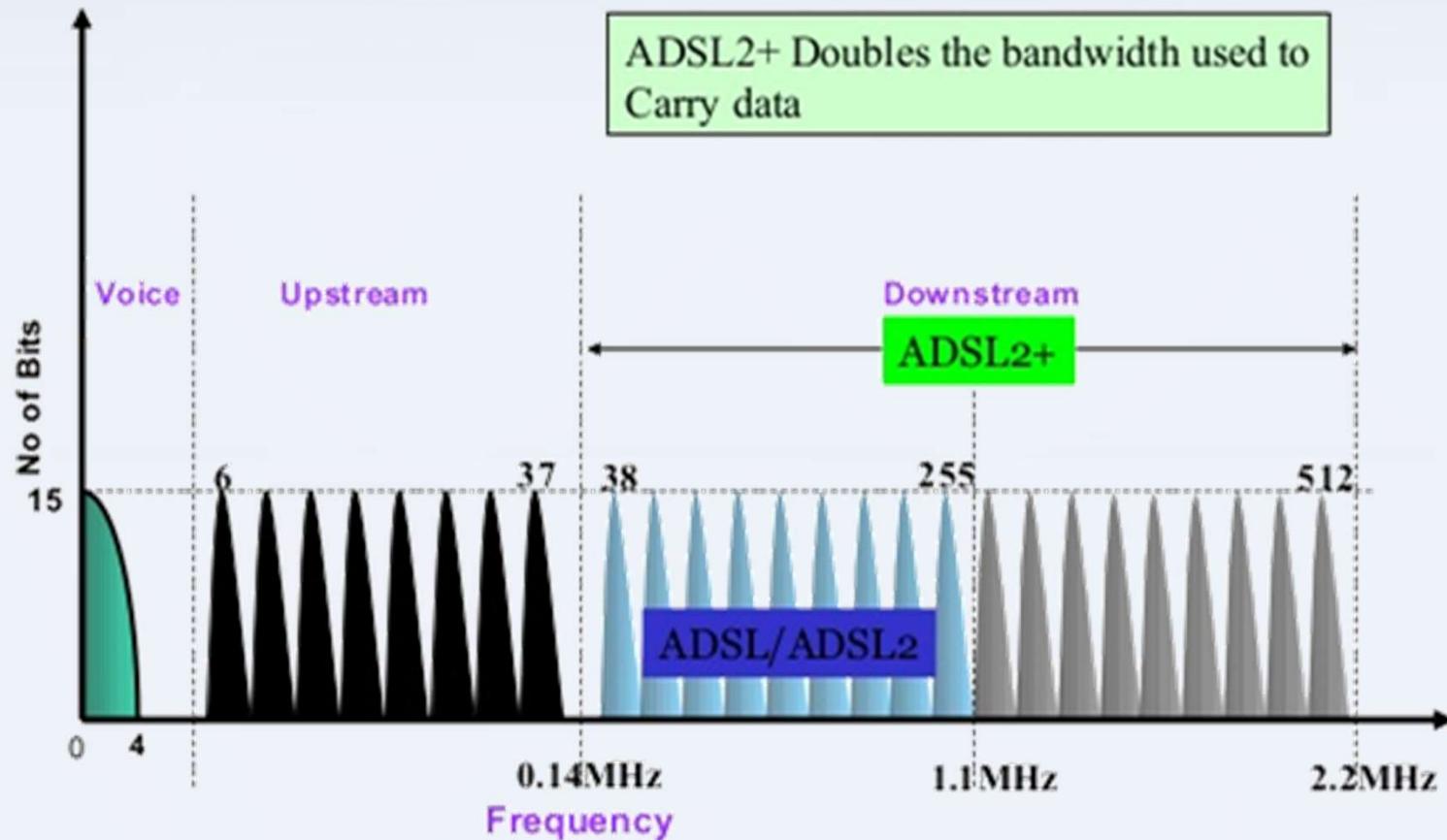
## Infrastructure classique ADSL

- L'authentification est réalisée soit à travers une interface Ethernet où les données IP sont encapsulées dans des trames PPP (*Point to Point Protocol*), qui sont encapsulés ensuite dans des trames Ethernet (PPPoE, PPP over Ethernet), créant ainsi un tunnel entre le modem (PPPoE client) de l'utilisateur et le BRAS (PPPoE server).
- Ou bien à travers une interface USB (**PPPoA**, *PPP over ATM*) pour la partie utilisateur...

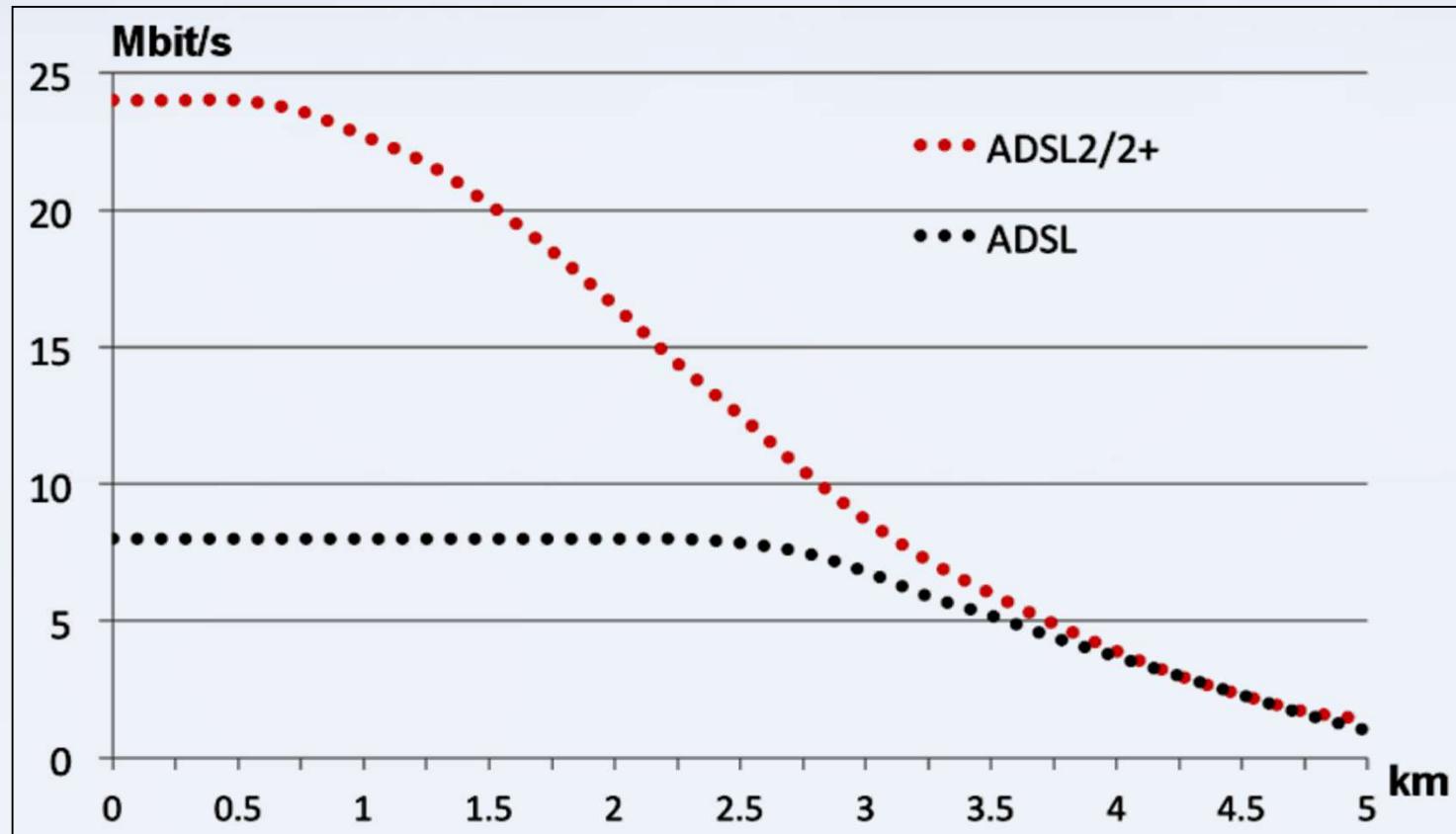
## La technologie ADSL2+

- C'est l'évolution de l'ADSL, cette norme est basée sur le doublement de la bande passante utilisée par l'ADSL première génération,
- Elle exploite une bande de jusqu'à 2,2 MHz au lieu de 1,1 MHz.
- Cela se traduit par une augmentation du débit maximal possible qui peut atteindre 24 MB/s.
- L'ADSL2+ est orienté débit plutôt que portée, ce qui fait que les améliorations par rapport à l'ADSL ne sont perceptibles que si l'abonné se situe à moins de 3 000 m du central téléphonique. Au-delà, les débits sont les mêmes que ceux proposés par l'ADSL.

# La technologie ADSL2+

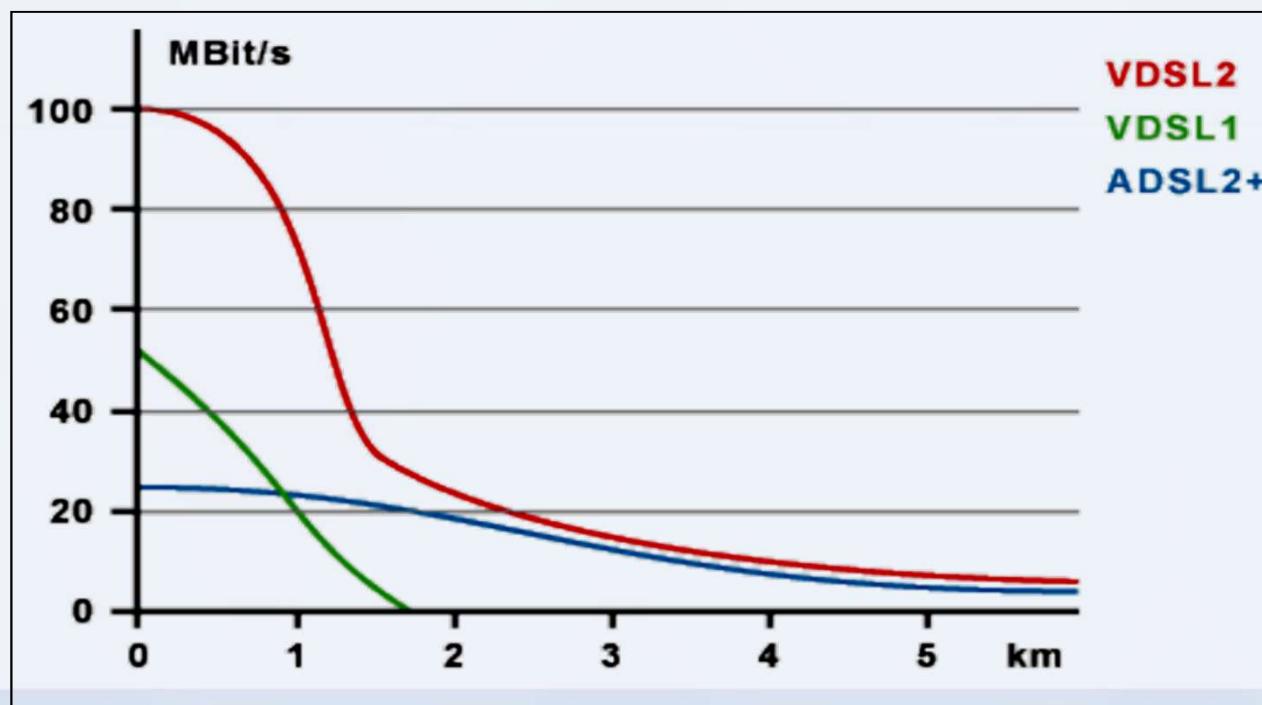


## La technologie ADSL2+



## Un débit encore plus élevé : le VDSL

- Avec une bande de fréquence encore plus large et un encodage plus efficace, le VDSL *very high bitrate DSL* et le VDSL2 (portée et débit largement supérieurs) offrent des débits plus élevés, ainsi qu'une possibilité de symétrie.
- La bande utilisée dans cette technologie est jusqu'a 12MHz, et utilise toujours la DMT.

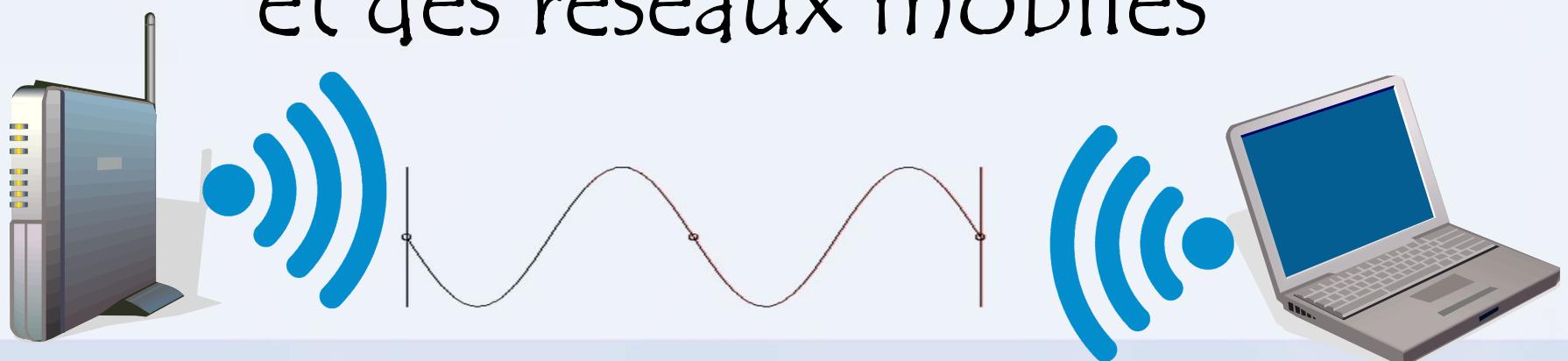


# *Chapitre IV*

# Normes et Protocoles

## Chapitre 04 P.1

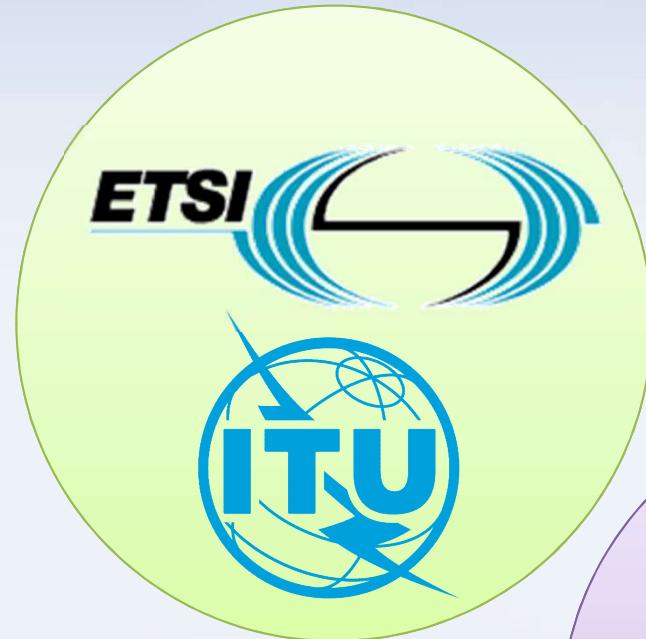
Les protocoles des réseaux sans fil  
et des réseaux mobiles



## Origine

- La norme *IEEE 802.11 (ISO/IEC 802-11)* est un standard international décrivant les caractéristiques d'un réseau local sans fil (*WLAN*).
- Le nom Wi-Fi (contraction de *Wireless Fidelity*, parfois notée à tort *Wifi*) correspond initialement au nom donné à la certification délivrée par la Wi-Fi Alliance, anciennement WECA (*Wireless Ethernet Compatibility Alliance*), l'organisme chargé de maintenir l'interopérabilité entre les matériels répondant à la norme 802.11.

# Origine



Régulation



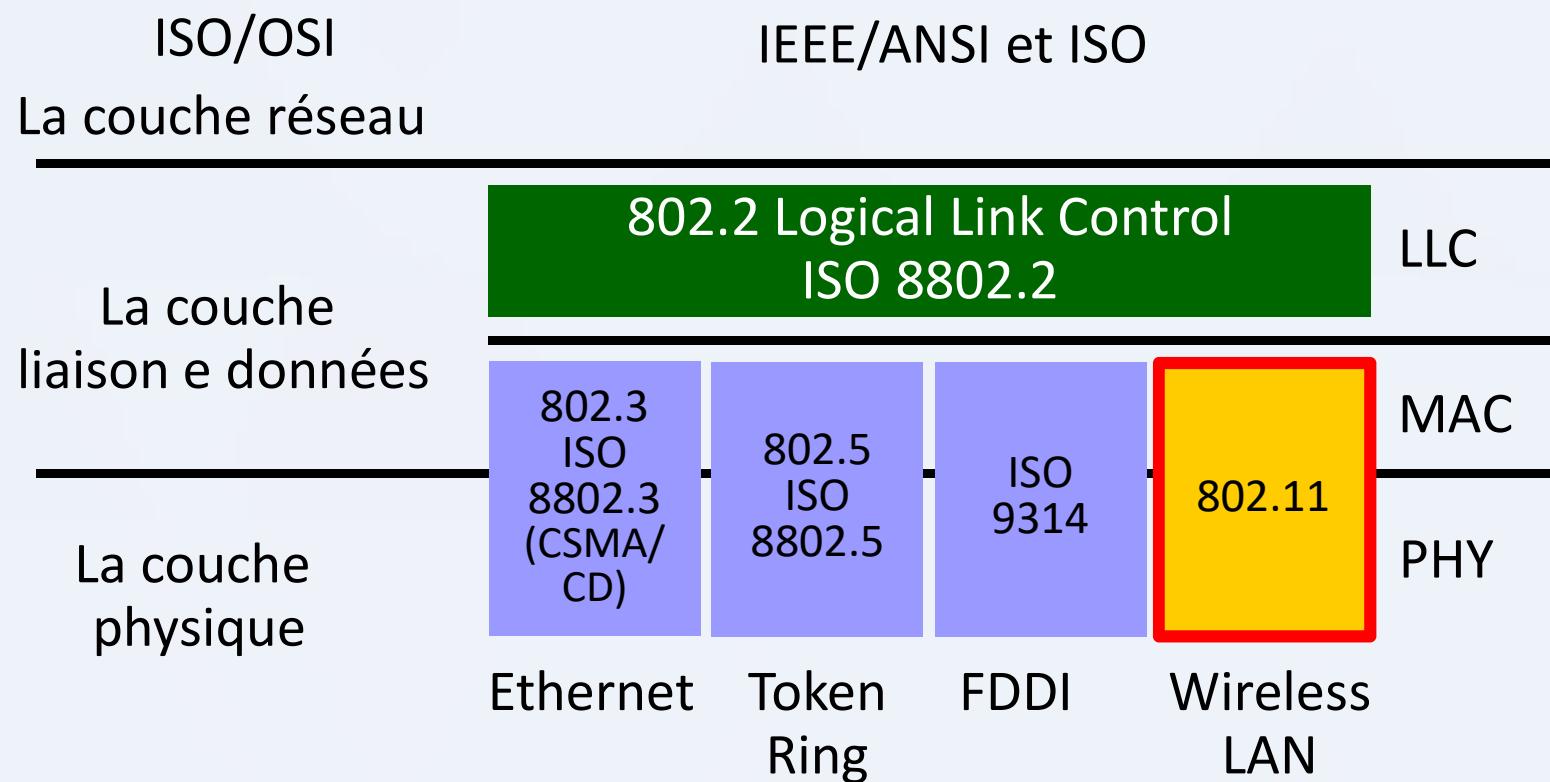
Compatibilité



Standardisation

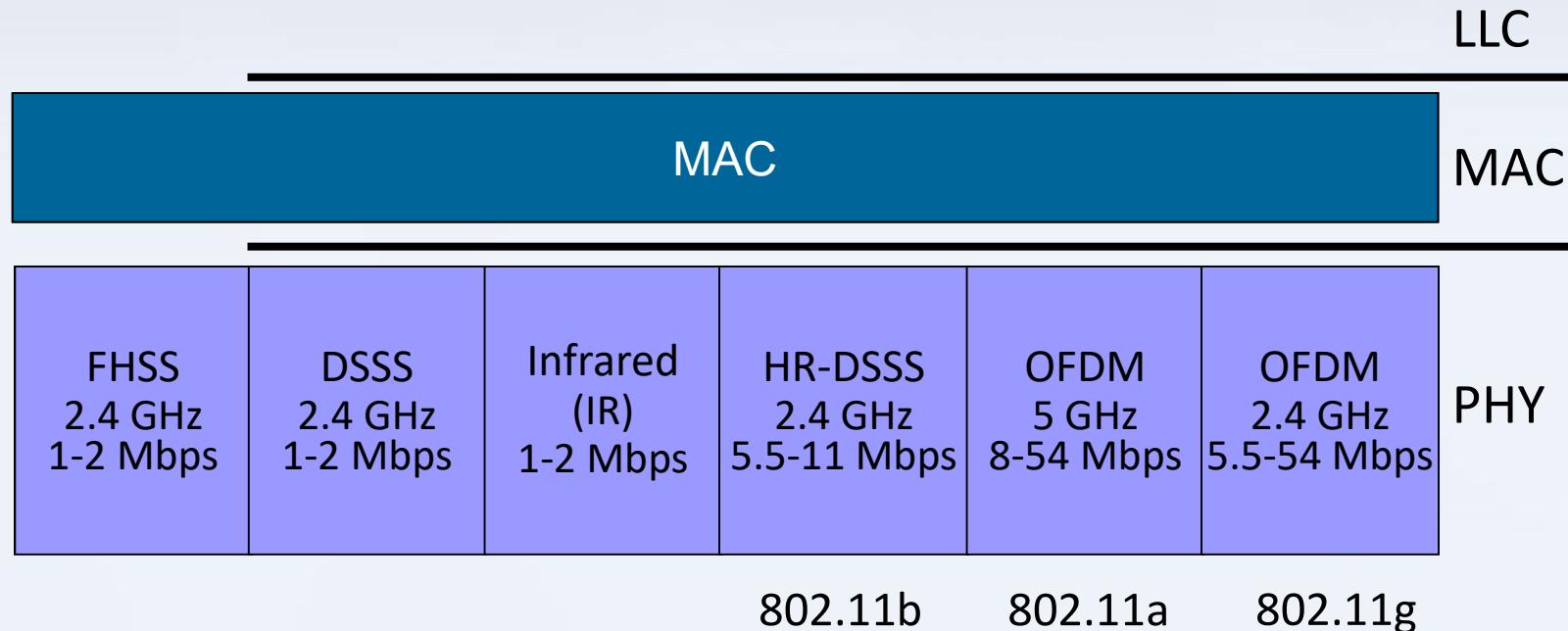
# Protocoles IEEE 802.11

La technologie WLAN du standard IEEE 802.11 couvre les couches “Physique” (L1) et “Liaison de données” (L2) du modèle OSI.



# IEEE 802.11 La couche physique

IEEE/ANSI et ISO



**LLC:** Logical Link Control Layer

**MAC:** Medium Access Control Layer

**PHY:** Physical Layer

**FHSS:** Frequency hopping SS

**DSSS:** Direct sequence SS

**SS:** Spread spectrum

**IR:** Infrared light

# Les standards IEEE 802.11

Protocol	Frequency	Signal	Date	Maximum data rate
Legacy 802.11	2.4 GHz	FHSS or DSSS	1997	2 Mbps
802.11a	5 GHz	OFDM	1999	54 Mbps
802.11b	2.4 GHz	HR-DSSS	1999	11 Mbps
802.11g	2.4 GHz	OFDM	2003	54 Mbps
802.11n	2.4 or 5 GHz	OFDM	2009	600 Mbps
802.11ac	5 GHz	256-QAM	2013	1.3 Gbps
802.11ax	2.4 or 5 GHz	1024-QAM	2018	9.6 Gbps

- Tous utilisent CSMA/CA pour un accès multiple,
- Tous ont des versions avec station de base et de réseau ad-hoc.

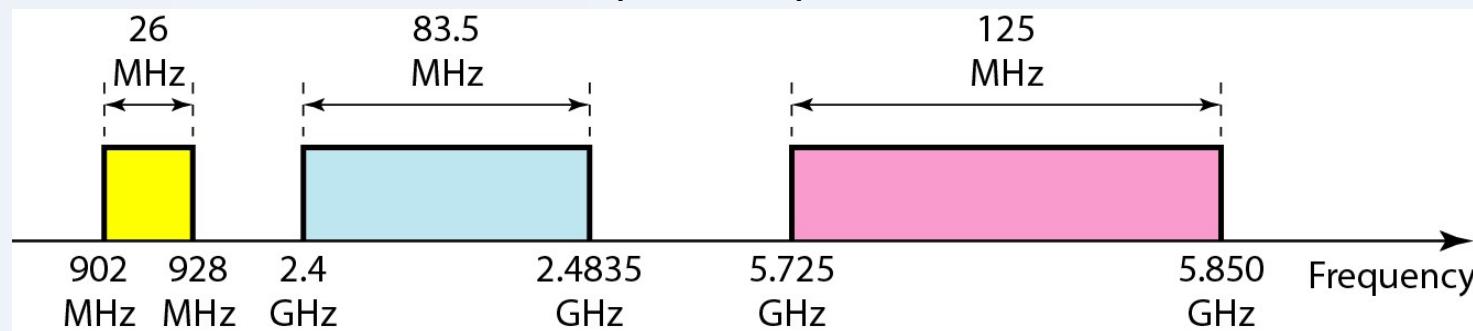
## Les couches 802.11

- Les détails de la réception et de la transmission sont traiter au niveau de la couche physique qui précise les caractéristiques de **bande de fréquence**, de **modulation**, **l'encodage** et les caractéristiques de la signalisation pour la transmission de données.
- Le standard 802.11 d'origine a défini trois couches physiques de base, FHSS, DSSS, IR. Les techniques IR (infrarouge) sont aujourd'hui obsolètes.
- La couche MAC définit un ensemble de **règles permettant d'accéder au médium** et d'envoyer des données, et les **règles de communication** entre les différentes stations.

# Bandes de fréquences

Les bandes ISM (industrielles, scientifiques et médicales) utilisées par le standard IEEE 802.11 et ses variantes sont les bandes en 2,4 GHz et en 5 GHz

- **Bande 2,4 GHz (IEEE 802.11b/g/n) :** 2,4 à 2,4835 GHz
- **Bande 5 GHz (IEEE 802.11a/n/ac) :**
  - ✓ 5,150 à 5,250 GHz (UNII-1)
  - ✓ 5,250 à 5,350 GHz (UNII-2)
  - ✓ 5,450 à 5,710 GHz (UNII-2e)
  - ✓ 5,725 à 5,875 GHz (UNII-3)

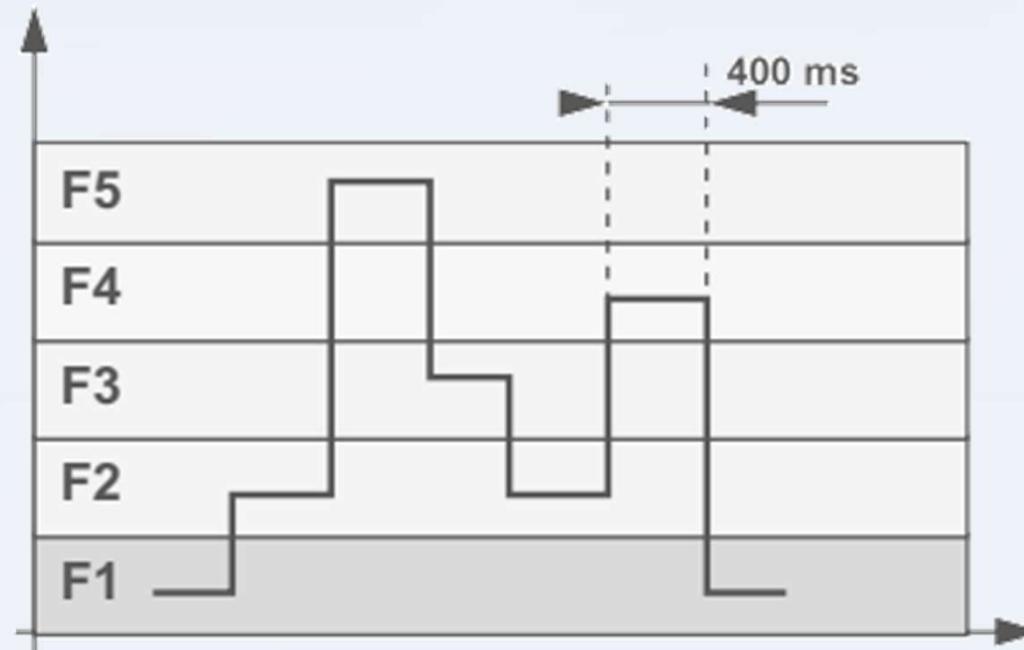


## La technique FHSS

- La technique **FHSS** (*Frequency Hopping Spread Spectrum*, en français étalement de spectre par saut de fréquence) consiste à découper la large bande de fréquence en un minimum de 75 canaux (hops ou sauts d'une largeur de 1MHz), puis de transmettre en utilisant une combinaison de canaux connue de toutes les stations de la cellule.
- Dans la norme 802.11, la bande de fréquence 2.4 - 2.4835 GHz permet de créer 79 canaux de 1 MHz.
- mais elles sont limitées à un débit de 2 Mbps
- En mode FHSS les données sont émises au moyen d'une modulation GMSK .

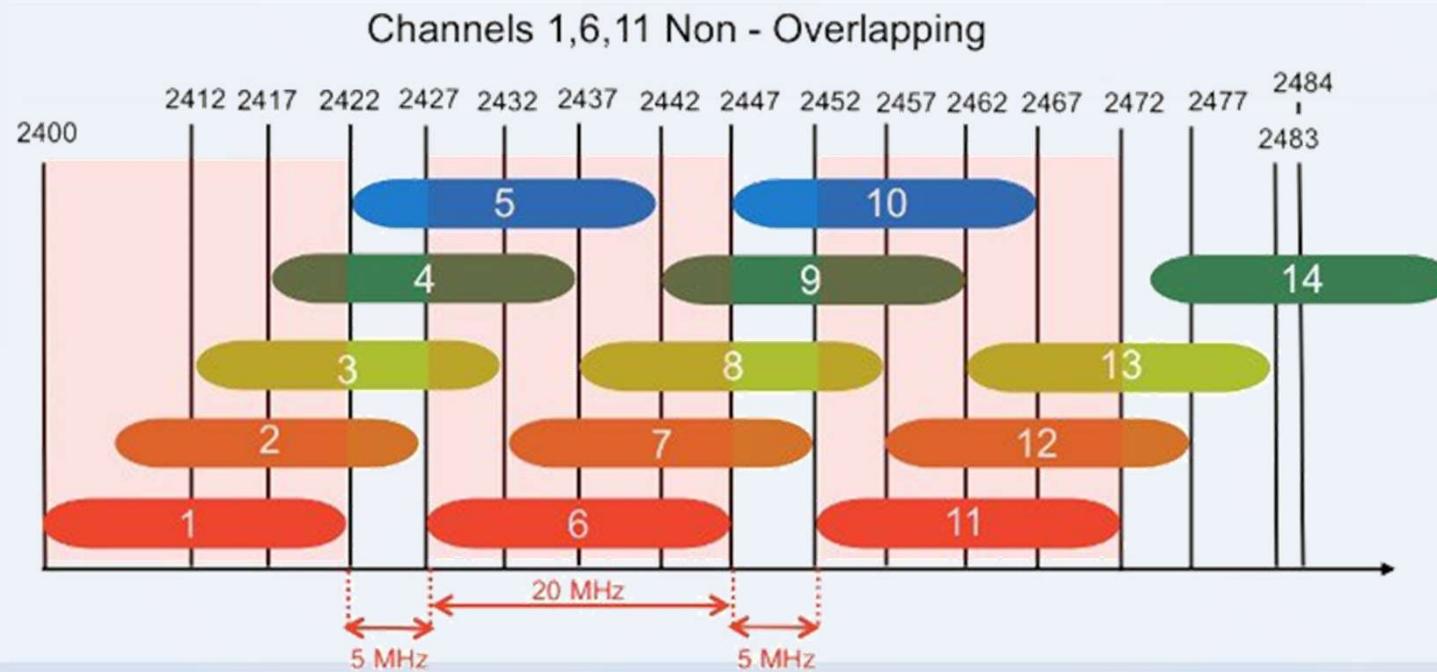
# La technique FHSS

Exemple de séquence pseudo-aléatoire de sauts de fréquence



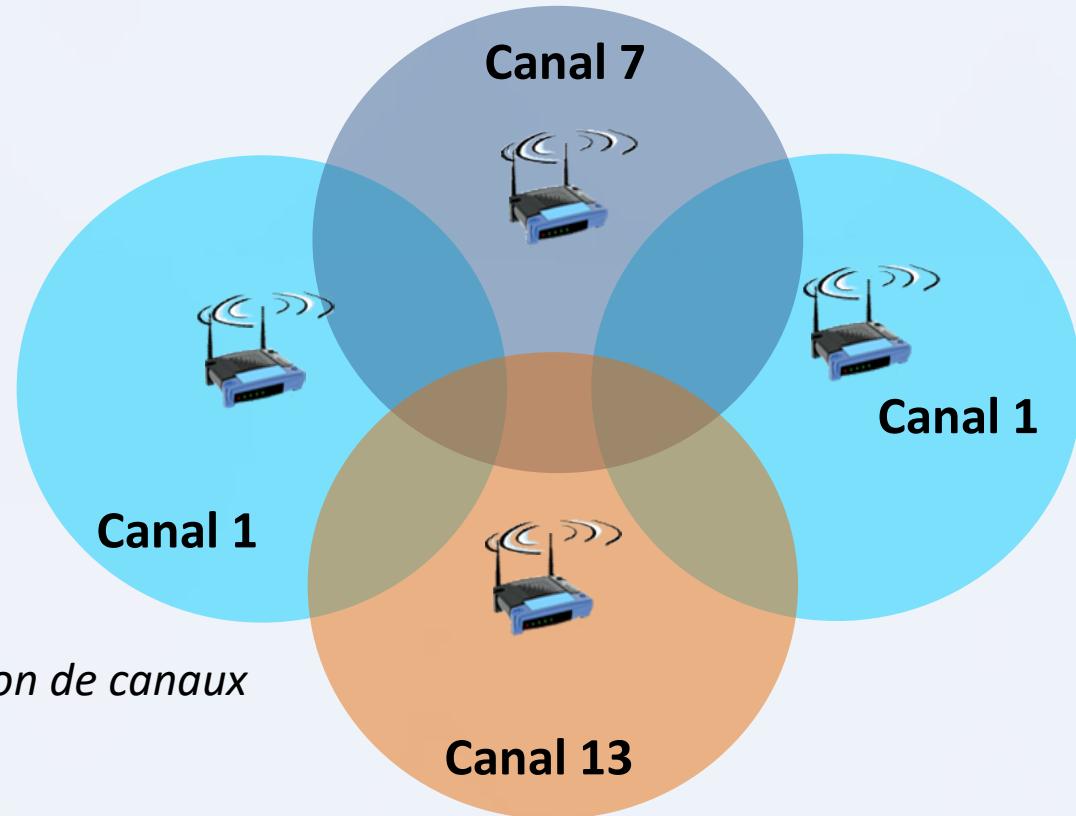
## La technique DSSS

- Comme le FHSS, le DSSS (**Direct Sequence Spread Spectrum**) divise la bande ISM en sous bandes. Cependant la division se fait ici en 14 canaux de 20 MHz chacun.
- La transmission ne se fait que sur un canal donné. La largeur de la bande ISM étant égale à 83.5 MHz, il est impossible d'y placer 14 canaux adjacents de 20 MHz.



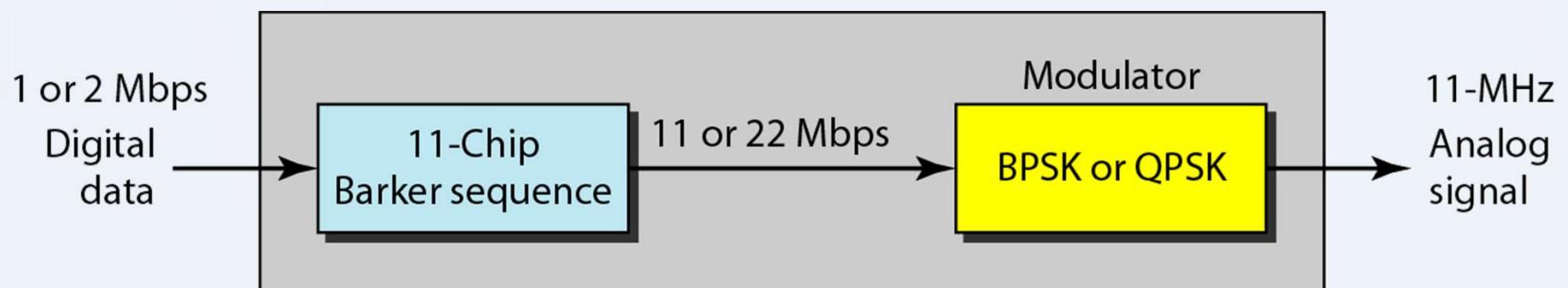
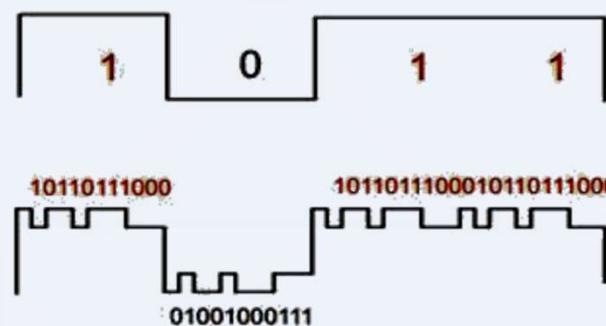
## La technique DSSS

- La transmission ne se fait que sur un seul canal,
- Un espace ne peut être couvert que par 3 canaux disjoints
- Si deux réseaux utilisant DSSS et l'un d'eux utilise le canal 6, le deuxième réseau peut utiliser les canaux 1, 11, 12, 13 et 14.



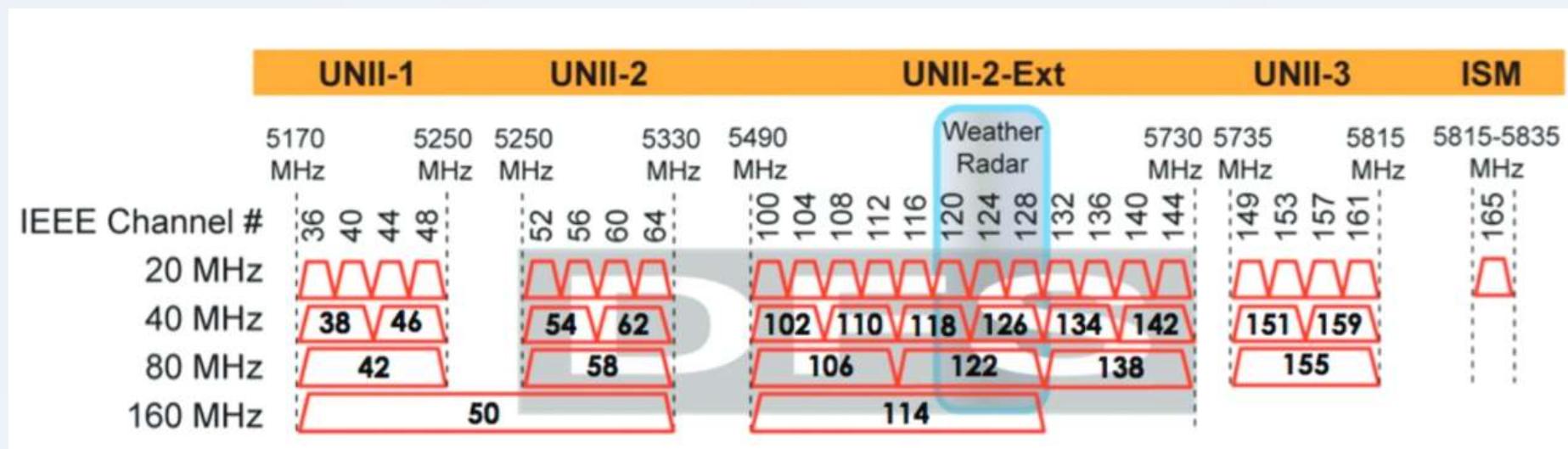
## La technique DSSS

- Dans le standard 802.11 DSSS, La technique du « chipping sur 11 bits » aide à compenser le bruit généré par un canal donné,
- cette technique consiste à transmettre pour chaque bit une **séquence Barker** (parfois appelée bruit pseudo-aléatoire, noté PN) de bits .



## Bande de fréquence 5 GHz

Le standard **802.11ac** supporte uniquement la bande de fréquence 5 GHz. Il propose l'usage de canaux d'une taille variant de 20, 40, 80 ou 160 MHz et il supporte jusqu'à huit flux simultanés (MU-MIMO).



## La couche liaison de données

- La couche liaison de données est scindée en deux sous-couches, la couche LLC et la couche MAC.
- La couche MAC définit deux modes d'accès au canal :
  - un mode d'accès par défaut qui organise un accès à compétition (**DCF**, *Distribution Coordination Function*)
  - et un mode d'accès optionnel proche du mode à réservation (**PCF**, *Point Coordination Function*) avec un contrôle centralisé géré par le point d'accès.

## La sous-couche MAC

- Au niveau de la sous-couche MAC, le standard IEEE 802.11 propose une méthode d'accès au support (medium) qui est bien différente de celle d'Ethernet.
- Alors que le standard Ethernet **IEEE 802.3** utilise CSMA/CD (*carrier sense multiple access collision Detection*) qui vise à détecter des accès concurrents sur un fil,
- Le standard Wi-Fi IEEE **802.11** se propose d'éviter les collisions avec **CSMA/CA** pour “Collision **Avoidance**” sur un support partagé comme l'air, avec des mécanismes de contention,
- Donc, le Wi-Fi est basé sur la contention, ce qui signifie qu'il y a des règles d'accès pour les stations qui tentent d'accéder au média et que les collisions sont traitées de manière équitable pour que chacun ait une chance de placer son trafic.

## Le protocole CSMA/CA

Le protocole CSMA/CA utilise :

- des trames d'acquittement;
- des temporisateurs d'espacement des trames (*Inter-Frame Spacing*) ;
  - **SIFS:** Short Inter-Frame space; est le plus petit intervalle inter-trame. Les nœuds utilisant SIFS ont la priorité la plus élevée pour accéder au canal. Utilisé pour accusé la réception à l'expéditeur,
  - **DIFS:** DCF Inter-Frame Space; une machine doit sonder le canal pendant une durée d'un DIFS. Il est calculé de la manière suivante :  $DIFS = SIFS + (2 * \text{Slot time})$
  - **EIFS** (*Extended IFS*) est utilisé pour toute retransmission après réception d'une trame incorrecte (CRC ou collision).
  - **PIFS** (*Point Coordination IFS*) de  $78\mu s$  est utilisée par le Point d'accès pour obtenir l'accès au support avant n'importe

 Remember!!!

Les communications WIFI sont  
Half-Duplex !



<b>Standard</b>	<b>Slot Time (<math>\mu</math>s)</b>	<b>DIFS (<math>\mu</math>s)</b>
IEEE 802.11b	20	50
IEEE 802.11a	9	34
IEEE 802.11g	9 or 20	28 or 50

## Le protocole CSMA/CA

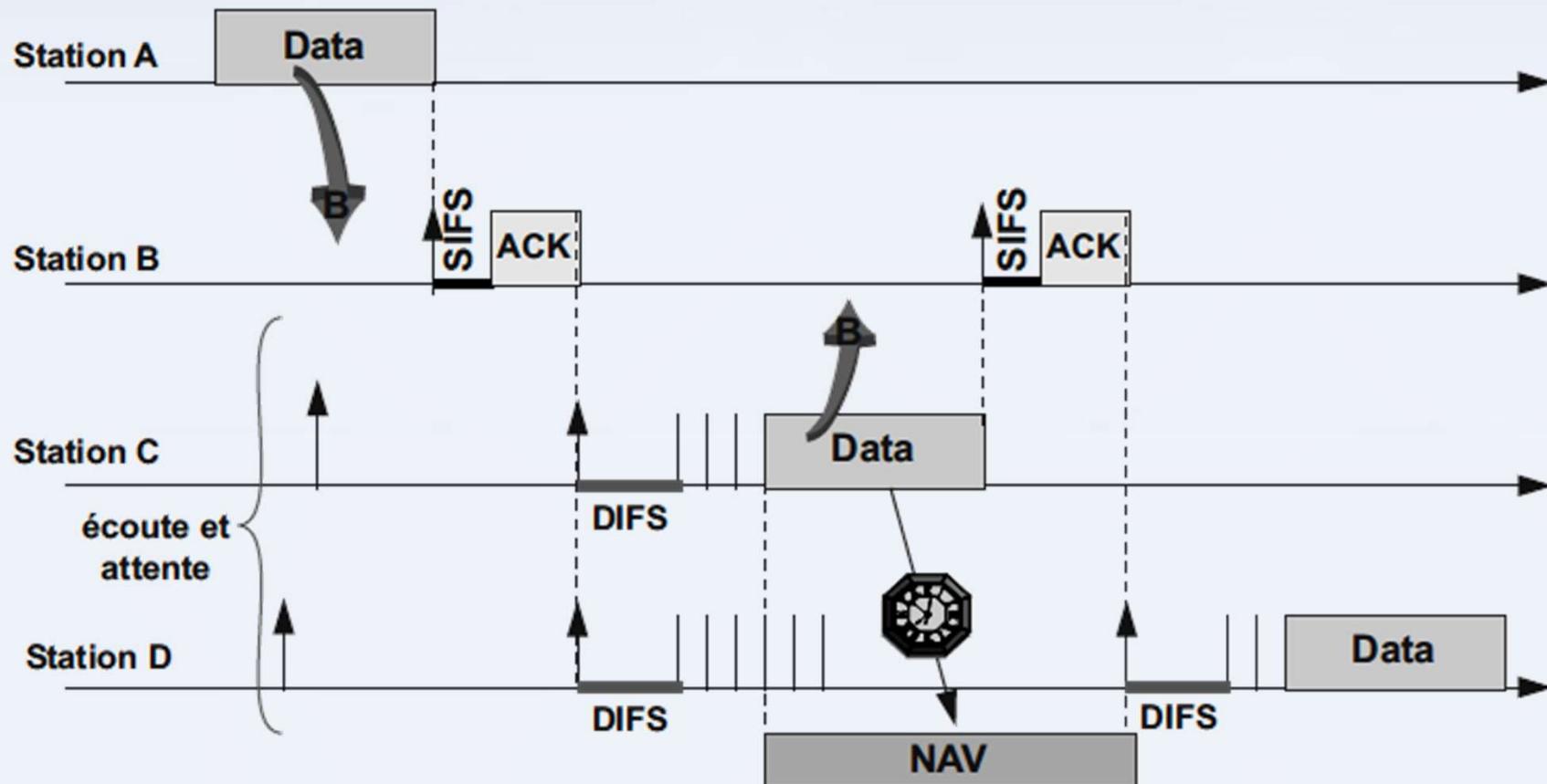
- Pour réduire la probabilité de collision, le CSMA/CA est complété par un mécanisme de réservation dit : ***Virtual Carrier Sense***.
- Toute trame émise contient une information sur la durée totale du cycle de transmission (données + ACK).
- Ainsi toute station écoutant le support, à réception de cette information, positionne un temporisateur (**NAV**, *Network Allocation Vector*) et s'interdit toute émission durant cet intervalle de temps.
- À l'échéance de ce timer,  $D$  réinitialise un cycle d'acquisition du support (DIFS + *BackOff* ).

## Le protocole CSMA/CA

- l'algorithme de Backoff
  - ✓ initialise un temporisateur avec une valeur aléatoire (0 à 7) ;
  - ✓ décrémente le temporisateur dès que le support est libre ;
  - ✓ quand la valeur est nulle, la station peut émettre ;
  - ✓ si le support est occupé avant la valeur 0, le décompte est bloqué ;
  - ✓ à chaque nouvelle tentative la valeur du temporisateur est

- A la fin de la transmission d'un paquet de données, le support redevient libre, et il est possible que deux stations démarrent un échange simultanément. => La norme IEEE802.11 a mis en place une temporisation aléatoire appelée contention ou backoff.
- chaque station choisit un nombre aléatoire entre 0 et N et attend ce nombre de slots avant d'accéder au support.
- le back off est exponentiel, c'est-à-dire qu'à chaque fois qu'une station entre en collision, le temps d'attente augmente exponentiellement.
- l'algorithme de backoff exponentiel est exécuté quand une station veut émettre et que le support est occupé ou après chaque transmission ou retransmission réussie
- ce mécanisme n'est pas utilisé quand la station décide de transmettre un nouveau paquet et que le support a été libre pour un temps supérieur au DIFS.

# Le protocole CSMA/CA



 Remember!!!

C'est la non-réception de l'ACK qui informe la station de l'état de collision.



 Remember!!!

**Mode ad-hoc** : Uniquement DCF

**Mode Infrastructure** : utilise DCF et PCF



 Remember!!!

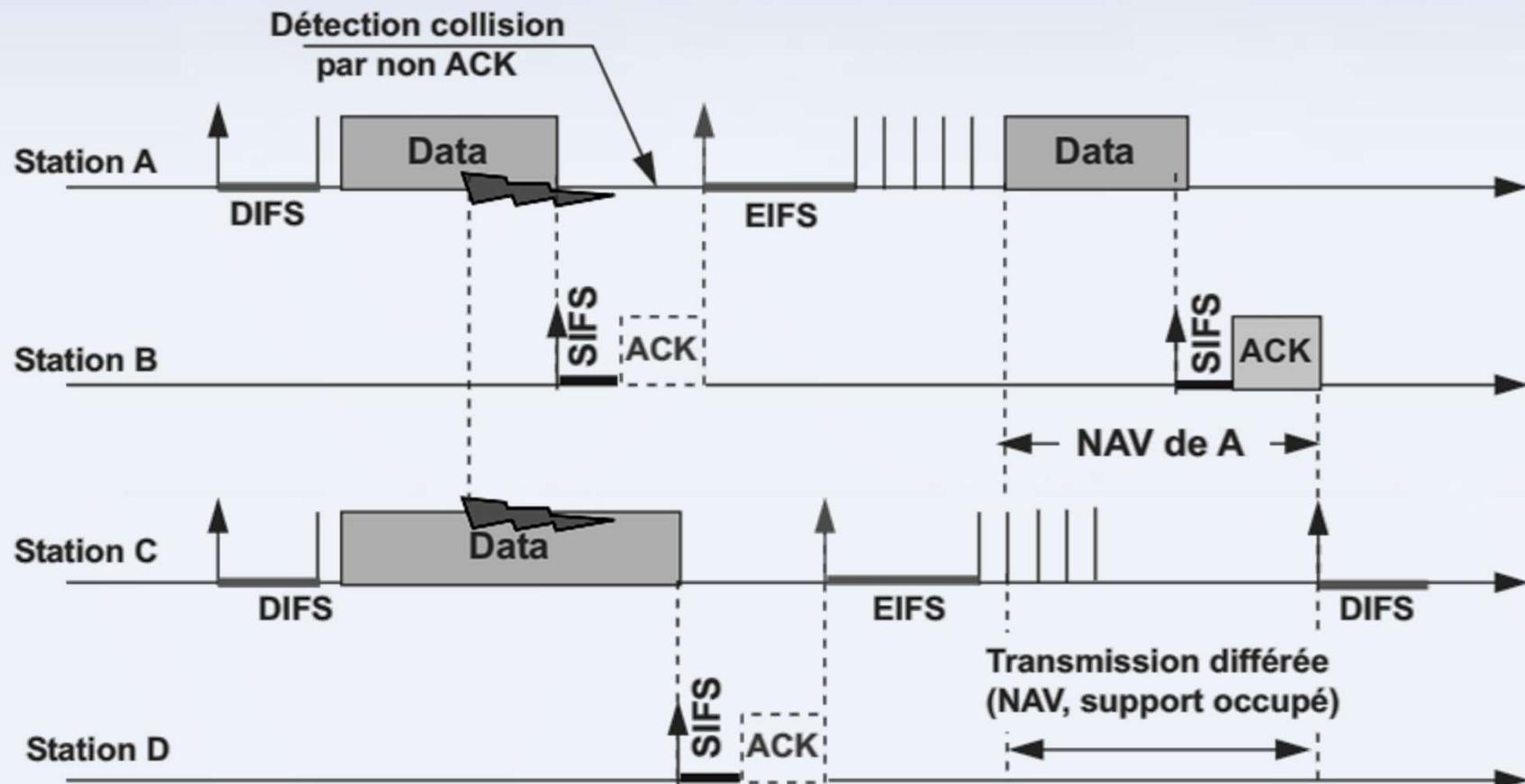
**Le SIFS** est utilisé pour séparer les transmissions appartenant à un **même dialogue**



## Le protocole CSMA/CA

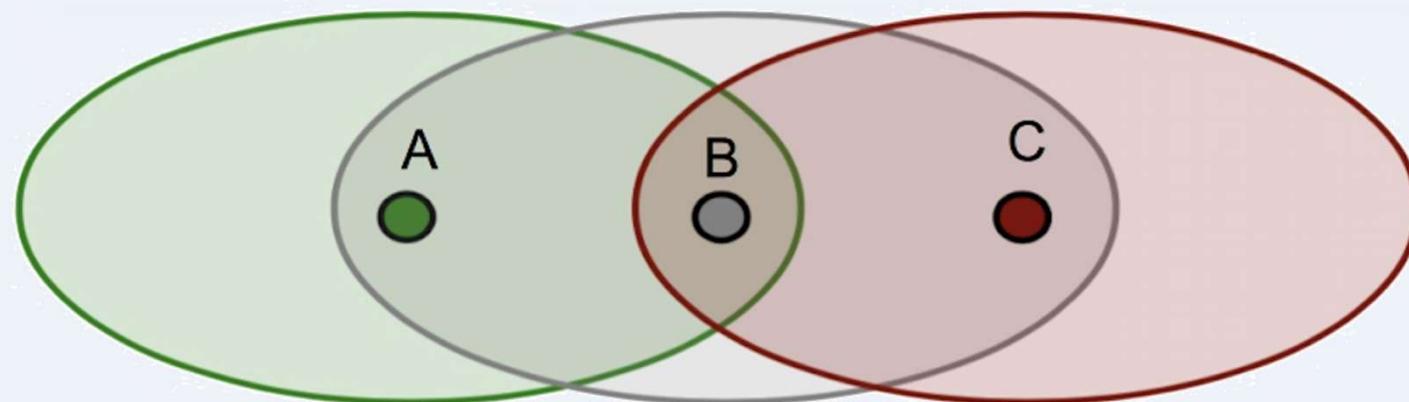
- Une station voulant transmettre écoute le support, et s'il est occupé, la transmission est différée.
- Si le support est libre pour un temps spécifique (appelé **DIFS**, *Distributed Inter Frame Space*), alors la station est autorisée à transmettre après une durée tirée aléatoirement en se basant sur l'**algorithme de Backoff**,
- La station réceptrice va vérifier le CRC du paquet reçu et renvoie un accusé de réception (ACK).
- La réception de l'ACK indiquera à l'émetteur qu'aucune collision n'a eu lieu.
- Si l'émetteur ne reçoit pas l'accusé de réception, alors il retransmet le fragment jusqu'à ce qu'il l'obtienne ou abandonne au bout d'un certain nombre de retransmissions.

# Exemple de collision CSMA/CA



## Problème de la station « cachée »

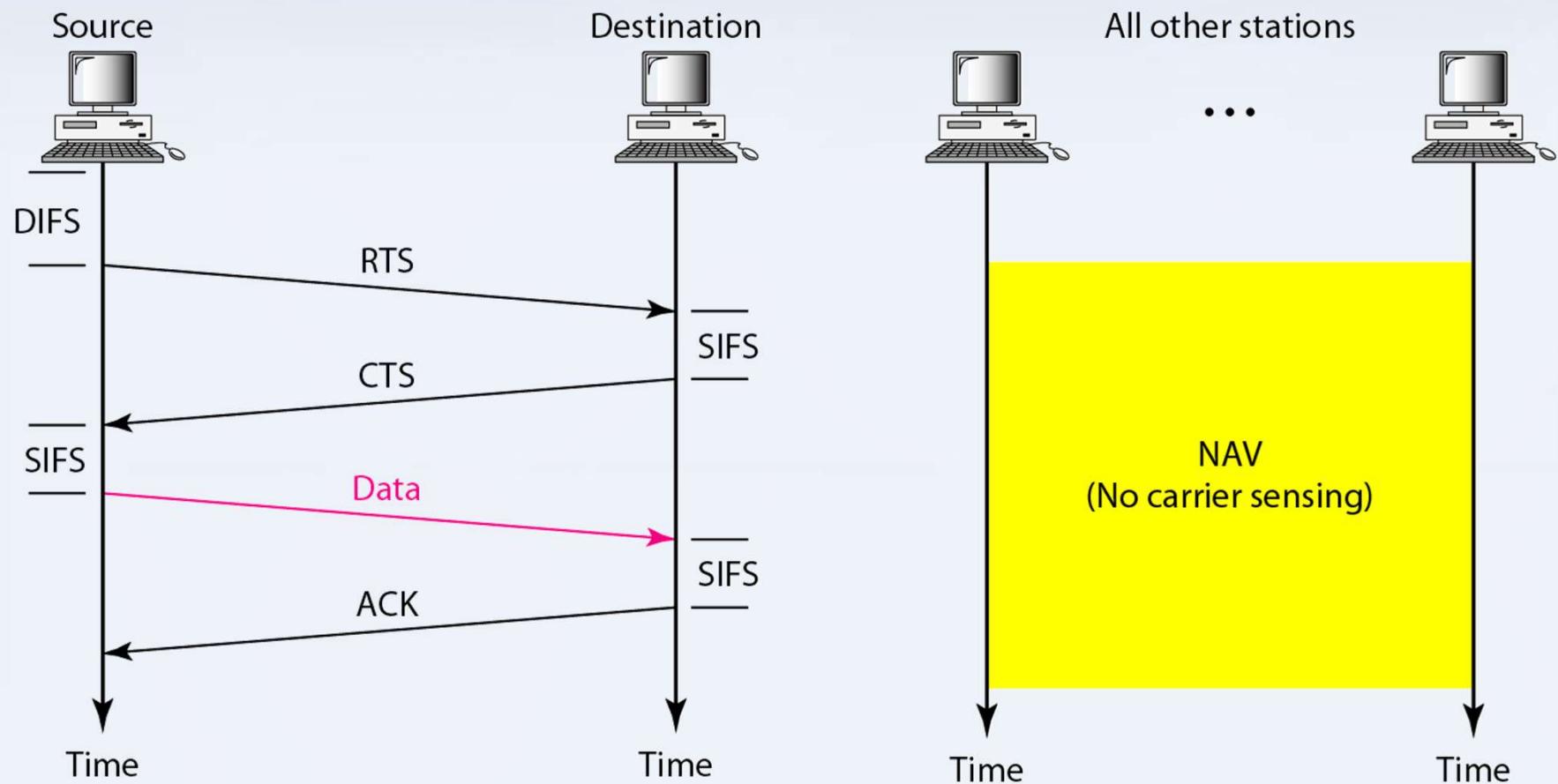
- Une station n'est pas obligatoirement reçue par toutes les autres stations. La station A ne reçoit pas les trames de la station C ;
- Si les 2 stations veulent émettre, elles détecteront toutes les deux un support libre et émettront leurs trames. Il y aura une collision.



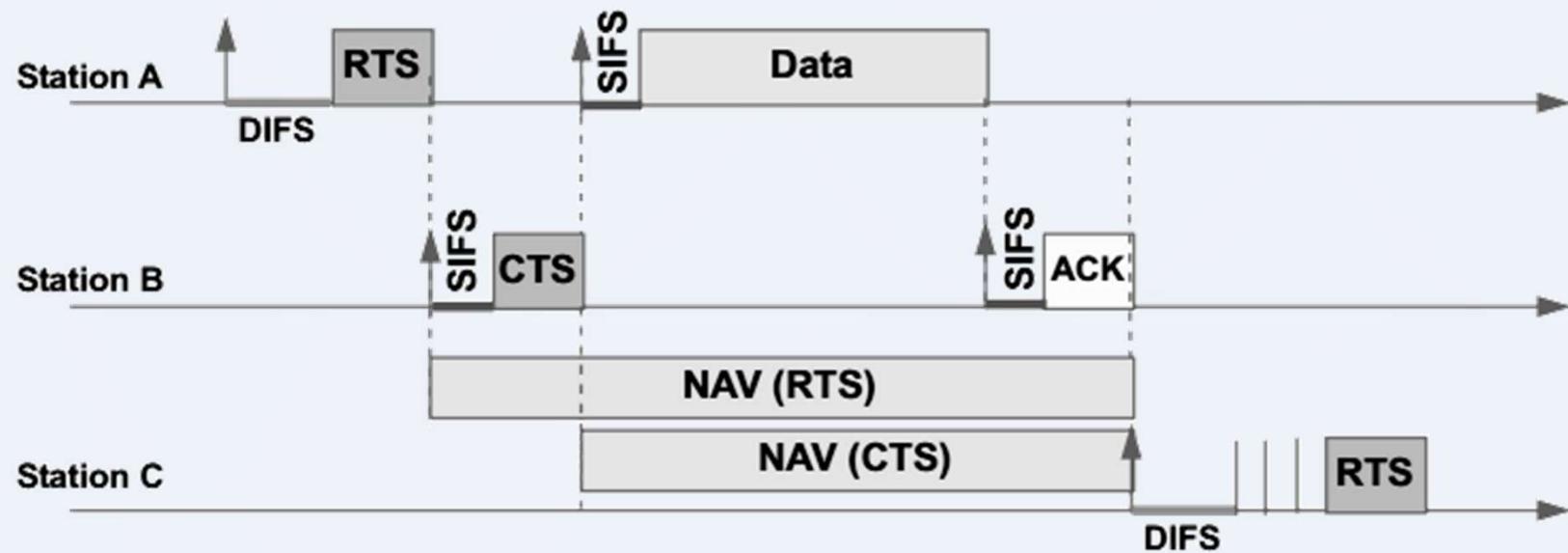
## Le protocole CSMA/CA avec RTS/CTS

- Pour minimiser les collisions, un mécanisme optionnel peut être utilisé (RTS/CTS),
- L'idée est de « **réserver** » le canal plutôt que l'accès aléatoire: éviter les collisions de trames de données longues,
- L'expéditeur transmet d'abord de petits paquets de demande d'envoi , RTS (*request to send*) au point d'accès, ne contenant que l'information de réservation du support (**NAV**) ,
- Les RTS peuvent toujours entrer en collision les uns avec les autres (mais ils sont courts), peu probablement,
- Le point d'accès diffuse un CTS (*clear to send*) en réponse à un RTS donné, qui sera entendu par tous les nœuds, et qui comprendront qu'un échange de données suivra, et reportent les transmissions
- La valeur du NAV de cette trame est décrémentée du temps déjà écoulé,

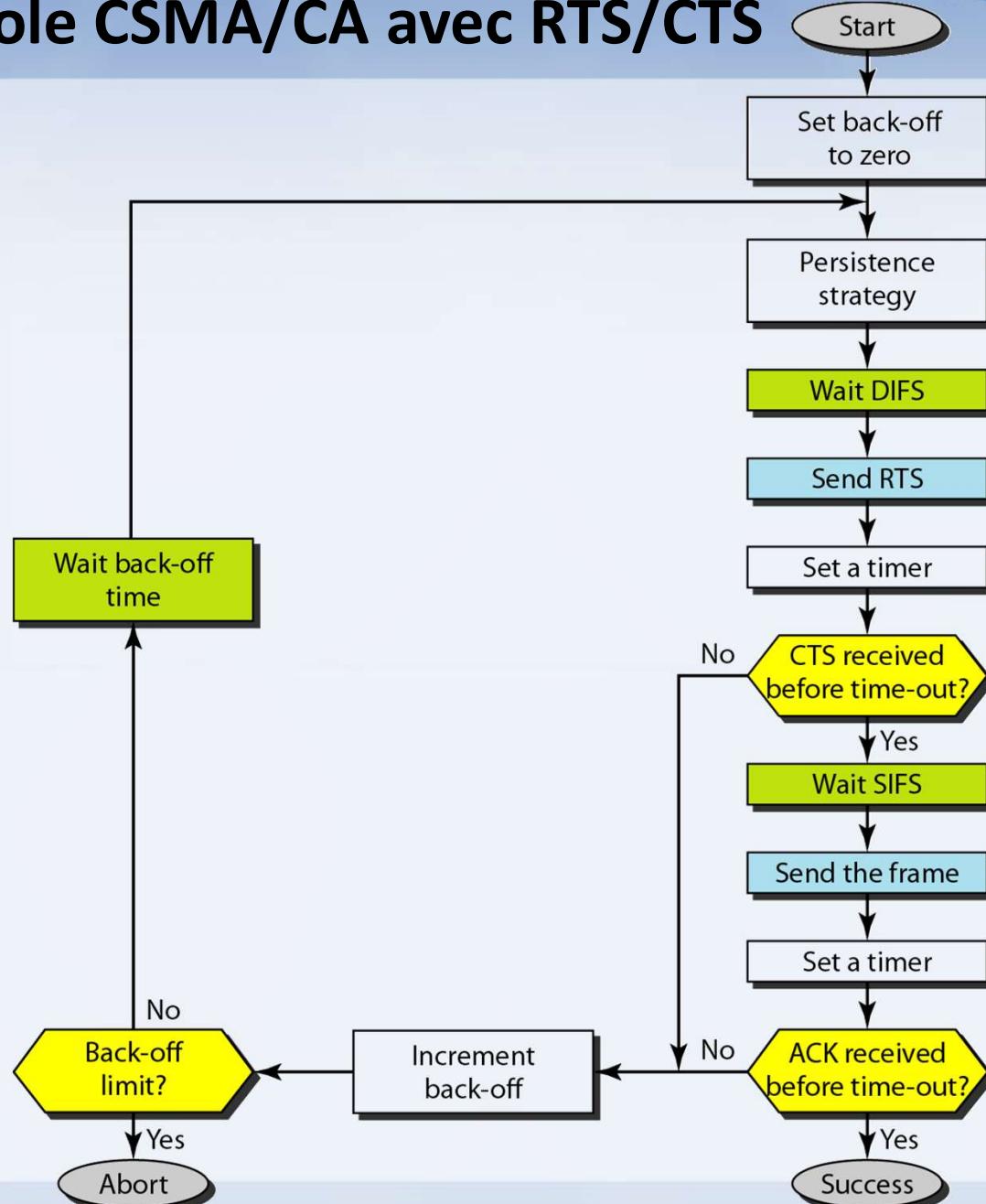
# Le protocole CSMA/CA avec RTS/CTS



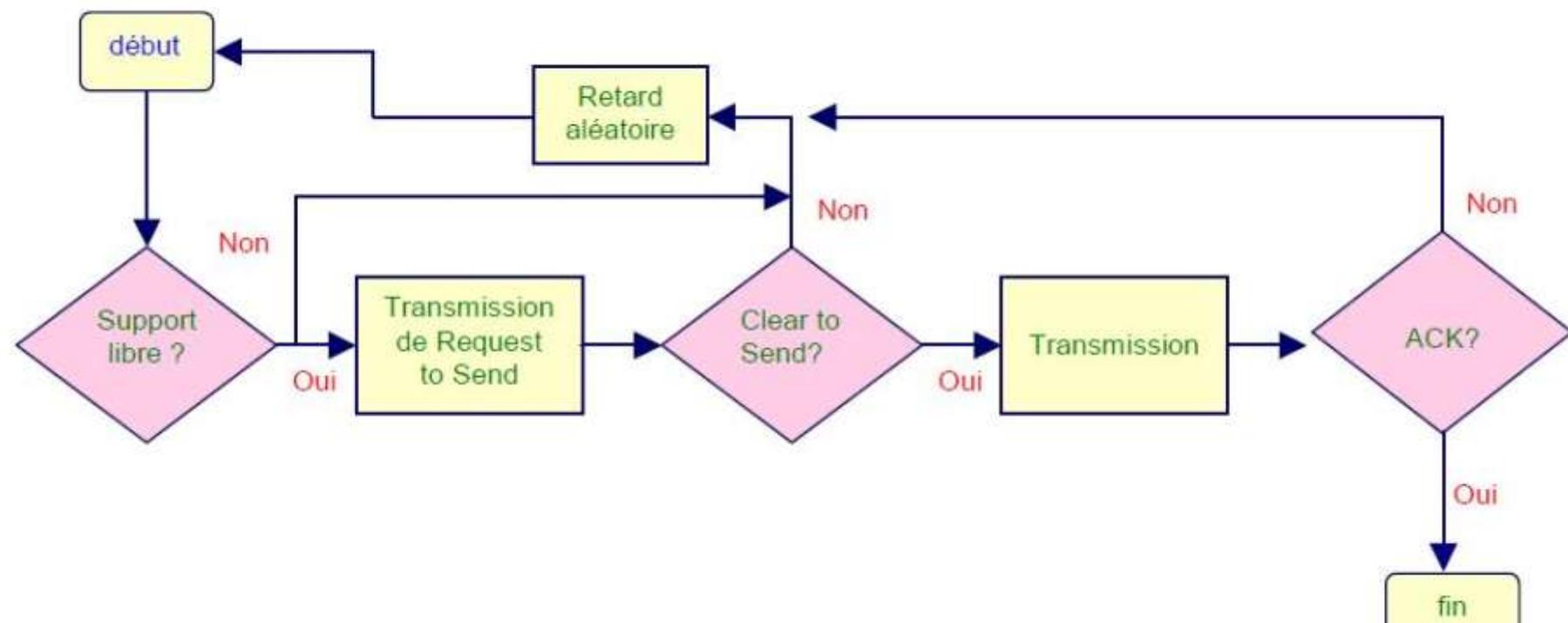
# Le protocole CSMA/CA avec RTS/CTS



# Le protocole CSMA/CA avec RTS/CTS

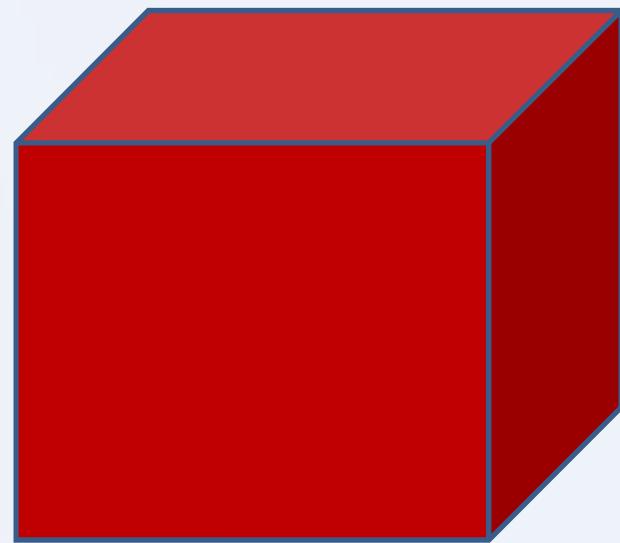


# Le protocole CSMA/CA avec RTS/CTS



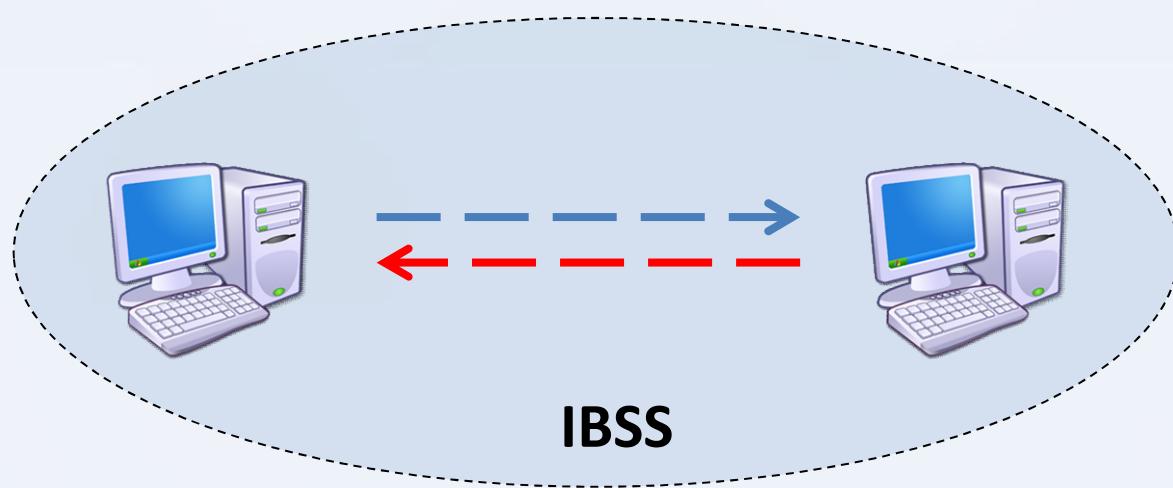
## Service Set et SSID

- Dans les technologies WLAN IEEE 802.11, un “**Service Set**” ou “ensemble de services” est un groupe logique de périphériques radios faisant partie d’un réseau identifié par un nom appelé le **SSID** (Service Set Identifier)
- Le SSID est diffusé par les stations grâce des trames de balises (*beacon*) pour annoncer la présence d’un réseau.
- Les **stations** désignent les ordinateurs du réseau WLAN ou d’autres types de clients.
- Les point d'accès, point de centralisation physique des communications sans fil est aussi appelé “station de base”.



## Le mode Ad- Hoc sans infrastructure

- Permet de réaliser un réseau poste à poste (chaque poste peut communiquer avec chacun des autres postes),
- On n'utilise aucun point d'accès,
- Ce mode est également appelé ***Ensemble de Services de Base Indépendants*** (Independent Basic Service Set).



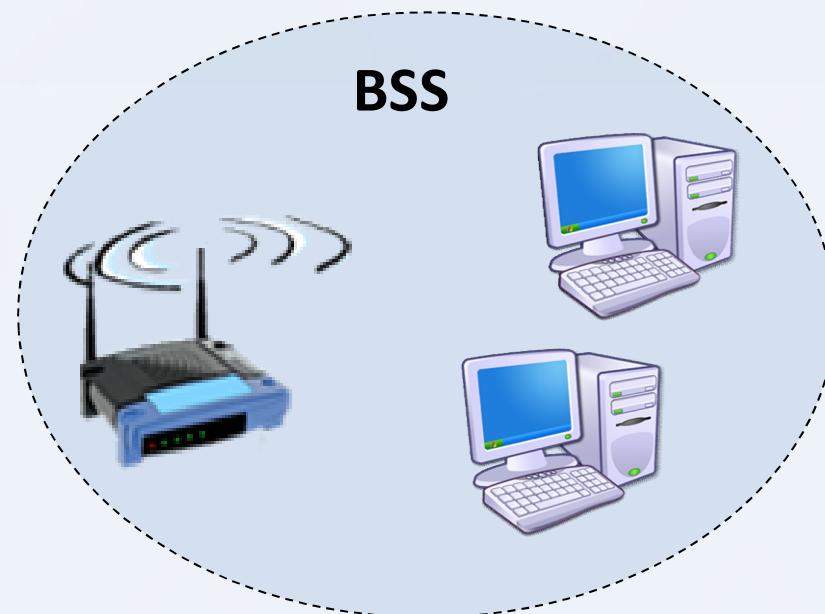
## Le mode infrastructure

Un réseau sans fil en mode infrastructure conforme à la norme IEEE 802.11 comprend des composants essentiels :

- **Les stations** : désignent les ordinateurs du réseau WLAN ou d'autres types de clients.
- **Les stations de base, ou points d'accès (AP)**, servent de "ponts" (L2) pour la communication entre les stations entre elles et entre les stations et les hôtes externes au réseau sans fil via le système de distribution (DS).
- **Le système de distribution**: ou DS a pour tâche de permettre la communication entre les points d'accès (AP) et le monde extérieur ou entre les points d'accès. Le protocole IEEE 802.11 ne définit pas la nature du DS.

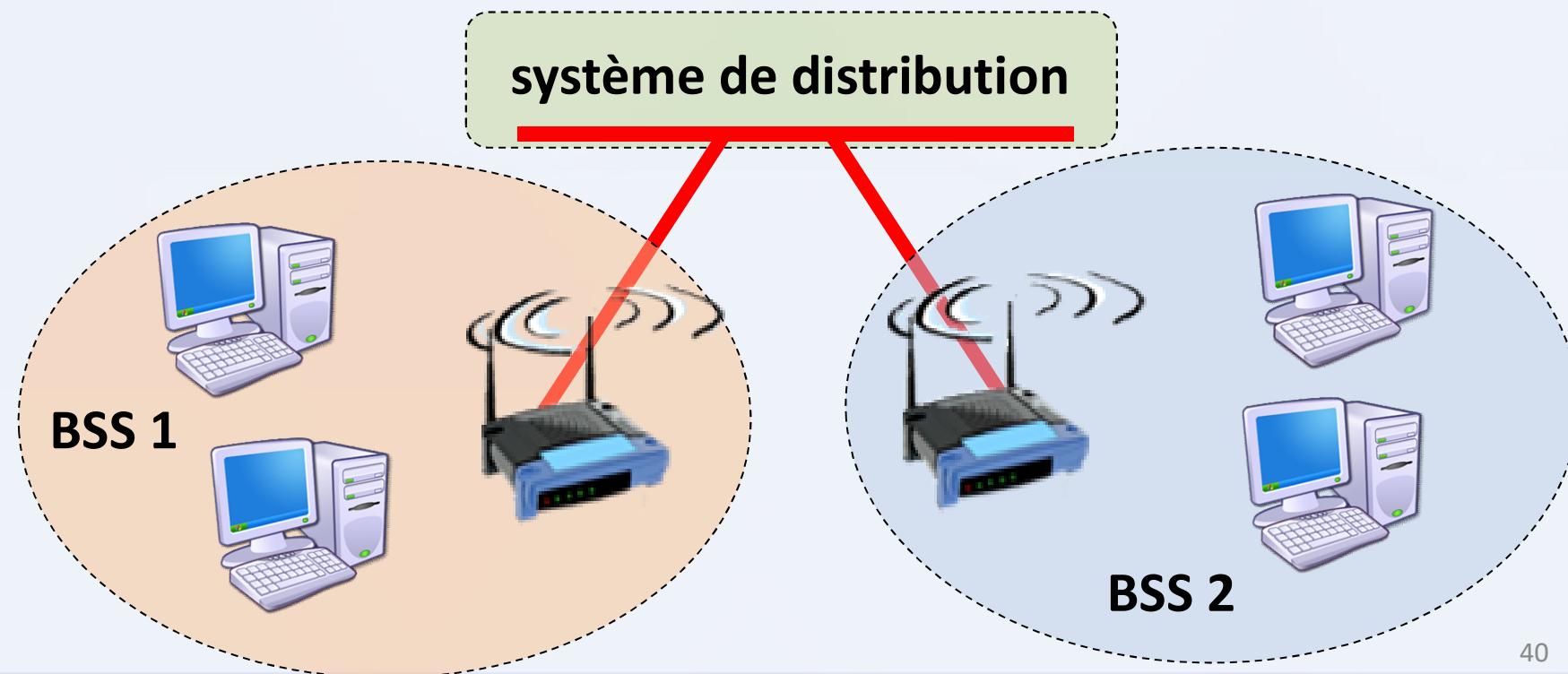
## Le mode infrastructure

- Chaque point d'accès définit une cellule, (**BSA**, “Basic Service Area”), .
- L'ensemble A.P et postes inclus dans la cellule constituent un **Ensemble de Services de Base** (Basic Service Set).
- Un BSS est identifié par un **BSSID** (*Basic Service Set Identifier*), cet identifiant, sur 6 octets, correspond à l'adresse MAC du point d'accès.



# Extended Service Set

- Les ESS connectés en sous-réseau constituent un ***Ensemble de Services Etendus*** (Extended Service Set).
- Chaque AP desservant un BSS dans un ESS communique avec les autres BSS via un réseau fédérateur faisant partie du système de distribution (DS).



## Réseaux sans fil nouvelle génération

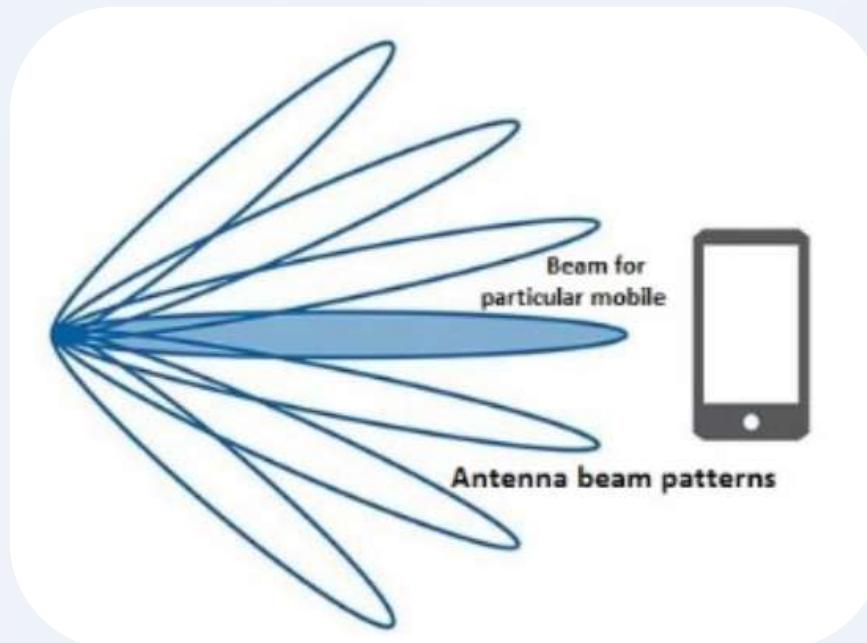
- Dans les réseaux locaux, le nombre de périphériques connectés, ainsi que les débits de données augmentent rapidement.
- L'Alliance Wireless Gigabit (WiGig) et **IEEE 802.11ad/ay** ont développés les spécifications des réseaux sans fil personnels et locaux opérant sur la fréquence millimétrique **60 GHz**,
- Cette bande est beaucoup plus attractive que les 2,4 et 5 GHz traditionnels, plusieurs normes à 60 GHz ont émergé tels que l'**IEEE 802.11ad et ay**,
- Par conséquent, la bande millimétrique, fonctionnant entre 57 et 66 GHz, est avant tout un choix pour l'avenir, car elle permet des transmissions de plusieurs Gigabit/s.
- Le débit peut aller jusqu'à 6,8 Gbit/s en utilisant l'OFDM.

## Caractéristiques de la bande 60

- Bande sans licence,
- Cette plage de 60 GHz permet des bandes passantes de canal plus élevées pour un débit plus élevé.
- La petite longueur d'onde (env. 5 mm) permet d'utiliser des antennes ou des réseaux d'antennes compacts et compétitifs (par exemple pour **la formation de faisceaux**),
- La formation de faisceaux peut être utilisée pour concentrer la puissance sur le récepteur.
- Cependant, étant donné que la transmission a généralement lieu dans une portée limitée de **moins de 10 m**, le degré élevé d'atténuation peut également être considéré comme un avantage.
- L'interférence des transmissions adjacentes est très peu probable et la transmission est très difficile à intercepter, ce qui la rend encore plus sécurisés.

## Le WIGIG

- L'IEEE **802.11-ad** appelé aussi WIGIG (Wireless Gigabit Alliance) peut se considérer comme la première norme exploitant la fréquence 60 GHz, en utilisant la communication directionnelle ou la formation de faisceaux (**Beamforming**) sur une large bande passante (2160MHz).



## Les défis de la bande autour de 60 GHz

- La forte atténuation en espace libre,
- couverture radio limitée à de faibles distances (une pièce)
- L'absorption de l'oxygène : La fréquence des signaux aux alentours de 60 GHz correspond à une fréquence de résonance de l'oxygène. Il en résulte une atténuation linéique d'environ 15 dB/km en plus des pertes dues à la propagation en espace libre.

Fréquence (GHz)	Atténuation en espace libre (dB)
2.4	60.04
5	66.42
60	88

## Les défis de la bande autour de 60 GHz

- Le WiGig ne peut pas traverser les murs, en effet, sa portée ne dépasse pas 10mètres et le signal ne doit rencontrer aucun obstacle, qu'il s'agisse d'objets, d'un mur ou même d'un corps humain.
- Le WiGig ne viendra donc **pas remplacer** le Wi-Fi dans une installation domestique mais plutôt le **compléter** pour les applications nécessitant une bande passante importante.
- Lorsque vous vous éloignez de la pièce principale, le protocole peut **basculer** pour utiliser les autres bandes inférieures à un débit beaucoup plus faible, qui peuvent toutes deux se propager à travers les murs.

## La bande de fréquences libre

Sur cette bande, il n'est pas nécessaire d'obtenir une licence d'utilisation, mais des limitations sur la puissance d'émission sont imposées.

Pays	Bande (GHz)	Puissance émise (dBm)
USA/Canada	57-64	27 max
Japon	59-66	10 max
Corée	57-64	10 max
Australie	59,4-62,9	10 max
Europe	57-66	13 max

## Les canaux

- La bande passante nominale du canal est de 2,16 GHz.
- La bande ISM utile autour de 60 GHz (57 GHz à 66 GHz) est réglementée différemment selon les régions du monde.
- Six canaux sont définis pour cette bande, mais ils ne sont pas universellement disponibles.
- Le canal 2 est disponible dans toutes les régions et est donc utilisé comme canal par défaut.

Canal	Fréquence
1	58.32 GHz
2	60.48 GHz
3	62.64 GHz
4	64.80 GHz
5	66.96 GHz
6	69.12 GHz

# Systèmes de communication en bande millimétrique

Afin de pouvoir concevoir un système de communication en bande millimétrique, capable de communiquer avec succès malgré tous les défis plusieurs techniques peuvent être utilisées, principalement :

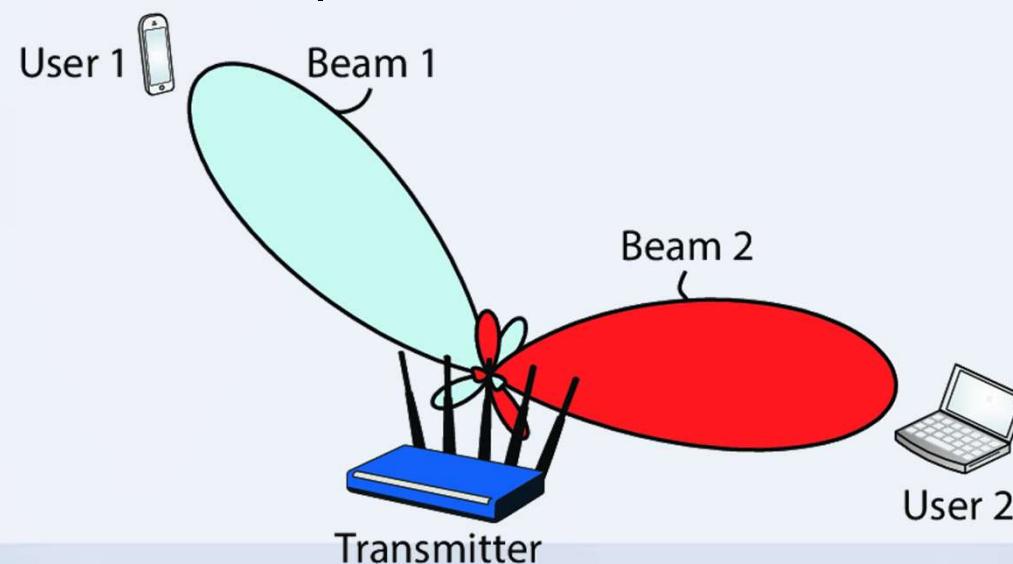
**Le Beamforming** : ou bien la technique de formation des faisceaux, utilisés pour surmonter les pertes de trajets élevées, en utilisant au moins un réseau d'antennes.

Cette technique est appliquée en focalisant le signal transmis vers le récepteur (**direct path**) ou vers le meilleur trajet indirect (**best indirect path**) arrivant lorsque le trajet direct est obstrué,

**Le Massive MIMO** : est un concept basé sur l'utilisation d'un grand nombre d'antennes en émission et en réception, capable d'améliorer considérablement l'efficacité spectrale sans aucun supplément de bande passante ni de consommation de puissance.

# Beamforming

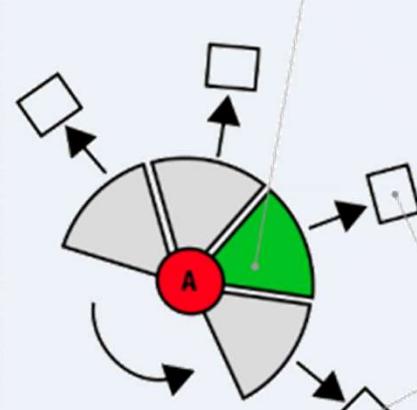
- La communication directionnelle consiste à concentrer l'énergie de l'onde électromagnétique dans une direction donnée.
- Par conséquent, pour faire communiquer deux nœuds à travers un lien directionnel, on doit aligner leurs secteurs d'émission et de réception afin de maximiser le SNR de la liaison.
- Ce mécanisme consiste en une collaboration entre les deux nœuds communicants afin de déterminer le meilleur secteur d'émission ou de réception



# Beamforming

Beamforming pour l'émission  
(TXSS)

secteur de transmission optimal

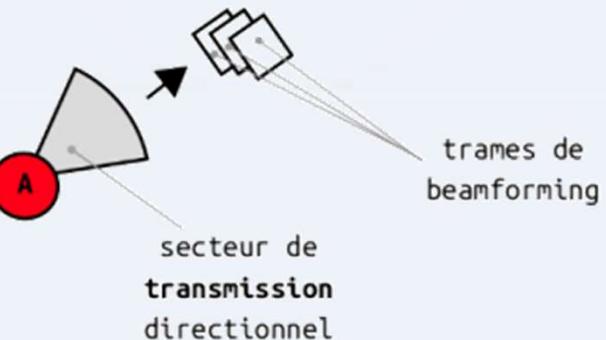


secteur de réception quasi-omnidirectionnel

trames de beamforming

Beamforming pour la réception  
(RXSS)

secteur de réception optimal



trames de beamforming

secteur de transmission directionnel

## Produit WIGIG

- En 2017, l'entreprise TP Link a annoncé la sortie du premier routeur WiFi **tri-bande** 2,4/5/60 GHz, le TP Link Talon AD7200 .
- Ce produit devrait être le premier routeur à embarquer la technologie IEEE 802.11ad.
- Cette nouvelle norme permet d'atteindre des vitesses de 4,6 Gbit/s, soit une vitesse 4 fois supérieure aux routeurs les plus rapides utilisant la norme IEEE 802.11ac

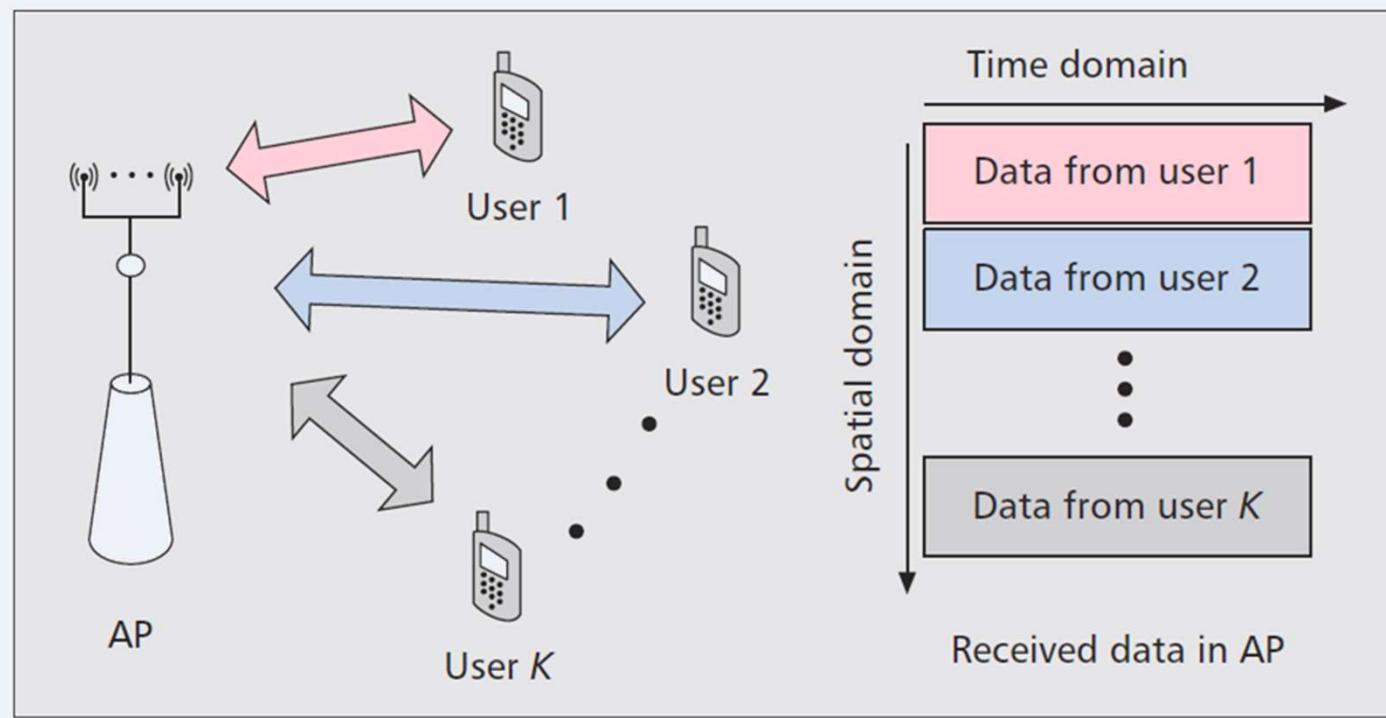


## Le MIMO

- Au début le MIMO était appliqué entre un point d'accès et un terminal à la fois, mais en développant les algorithmes et les technologies d'accès aux supports, comme le beamforming, on a pu garantir des accès MIMO pour plusieurs utilisateurs simultanés. On l'appelle MU-MIMO.
- On distingue aussi 2 variantes de MIMO selon le nombre d'utilisateurs recevant simultanément des données sur les mêmes porteuses :
- Le SU-MIMO (*Single User*), le plus courant, permet d'envoyer des données via les différentes antennes vers un seul utilisateur à un instant donné ; il impose d'avoir plusieurs antennes dans chaque récepteur. Ce mode permet d'atteindre un débit unitaire crête plus élevé...

# Le MIMO

- Le MU-MIMO (*Multi User*) permet de partager le débit radio et d'émettre des flux de données vers 2 (ou plusieurs) utilisateurs,
- Il utilise le mode « multiplexage spatial » et permet d'augmenter l'efficacité spectrale de la cellule radio sans imposer un nombre élevé d'antennes dans chaque terminal.



# **Normes et Protocoles**

## **Chapitre 04 P.2**

Les protocoles des réseaux sans fil  
et des réseaux mobiles

# Les protocoles 802.15



ZigBee® Bluetooth®

# **Le protocole 802.15.1 Bluetooth Classique**

# Qu'est-ce que Bluetooth (IEEE 802.15.1) ?

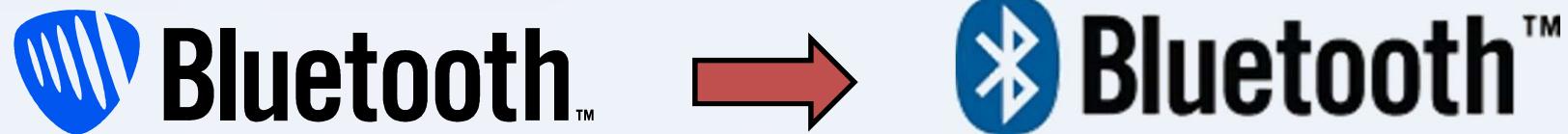
Le Bluetooth est une technologie de **réseau personnel sans fil** (noté **WPAN** pour **Wireless Personnel Area Network**), c'est-à-dire une technologie de réseaux sans fil à **faible portée** (quelques dizaines de mètres).

L'origine de l'appellation est inspiré du surnom du roi viking danois Harald « **Dent bleue** » qui aurait unifié les différents royaumes nordiques à la fin du Moyen Âge.



## Début de Bluetooth

Il a été mise au point par **Ericsson en 1994**. En 1998, un groupe nommé Bluetooth **SIG (Special Interest Group)** réunissais plus de 2000 entreprises a été formé afin de produire les spécifications **Bluetooth 1.0**, en juillet **1999**.



# L'évolution du Bluetooth

- 1999 : sortie de la spécification 1.0, puis 1.0B utilisant une modulation GFSK (Gaussian FSK),
- 2004 : publication de la norme Bluetooth 2.0 et du mode **EDR** (Enhanced Data Rate) qui permet un meilleur débit avec les QPSK et 8DPSK,
- 2006 : le SIG annonce la commercialisation de produits compatibles avec Bluetooth 2.0 (puis 2.1 en 2007)
- 2009 : le Bluetooth SIG publie la norme Bluetooth 3.0 et la variante **HS** (*High Speed*) (très peu utilisée),
- 2010 : apparition du Bluetooth 4.0 plus performant et moins gourmand en énergie : il intègre la variante Bluetooth à basse consommation (connue sous le nom de *Bluetooth Low Energy (BLE)*)
- décembre 2013 : sortie de la version 4.1,
- décembre 2014 : sortie de la version 4.2,
- décembre 2016 : publication de la version 5,
- janvier 2019 : présentation de la norme 5.1,
- décembre 2019 : publication de la norme 5.2.
- Juillet 2021 : publication de la norme 5.3

# L'évolution du Bluetooth

Version Bluetooth	Parution	Débitmax.	Principales améliorations
Bluetooth 1.0a	Juillet 1999	732,2 kbit/s	Première version officielle
Bluetooth 1.0b	Décembre 1999	732,2 kbit/s	Améliorations générales
Bluetooth 1.1	Février 2001	732,2 kbit/s	Correction de problèmes de connexion et de sécurité ; première version pour produits commercialisables ; cryptage ; jusqu'à sept connexions simultanées
Bluetooth 1.2	Novembre 2003	1 Mbit/s	Rétrocompatibilité avec Bluetooth 1.1 ; moins sensible aux interférences grâce au AFH (Adaptive Frequency Hopping)
Bluetooth 2.0 + EDR	Novembre 2004	2,1 Mbit/s	Débit triplé grâce à l'EDR (Enhanced Data Rate) ; différentes procédures d'économie d'énergie ; utilisation complémentaire de la NFC (Near Field Communication) lors de l'appairage
Bluetooth 2.1 + EDR	Août 2007	2,1 Mbit/s	Connexion automatique sans PIN grâce au Secure Simple Pairing
Bluetooth 3.0 + HS	Avril 2009	24 Mbit/s	Canal « highspeed » (HS) supplémentaire basé sur le Wi-Fi et l'UWB (Ultra Large Bande)

# L'évolution du Bluetooth

<b>Bluetooth 4.0 LE (ou : Bluetooth smart)</b>	Décembre 2009	24 Mbit/s	Pile de protocoles Low Energy (LE) pour différentes procédures basse consommation (par ex. profil GATT) pour les petits appareils ; amélioration de la correction des erreurs ; Cryptage 128 bits
<b>Bluetooth 4.1</b>	Décembre 2013	25 Mbit/s	Les appareils plus petits n'ont plus besoin d'intermédiaire ; IPv6
<b>Bluetooth 4.2</b>	Décembre 2014	25 Mbit/s	Améliorations générales
<b>Bluetooth 5</b>	Décembre 2016	50 Mbit/s	Nette augmentation de la portée et du débit

## Description

Le Bluetooth a pour principal objectif de **remplacer les câbles**. Les principales caractéristiques de la technologie Bluetooth sont les suivantes :

- **faible coût** ;
- faible puissance d'émission, d'où une **courte distance d'émission (10 m)**;
- **faible consommation d'énergie** (adapté aux produits portables) ;
- topologie de **réseau ad hoc** ;
- configurable dynamiquement ;
- support des transferts voix et données ;
- destiné à un **usage personnel** (PAN : Personal Area Network) ;
- Échange bidirectionnel utilisant des ondes radio UHF...

## La portée

La **portée** dépend : de la **puissance d'émission** ; de la **qualité de l'antenne** et de l'**environnement** (obstacles, interférences...).

La puissance d'émission permise pour un équipement Bluetooth classique est réglementée sous 3 classes :

Classe	Puissance (affaiblissement)	Portée
I	100 mW (20 dBm)	100 m
II	2,5 mW (4 dBm)	15-20 m
III	1 mW (0 dBm)	10 m

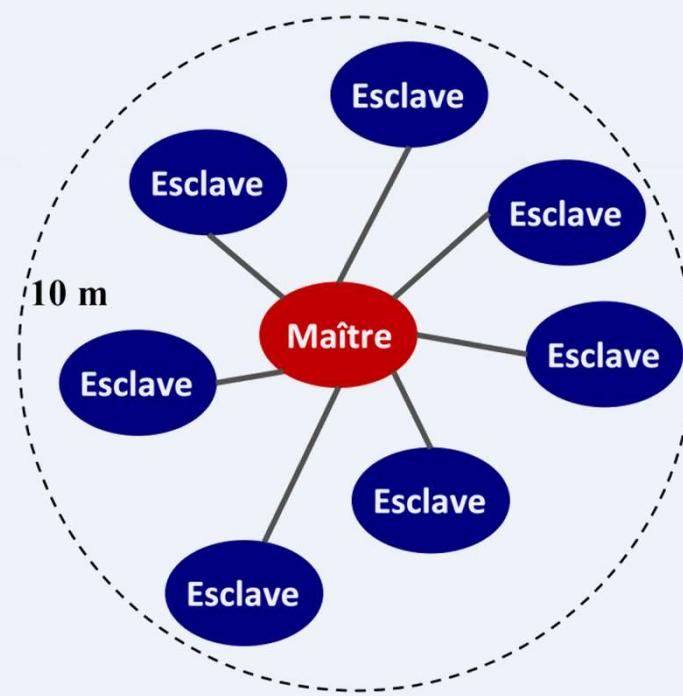
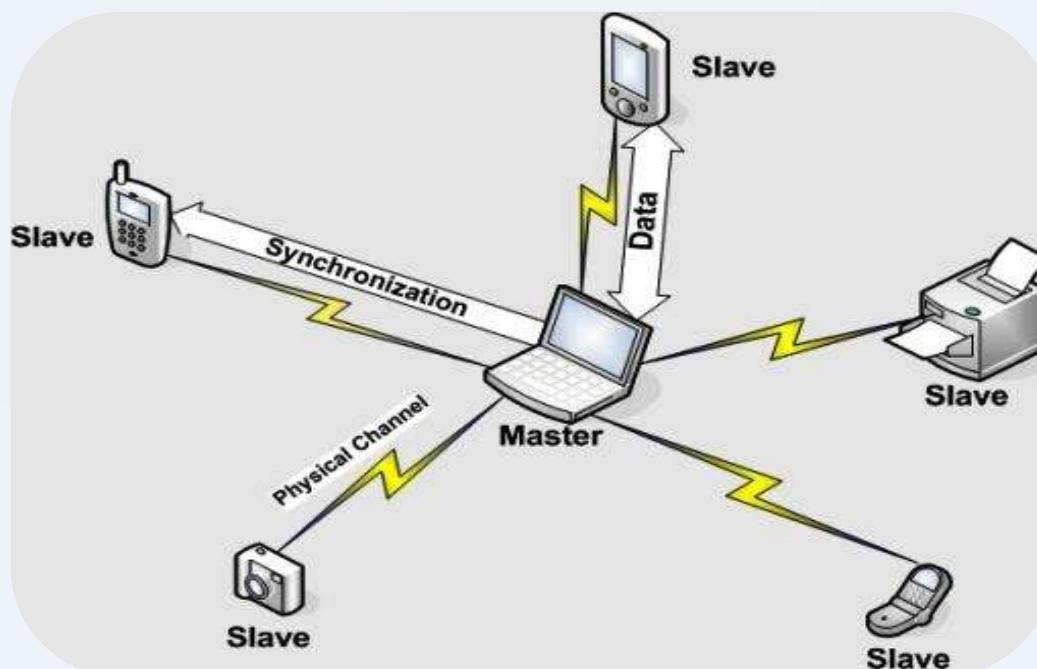
À noter que les distances sont mesurées en champ libre c'est à dire sans obstacle entre l'émetteur et le récepteur.

La plupart des fabricants d'appareils électroniques utilisent des modules de classe 2 .

# Topologie des réseaux Bluetooth

## 1- Les « piconets »

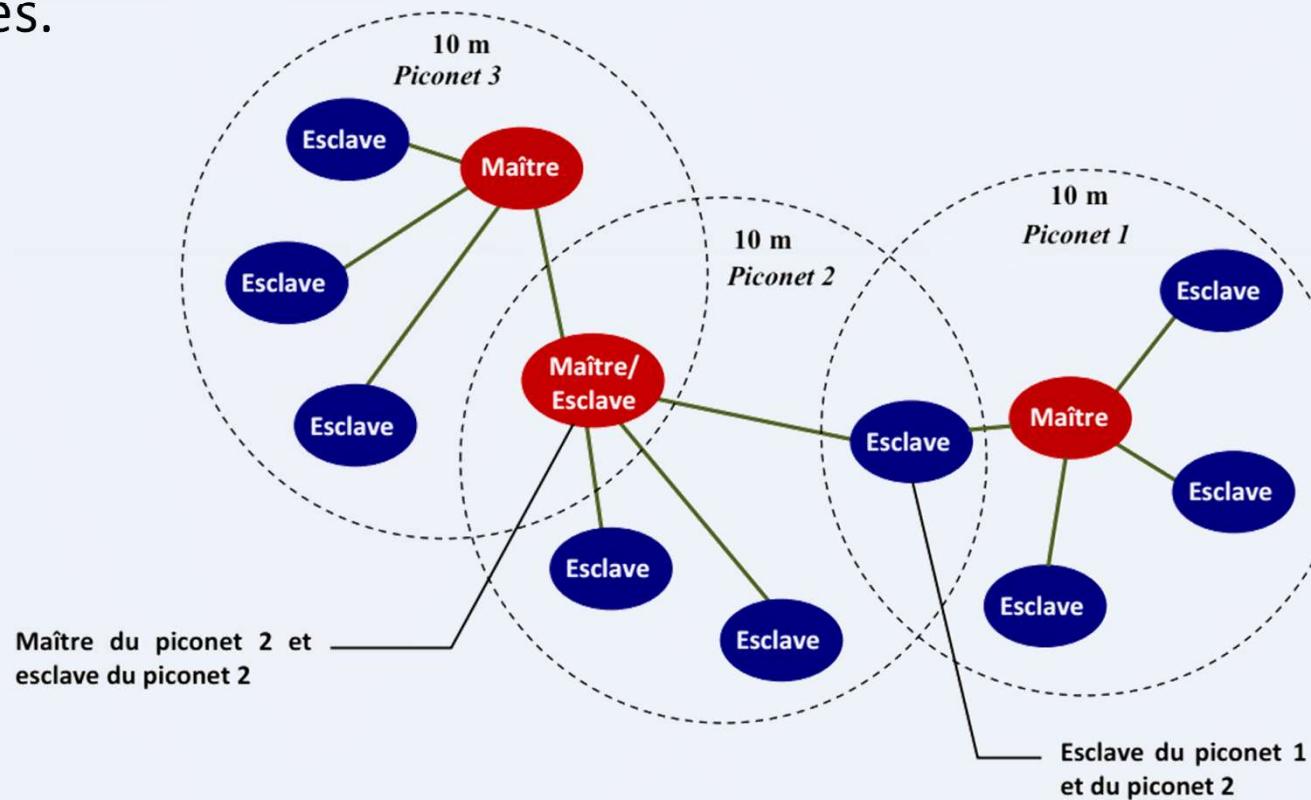
Un « **piconet, picoréseau**» est un réseau qui se compose de plusieurs périphériques dans un même rayon . Il suit une topologie en étoile. Il est constitué **d'un maître et 7 esclaves actifs au maximum** (possèdent une adresse logique de 3 bits).



# Topologie des réseaux Bluetooth

## 2- Les Scatternets

Un réseau **chaîné** « **scatternet** » est une **interconnexion de plusieurs « piconets »** (10 au maximum). Ces interconnexions sont possibles car les périphériques esclaves peuvent avoir plusieurs maîtres.



## Connexion entre périphériques

L'établissement d'une connexion entre deux périphériques passe par plusieurs étapes permettant d'assurer un certain niveau de sécurité :

- Phase d'inquisition (inquiry)
- Synchronisation avec le point d'accès (paging)
- Découverte des services du point d'accès
- Création d'un canal avec le point d'accès
- Pairage à l'aide d'un code PIN
- Utilisation du réseau

## Etablissement des connexions

- 1- L'établissement de la connexion commence par **la phase d'inquisition** » ( « inquiry »), pendant laquelle le périphérique maître envoie une requête à tous les périphériques présents dans sa portée, appelés **points d'accès**. les périphériques recevant la requête répondent avec leur adresse.
- 2- Le périphérique maître se synchronise avec le point d'accès selon une technique, appelée **paging**, consistant notamment à synchroniser son horloge et sa fréquence avec le point d'accès.
3. Un lien s'établit ensuite avec le point d'accès, permettant au maître d'entamer une phase de **découverte des services** du point d'accès, selon *SDP (Service Discovery Protocol)*.
4. A l'issue de cette phase, le périphérique maître est en mesure de créer un **canal de communication** avec le point d'accès en utilisant le protocole *L2CAP*.

## Etablissement des connexions

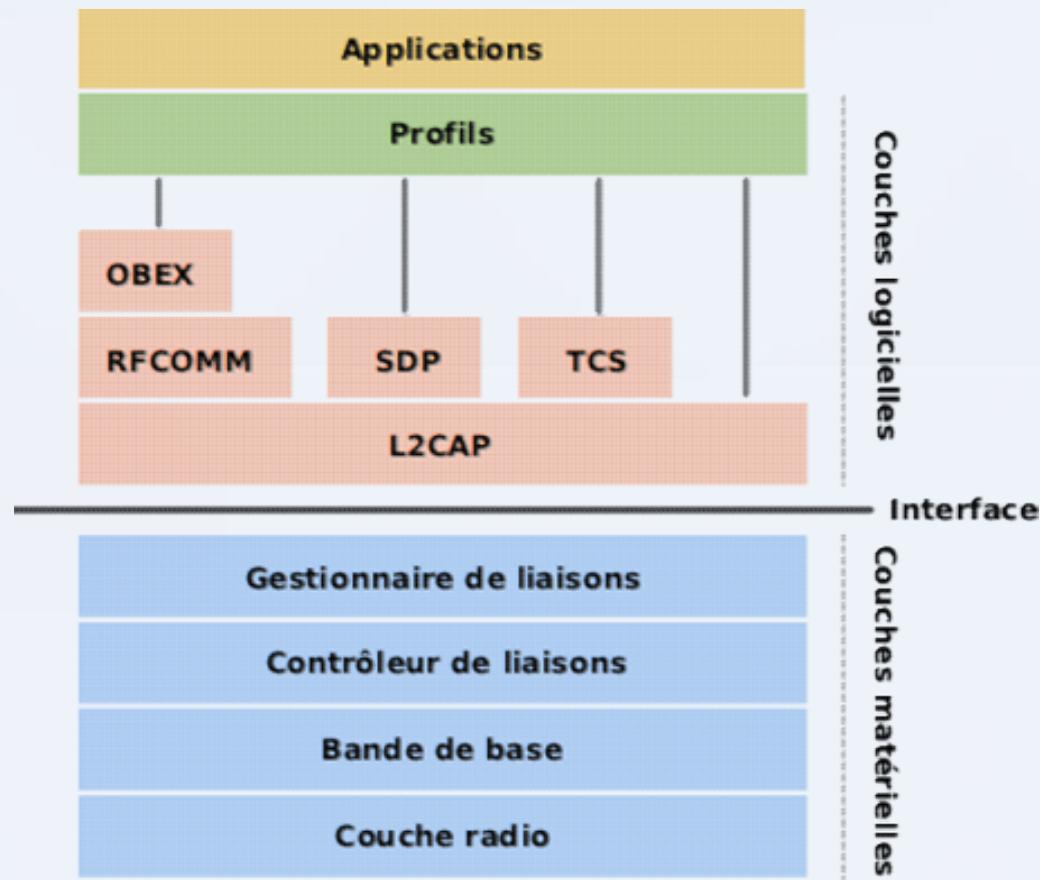
5. Il se peut que le point d'accès intègre un mécanisme de sécurité, appelé **pairage** (en anglais *pairing*), permettant de restreindre l'accès aux seuls utilisateurs autorisés afin de garantir un certain niveau d'étanchéité du picoréseau.
  - Le pairage se fait à l'aide d'une clé de chiffrement communément appelée « code PIN » (*PIN* signifie *Personal Information Number*).
  - Le point d'accès envoie ainsi une requête de pairage au périphérique maître. Ceci peut la plupart du temps déclencher une intervention de l'utilisateur pour saisir le code PIN du point d'accès. Si le code PIN reçu est correct, l'association a lieu.
6. Lorsque le pairage est effectif, le périphérique maître est libre d'utiliser le canal de communication ainsi établi !

## Etablissement des connexions

- Les appareils souhaitant entrer dans le picoréseau recherchent un signal en mode « scan » toutes les 2,56 secondes,
- Une appareil « appairé » est enregistré dans une liste et se connecte toujours automatiquement dès qu'il se trouve à portée du picoréseau, à condition que le Bluetooth soit activé.
- Le code **PIN** (généralement à quatre chiffres) est affiché sur l'écran de l'appareil esclave ou indiqué dans le manuel correspondant. Ce processus appelé « attribution des clés » sert à sécuriser l'accès contre des tiers et est généralement effectué **une seule fois**.
- Un appareil compatible Bluetooth peut être connecté simultanément dans plusieurs picoréseaux en tant qu'esclave, mais dans un seul en tant que maître.

# Architecture en couches

Bluetooth propose un modèle architectural qui comprend un empilement de protocoles au sens du modèle OSI,



## La couche radio

- C'est elle qui s'occupe de l'émission et de la réception des ondes radio. Elle définit les caractéristiques telles que la bande de fréquence et l'arrangement des canaux, les caractéristiques du transmetteur, de la modulation, du récepteur,
- Pour le Bluetooth classique, il opère dans les bande de fréquence **ISM (Industrial, Scientific and Medical)** 2,4 GHz, ne nécessite pas de licence, comprise entre **2 400 et 2 483,5 MHz**. au même titre que le WIFI et d'autres systèmes comme Zigbee.

## La couche radio

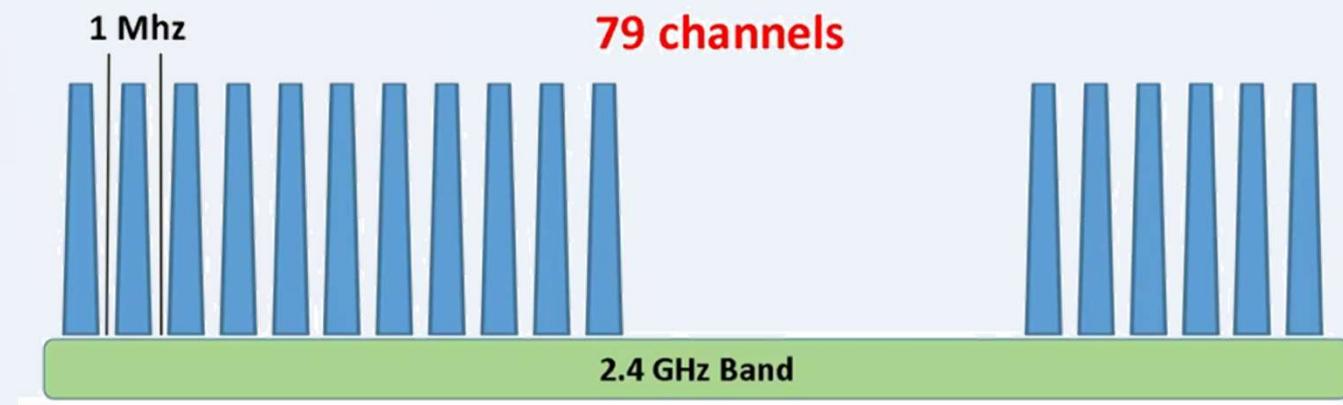
- La bande ISM des 2,4 GHz est **très perturbée**. Il est nécessaire de protéger la transmission radio contre les brouillages par une technique d'**étalement de spectre**.
- Le Bluetooth utilise la technique **FHSS (Frequency Hopping Spread Spectrum )** (étalement de spectre par saut de fréquence). Permet de découper la bande en **79 canaux**, de **1MHz**. En changeant le canal **1600 fois/s**, pour limiter l'atténuation et les interférences avec des autres modules radio.
- Chaque transmission Bluetooth **utilise les 79 canaux** et occupe la bande dans sa totalité (environ **80 MHz**)

## Bandes et canaux

Le principe du FHSS est la commutation rapide entre plusieurs canaux de fréquence, utilisant un **ordre pseudo aléatoire** connu tant à l'émetteur qu'au récepteur pour la synchronisation.

L'utilisation de FHSS dans Bluetooth permet :

- Une synchronisation parfaite entre l'émetteur et le récepteur ;
- D'émettre simultanément, les fréquences sont ainsi partageables.
- De limiter les interférences (collisions) car les fréquences ne sont plus polluées, plus la sécurité.

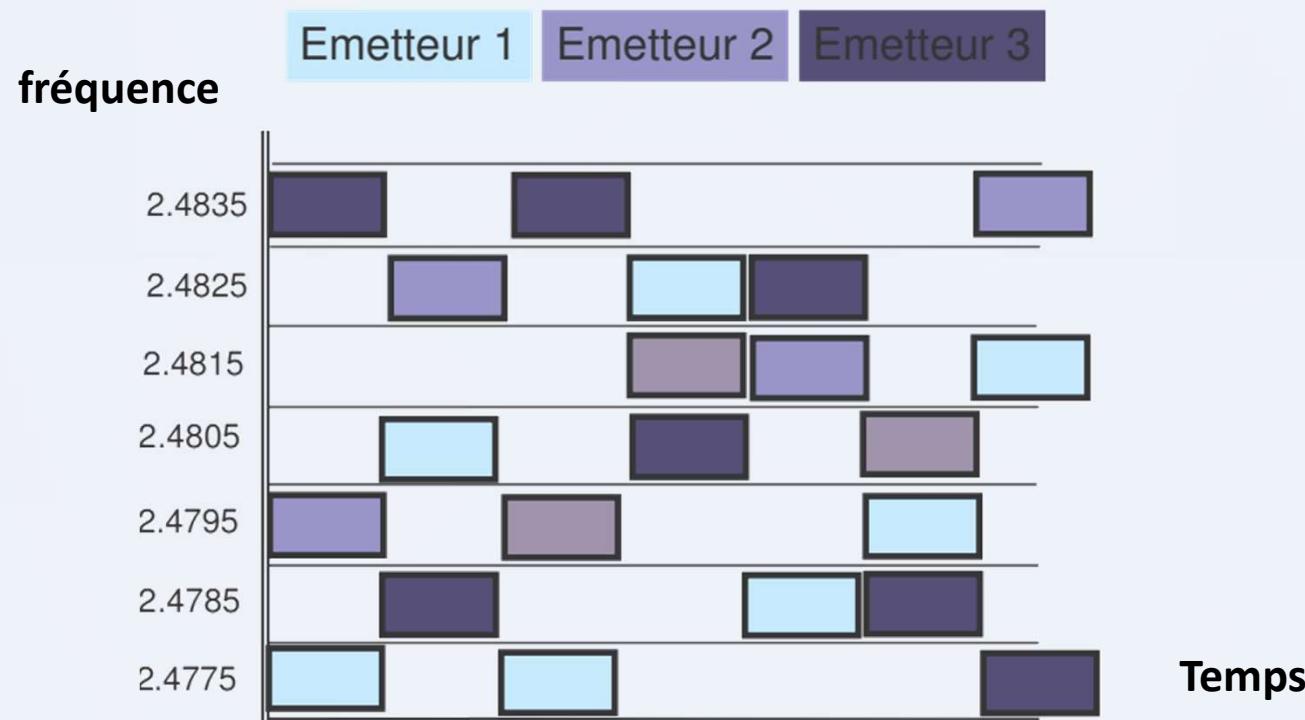


## Bandes et canaux

- Chaque équipement découpe les données à transmettre en courts paquets, un paquet étant transmis dans un slot.
- Un duplexage temporel TDD (Time Division Duplex) est employé pour permettre les transmissions bidirectionnelles, où le maître transmet pendant un slot et un esclave pendant le slot suivant.
- Dans la version 1.0, le saut de fréquences se fait, pour une liaison établie sur les 79 fréquences disponibles.
- La version 1.2 du SIG Bluetooth introduit la technique AFH (Adaptive Frequency Hopping), il n'utilise qu'un sous-ensemble de fréquences (minimum 20).
- C'est le maître qui décide quelles sont les fréquences à utiliser, en fonction des informations dont il dispose sur l'occupation des canaux .

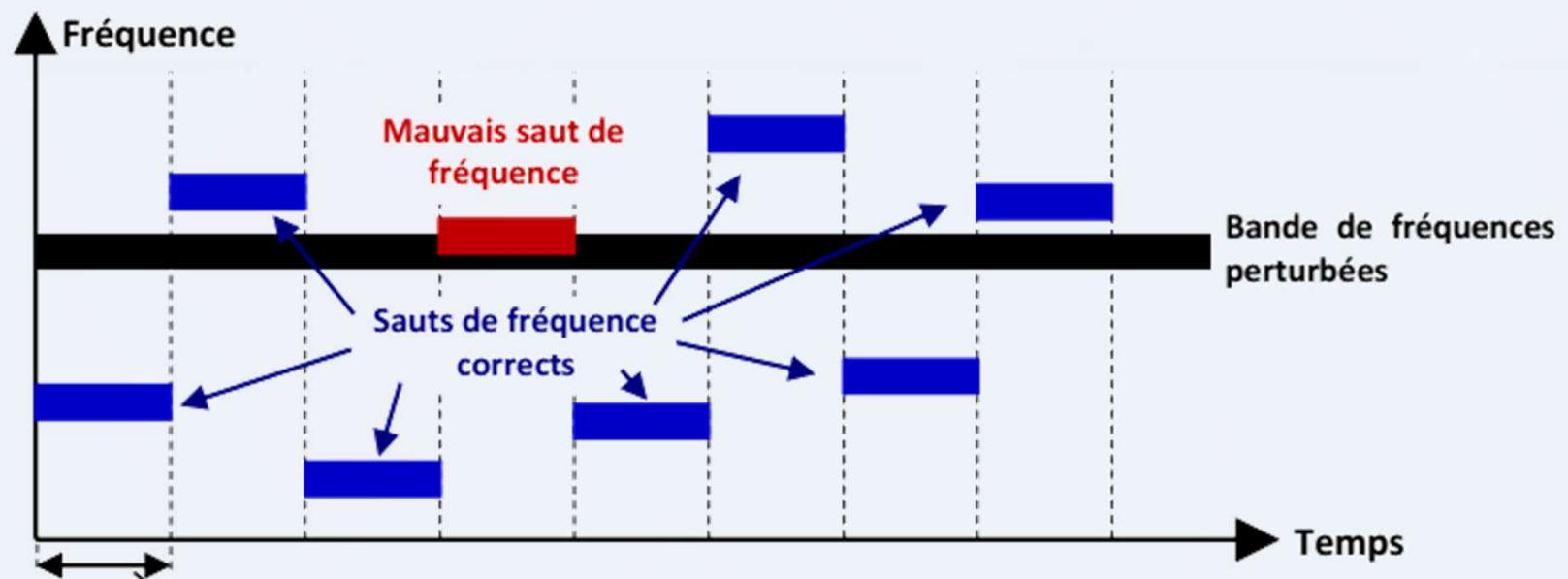
## Bandes et canaux

Comme on le remarque sur ce diagramme, 3 équipements Bluetooth peuvent émettre simultanément en utilisant les différents canaux de la bande de fréquence.



## Bandes et canaux

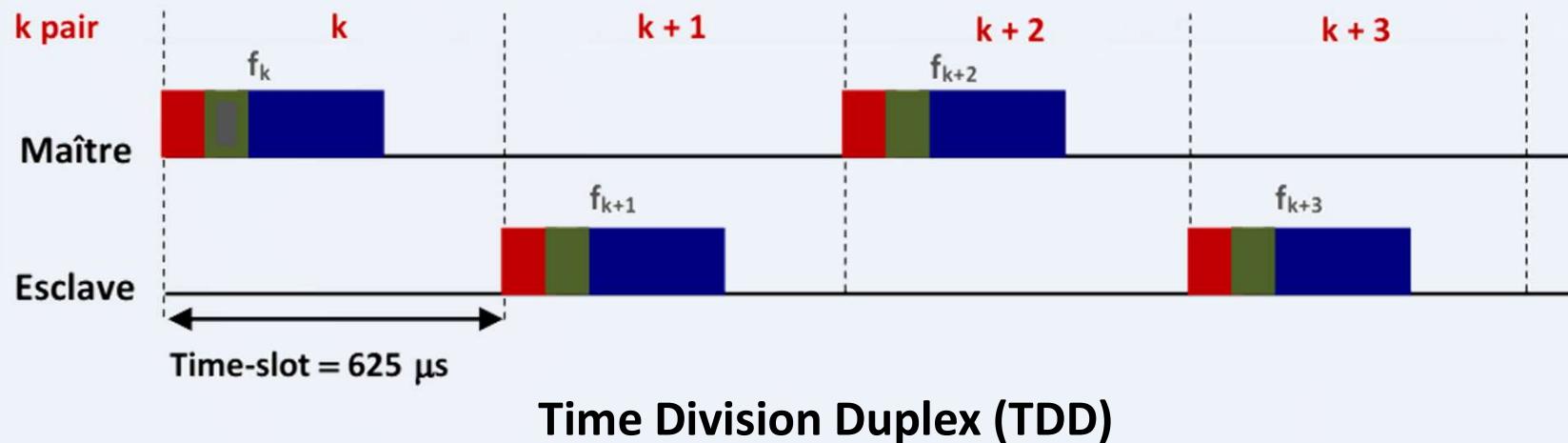
- L'information est transmise sur une fréquence pendant un **time-slot** puis l'émetteur passe sur la fréquence suivante ;
- Les sauts en fréquence (période de 625 µs.).
- Les sauts de fréquence sont aussi connus par le récepteur.
- Chaque réseau « piconet » utilise une succession de fréquences différentes.



# Les échanges de données

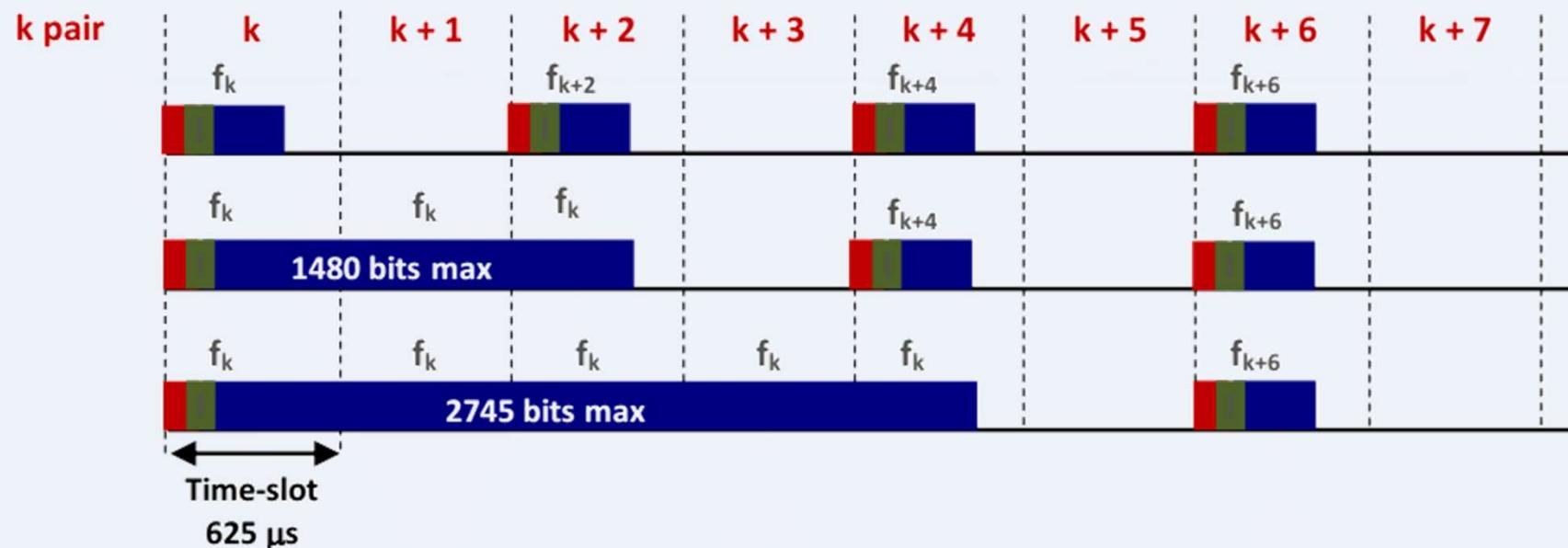
Les échanges de données sont régis par les règles suivantes :

- le **choix des fréquences** se fait selon une séquence **pseudo-aléatoire** définie par le **maître** ;
- le maître émet dans les **time-slots pairs** et l'esclave dans les **time-slots impair**



## Les échanges de données

Il est possible de transmettre des **paquets de données courts** (1 time-slot, 240 bits au maximum), **moyens** (3 time-slot, 1480 bits max) ou **longs** (5 time-slot, 2745 bits max). Dans les 2 derniers cas le saut de fréquence ne se fait pas à la fin du time-slot, mais après transmission du paquet complet.



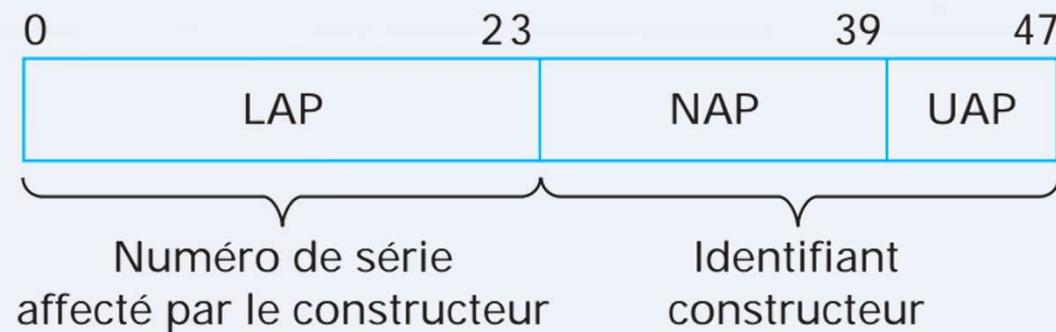
## La couche radio

Pour le Bluetooth classique deux modulations sont définies :

- Une obligatoire utilisant une modulation de fréquence (GFSK) pour minimiser la complexité de l'émetteur, C'est une modulation de fréquences de type FSK à deux états, dont le signal modulant est filtré par un filtre gaussien,
- Bluetooth EDR (Enhanced Data Rate) défini dans la version 2.0 du SIG augmente le débit par un facteur de 2 à 3 grâce à des modulations plus évoluées. Avec la modulation PSK (Phase Shift Keying) de type 4-DQPSK (Differential Quadrature PSK), on dispose de 2 bits par symbole et on multiplie le débit par 2. Avec une modulation 8-DPSK, on dispose de 3 bits par symbole et on multiplie donc le débit par 3.

## La couche bande de base

- C'est au niveau de la bande de base que sont définies les adresses matérielles des périphériques (équivalentes à l'adresse MAC d'une carte réseau).
- Cette adresse est nommée ***BD\_ADDR*** (*Bluetooth Device Address*) et est codée sur 48 bits. Ces adresses sont gérées par la *IEEE Registration Authority*.



## La couche bande de base

- C'est également la bande de base qui gère les différents types de connexions entre les appareils, qui peuvent être synchrones ou asynchrones, sont appelées « Liens Logiques » (*Logical Link*) :
  - ✓ les liens SCO (*Synchronous Connection-Oriented*) ;
  - ✓ les liens ACL (*Asynchronous Connection-Less*).
- La connexion **SCO** est une liaison *point à point*. **Le maître ne peut avoir qu'un seul esclave.** Le maître maintient la connexion en envoyant et recevant des slots à intervalle régulier. Cette connexion est utilisée pour la voix et a un débit de 64 kb/s.
- La connexion **ACL** est une liaison *point à plusieurs point*. Ici, **le maître communique avec tous les esclaves participant au mini réseau.** Cette connexion est utilisée pour le transfert de données. Son débit est de 723.2 kb/s en asymétrique (57.6 kb/s en retour) ou 433.9 kb/s en symétrique.

## La couche bande de base

- Chaque paquet de données est composé globalement de la même manière. On retrouve trois parties essentielles :
  - ✓ Le code d'accès → 72 ou 68 bits ;
  - ✓ L'entête (*Header*) → 54 bits ;
  - ✓ La charge utile (*Payload* = les données utiles) → de 0 à 2 745 bits. (qui peut être un paquet SCO ou ACL)



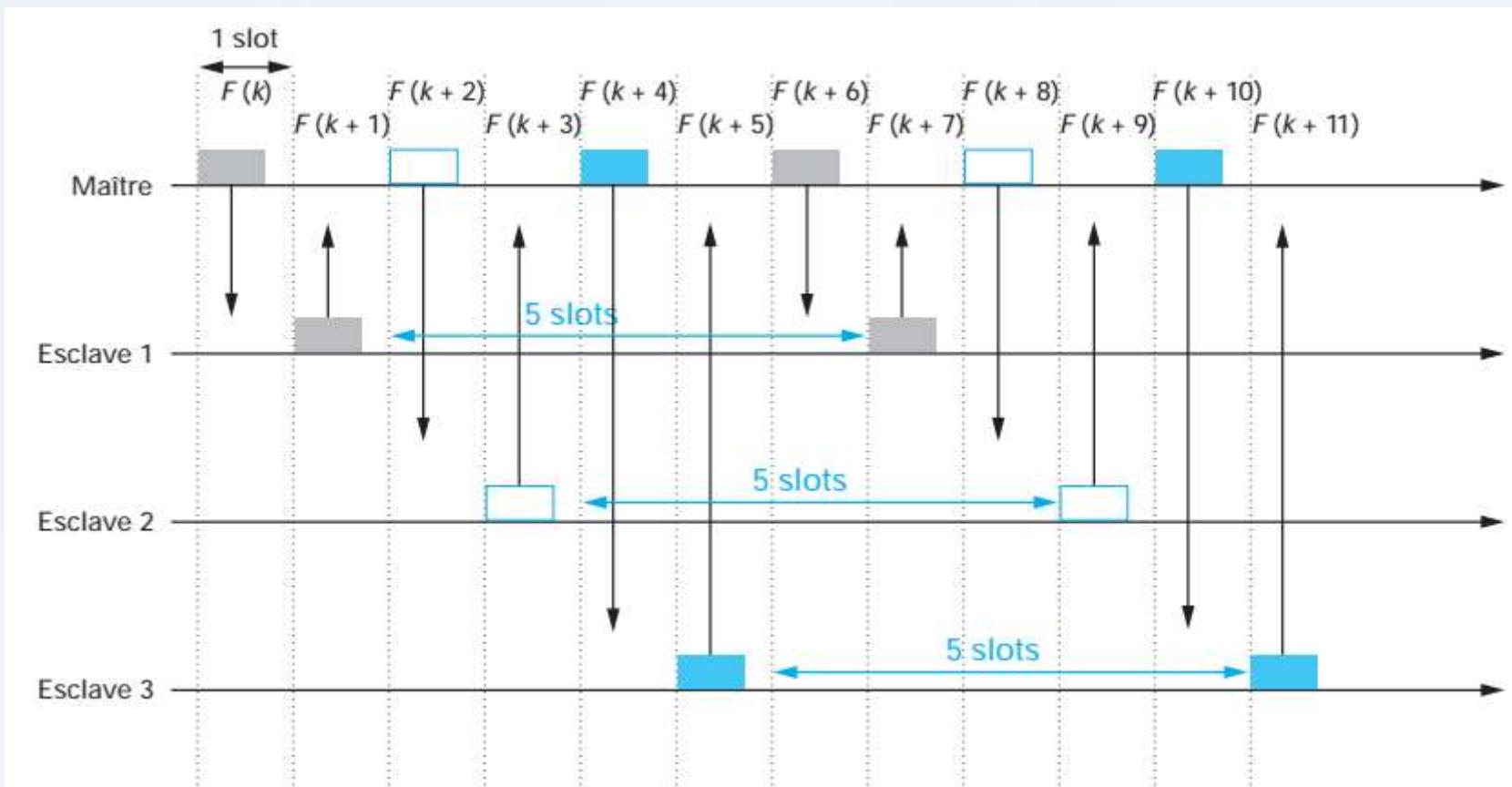
## La couche L2CAP

- La couche L2CAP (*Logical Link Control & Adaptation Protocol*) fournit les services de multiplexage des protocoles de niveau supérieur et la segmentation et le réassemblage des paquets,
- ainsi que le transport des informations de qualité de service.
- Les protocoles de haut niveau peuvent ainsi transmettre et recevoir des paquets jusqu'à 64 Ko. Elle autorise un contrôle de flux par canal de communication.
- La couche L2CAP utilise des canaux logiques.

## RFCOMM et SDP

- RFCOMM : pour « *Radio frequency communication* ». Ce service est basé sur les spécifications RS-232, qui émule des liaisons séries. Il peut notamment servir à faire passer une communication IP par Bluetooth.
- RFCOMM est utilisé lorsque le débit des données n'atteint pas plus de 360 kbit/s (par exemple, téléphones mobiles).
- SDP : pour « Service Discovery Protocol ». Ce protocole permet à un appareil Bluetooth de rechercher d'autres appareils et d'identifier les services disponibles. Il s'agit d'un élément particulièrement complexe de Bluetooth.

Pour éviter des tailles d'en-tête importantes, on utilise une adresse courte codée sur 3 bits appelée AM\_ADDR qui est allouée lors de la constitution du piconet.



# **Le protocole 802.15.1 Bluetooth BLE**

# L'évolution du Bluetooth

Les appareils Bluetooth peuvent être de l'un de ces deux types :

- Single mode – prend en charge : BR/EDR **ou** LE profile
- Dual mode – prend en charge : BR/EDR **et** LE profiles

Low Energy only device



Classic and LE device



## Le Bluetooth Low Energy

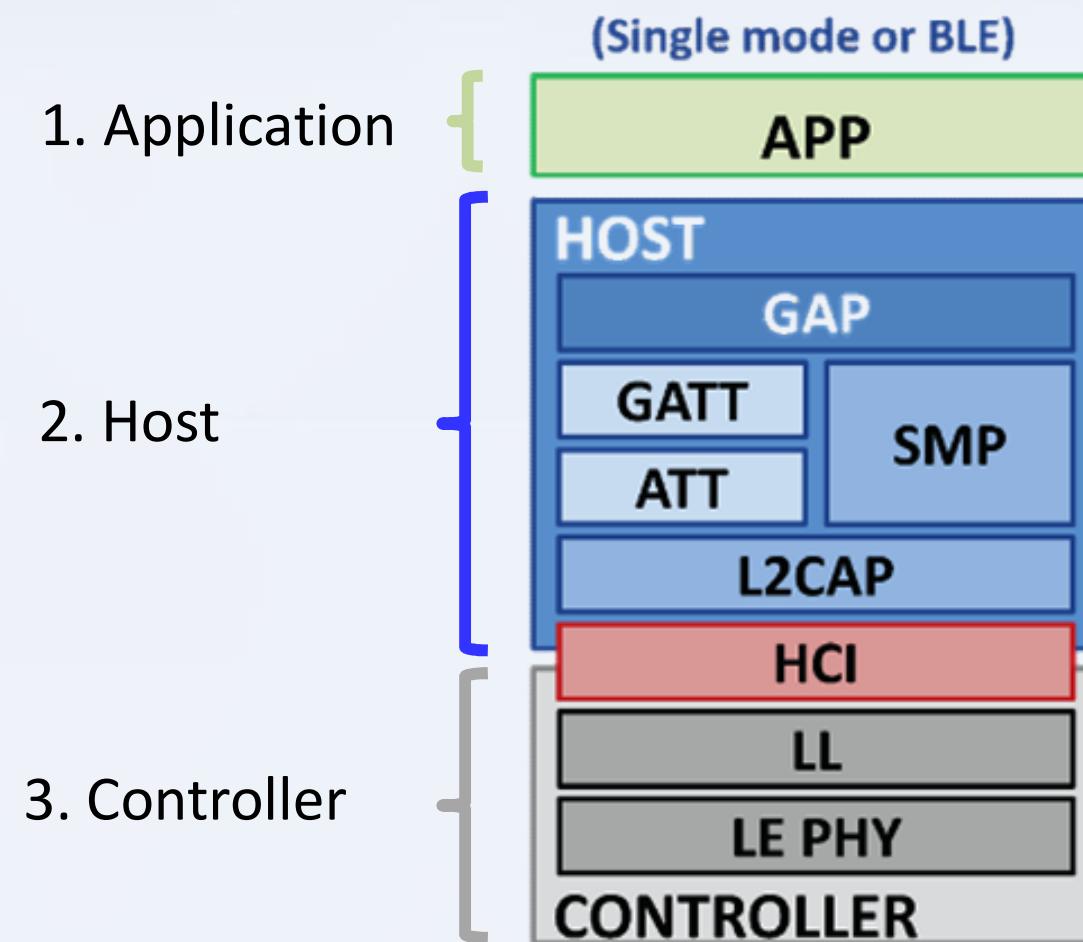
- Après que certains utilisateurs et experts ont parlé du Bluetooth comme d'une « étoile en déclin », la **version 4.0 LE** a fait souffler *un vent de fraîcheur* sur cette technologie.
- Le Bluetooth Low Energy ou Bluetooth smart, a l'origine, il a été conçu par Nokia sous le nom de **Wibree** avant d'être adopté définitivement par le SIG (the Bluetooth Special Interest Group)
- L'atout majeur du Bluetooth Low Energy est **sa faible consommation d'énergie**. Tacile à déployer, utilisé pour le transfert périodique de **petites** quantités de données à courte portée,
- Il est de plus en plus adapté pour tout ce qui a trait à l'Internet des Objets (IoT) qui connaît une forte croissance aujourd'hui.

## Le Bluetooth Low Energy

- La **version 4.1** permet aux petits appareils de communiquer **sans intermédiaire.**, ajout de la compatibilité avec IPv6, qui attribue à chaque appareil IoT compatible Bluetooth une adresse IP propre permettant à son utilisateur de le commander depuis Internet.
- Le **pic technique** a néanmoins été atteint avec la **version** par des paquets plus petits, ainsi qu'une vitesse plus importante, une durée de vie de la batterie accrue et davantage de sécurité.
- Le **Bluetooth 5** se spécialise une fois encore sur les appareils IoT, cette version permettrait une **capacité d'envoi augmentée de 800 pour cent** et une **portée de jusqu'à 200 mètres** (en extérieur) ou 40 mètres (en intérieur) avec une consommation d'énergie toujours aussi faible. Cette version entend également faire progresser le développement des balises **Beacons**,

# Architecture Bluetooth Low Energy

La pile de protocoles BLE est divisée en trois parties :



# Architecture Bluetooth Low Energy

La pile de protocoles BLE est divisée en trois parties :

**1. Application** : responsable de l'interface utilisateur et du traitement des données. Son architecture dépend de l'implémentation.

**2. Host** : est composé de plusieurs couches :

- ✓ Generic Access Profile (GAP),
- ✓ Generic Attribute Profile (GATT),
- ✓ Logical Link Control and Adaptation Protocol (L2CAP),
- ✓ Attribute Protocol (ATT),
- ✓ Security Manager (SM), and
- ✓ Host Controller Interface (HCI) — *Host side*

**1. Controller** : comprend les couches suivantes :

- ✓ Host Controller Interface (HCI) — *Controller side*,
- ✓ Link Layer (LL),
- ✓ Physical Layer (PHY)

## La couche GAP

- La **couche GAP** (*Generic Access Profile*) introduit les différents rôles que peut avoir un objet connecté en BLE : le broadcaster, l'observer, le central et le peripheral.
- Cette couche est celle qui **rend les appareils BLE visibles au monde extérieur** et qui détermine la manière dont deux appareils peuvent (ou pas) interagir.
- Le rôle va être défini par le fabricant, qui va décider la nature de celui-ci en fonction de l'utilisation et les fonctions qu'il souhaite donner à son produit.

## Définition des rôles des objets

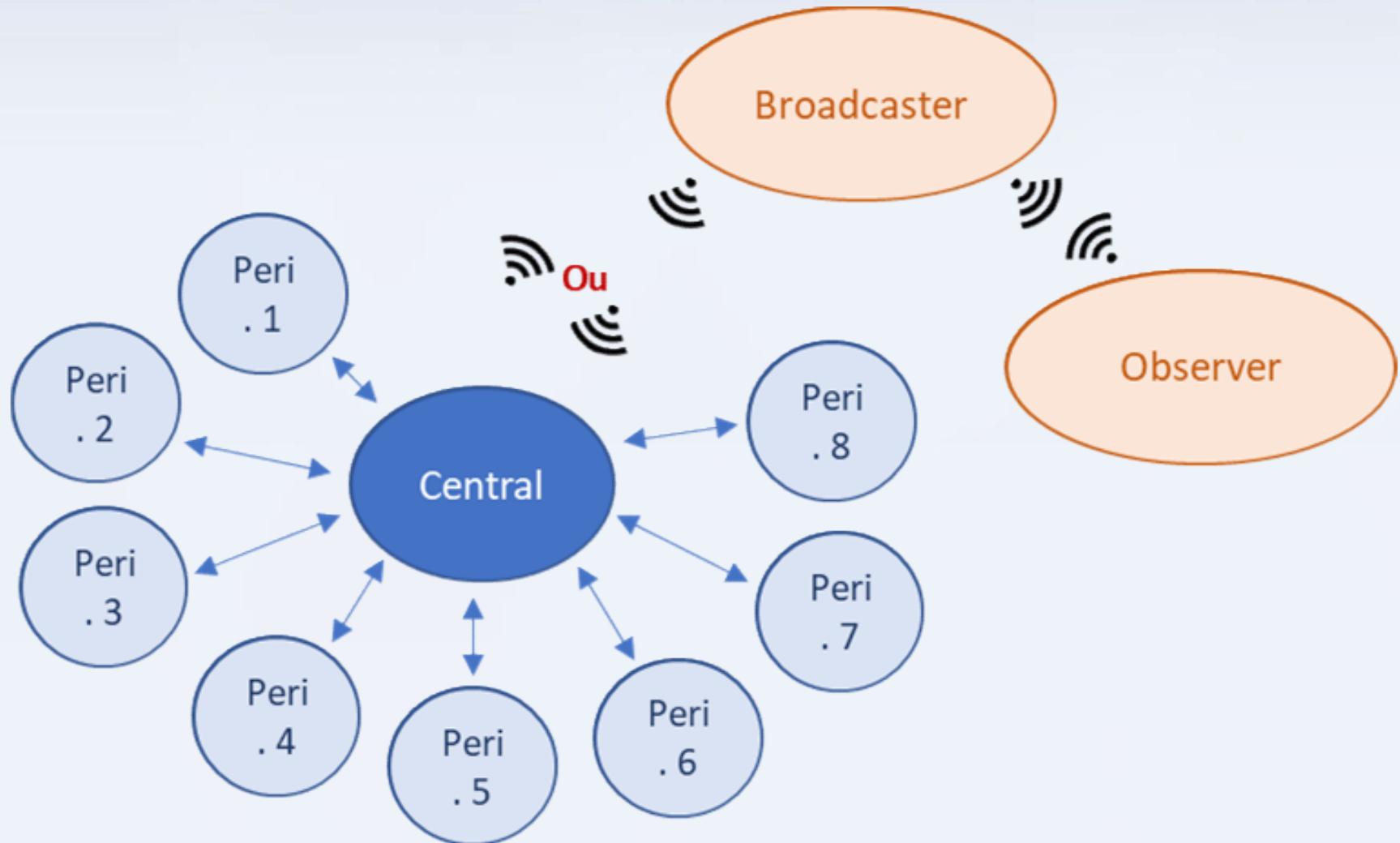
**Le broadcaster** : il peut être utilisé comme serveur. Ainsi, il a pour objectif de transmettre régulièrement des données à un appareil (mode advertising), mais il n'accepte aucune connexion entrante (ne supporte pas le mode « connecté »).

**L'observer / scanner** : l'objet est à l'écoute des broadcaster environnants. Il interprète les données envoyées par le broadcaster et va réagir en conséquence. Il fonctionne en mode advertising et ne supporte pas le mode « connecté ».

**Le central** : Souvent un Smartphone ou une tablette. C'est un élément qui interagit de deux façons différentes : soit en mode advertising, soit en mode connecté. Il est alors le dirigeant et c'est de lui que part l'échange de données.

**Le peripheral** : il va accepter toutes les connexions du central et lui transmettre des données de façon périodique. Il supporte donc le mode « connecté ».

# Définition des rôles des objets BLE



## Les couches GATT et ATT : relation client serveur

- La **couche GATT** (*Generic Attribute Profile*) est une **méthode de présentation des données** utilisée par les périphériques BLE.
- Ce protocole utilise des concepts de « **services et caractéristiques** » utilisés pour décrire l'information échangée :
  - ✓ Un service peut contenir une collection de caractéristiques
  - ✓ Une caractéristique contient une description, une valeur et des informations permettant de définir la valeur.
- Cette méthode se base sur la **relation client/serveur**, où l'objet connecté joue le rôle du **serveur** qui propose ses services au terminal (smartphone, ordinateur et autres passerelles) qui viendra se connecter dessus en tant que client.
- L'objet connecté va émettre périodiquement une trame pour signaler sa présence au « **client** » à proximité.

## La couche LL

- La **couche Link Layer (LL)** introduit les modes « **maître** » et « **esclave** ». Le « central » va jouer le rôle de « maître » et les périphériques vont jouer le rôle « d'esclave ».
- Le « maître » peut **donner un ordre**, envoyer une commande à un ou plusieurs « esclaves », alors que les périphériques, les « esclaves », vont pouvoir se connecter à un seul « maître » à la fois.



GATT Client  
GAP Central  
Master



GATT Serveur  
GAP Peripheral  
Slave

## Advertising et mode connecté

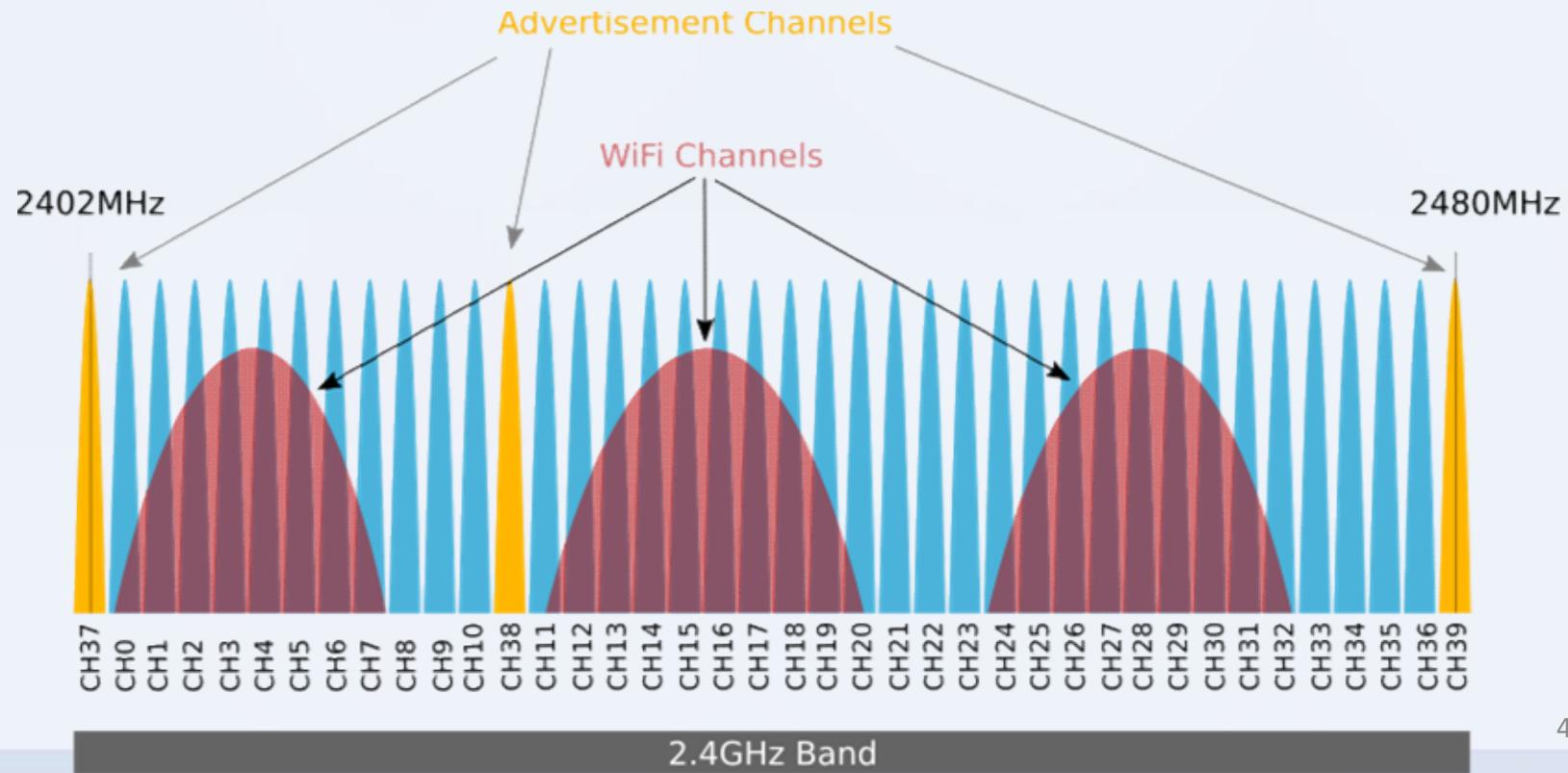
- Les appareils Bluetooth envoient des paquets pour broadcaster les données : c'est l'Advertising.
- Ceux-ci sont des blocs de 31 octets pouvant contenir des informations propres à l'émetteur. Ils sont également utilisés pour permettre à d'autres appareils (de type scanner en général) de se connecter à eux.
- Pour information, il y a plusieurs types de paquets d'Advertising permettant à chacun de réaliser différentes fonctionnalités (utilisés pour Advertising Direct ou Indirect avec ou sans possibilité de connexion).
- En BLE deux appareils peuvent établir une connexion sur un principe de maître / esclave. C'est le mode connecté. Dans ce cas, le protocole GATT est souvent utilisé pour transmettre les données.

## La couche physique

- Le Bluetooth BLE permet l'échange bidirectionnel de données en utilisant des ondes radio UHF et opère dans la bande 2.4 GHz. 40 canaux physiques sont alloués pour un multiplexage en temps et en fréquence, chacun étant espacés de 2 MHz (c'est à dire de 2.4 GHz à 2.8 GHz).
- Certains canaux sont utilisés pour l'Advertising Bluetooth alors que d'autres seront utilisés pour la partie connexion (mode connecté).
- La modulations GFSK est utilisée,
- la puissance d'émission peut varier de 0,01 mW (-20 dBm) à 10 mW (10 dBm). La modulation utilisée est de type GFSK (*Gaussian FSK*).

## Couche Physique (BLE)

- La bande est découpée en 40 canaux, trois canaux (à savoir 37, 38 et 39 servent de canaux d'advertising primaire) ont été placés sur des bandes peu utilisées par les autres protocoles comme le Wi-Fi. Les 37 canaux restants sont pour la transmission des données, ou en canaux secondaires pour l'advertising.



## Bluetooth classique Vs BLE

- En réalité, ces deux technologies sont utilisées à des fins très différentes. Le Bluetooth classique est employé pour traiter, transférer et échanger de nombreuses données sans interruption (par exemple en audio). Cependant, il consomme rapidement la vie de la batterie et coûte beaucoup plus cher.
- Le BLE, quant à lui, est utilisé pour des applications ne nécessitant pas l'échange de grandes quantités de données et récupère par conséquent des informations relativement légères (comme l'heure ou la température par exemple). Proposant ainsi une connexion non continue, il peut fonctionner sur batterie pendant plusieurs années à un coût inférieur à celui du Bluetooth.

# Bluetooth classique Vs BLE

	<b>Avantages</b>	<b>Inconvénients</b>
<b>Bluetooth classique</b>	<ul style="list-style-type: none"><li>▪ Données en continu, idéal pour le streaming audio par exemple</li><li>▪ Grande quantité de données : musiques, vidéos, photos</li></ul>	<ul style="list-style-type: none"><li>▪ Energivore</li><li>▪ Portée d'émission assez courte : entre 10 et 15 mètres maximum</li></ul>
<b>Bluetooth Low Energy</b>	<ul style="list-style-type: none"><li>▪ Faible consommation d'énergie offrant une très forte autonomie.</li><li>▪ Portée d'émission longue pouvant aller jusqu'à plusieurs centaines de mètres</li><li>▪ Coût d'acquisition compétitif</li></ul>	<ul style="list-style-type: none"><li>▪ Connexion non continue</li><li>▪ Informations relativement légères</li></ul>

## La technologie ZigBee IEEE 802.15.4

Le protocole Zigbee est basé sur le standard déploiement de Réseau personnel sans fil (WPAN) qui sont :

- dense à plus de 65000 nœuds
- avec une portée de l'ordre de 100 mètres
- pour un débit de 250 Kbits/s.

Ces caractéristiques en font aujourd'hui le principal protocole utilisé dans les réseaux de capteurs...



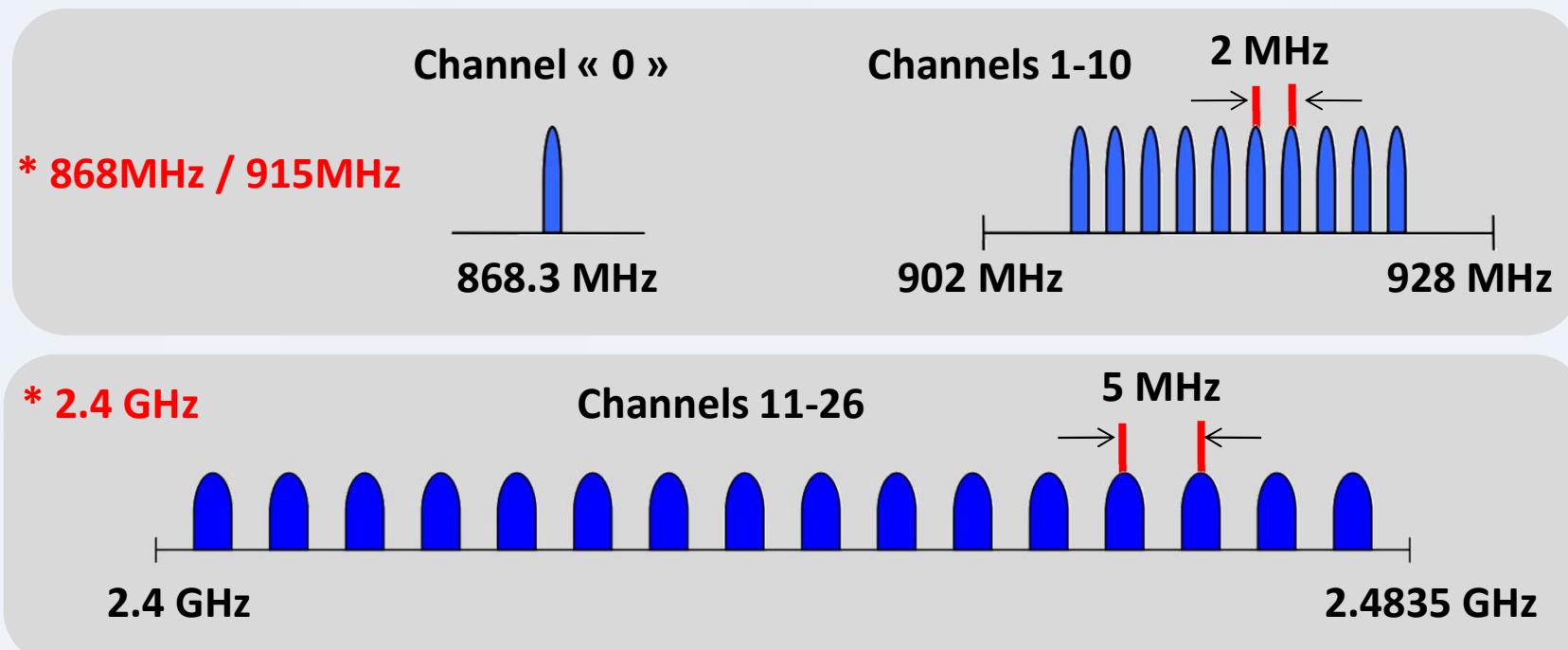
## La technologie ZigBee IEEE 802.15.4

- Destiné aux réseaux sans fil de la famille des LR WPAN (Low Rate Wireless Personal Area Network)
- Grand nombre d'entités communicantes,
- Facilité de déploiement/utilisation,
- Faible coût,
- Très économe en énergie,
- Très économe en ressources matérielles,
- Faible débit ...



# La technologie ZigBee IEEE 802.15.4

- 16 canaux dans la bande 2.4GHz ISM: Industrial, Scientific, Medical
- 10 canaux dans la bande 915MHz ISM
- 1 canal dans la bande 868MHz (en Europe).



## La technologie ZigBee IEEE 802.15.4

- Un réseau IEEE 802.15.4 est composé de :
  - Nœuds FFD (pour ***Full-Function Devices***)
  - Nœuds RFD (pour ***Reduced-Function Devices***).
- Un FFD peut communiquer avec des RFD et des FFD, mais un RFD ne peut communiquer qu'à un seul FFD.
- Un RFD ne peut être qu'une feuille.
- En général, les FFD ont plus de ressources que les RFD...

## Choix de la norme

Le choix d'une technologie de communication sans fil dépend des services proposés, ainsi que des besoins du concepteur du réseau. Certains paramètres comme :

- la consommation d'énergie,
- le débit,
- la durée de vie de la pile,
- la portée et
- le nombre de nœuds supportés...



# Comparaison

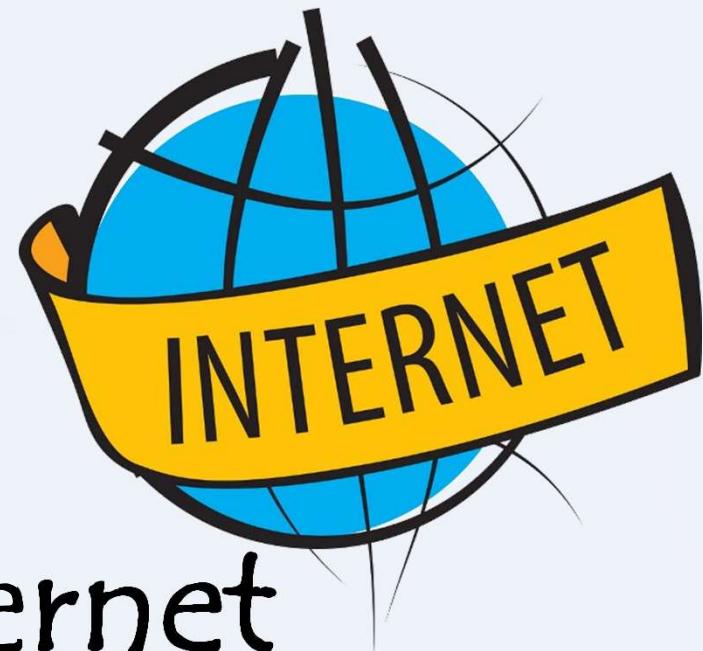
Protocole	Bluetooth	UWB	ZigBee	WiFi	IEEE 802.15.6
<b>Norme IEEE</b>	802.15.1	802.15.3	802.15.4	802.11x	802.15.6
<b>Nombre de nœuds maximum</b>	8	128	65000	32	256
<b>Durée de vie moyenne de la pile</b>	Plusieurs jours	Plusieurs minutes	Plusieurs mois à plusieurs années	Plusieurs minutes à plusieurs heures	---
<b>Débit théorique maximum</b>	Bluetooth Low Energy: 1 Mbit/s Bluetooth 3.0 + High Speed: 3-24 Mbit/s	110-480 Mbit/s	20 Kbit/s (EU), 40 Kbit/s (US) 250 Kbit/s (Global)	11-320 Mbit/s	10 Mbit/s
<b>Bandes de fréquence</b>	2.4 GHz	3.1-10.6 GHz	868 MHz (EU), 915 MHz (US) 2.4 GHz (Global)	2.4 GHz, 5 GHz	---
<b>Portée théorique maximum</b>	10 m	<10 m	10-100 m	10-100 m	5-10 m
<b>Consommation d'Energie</b>	100-200 mW	400 mW pour 200 Mbit/s	30 mW	750-2000 mW	Jusqu'à 50 mW

# *Chapitre V*

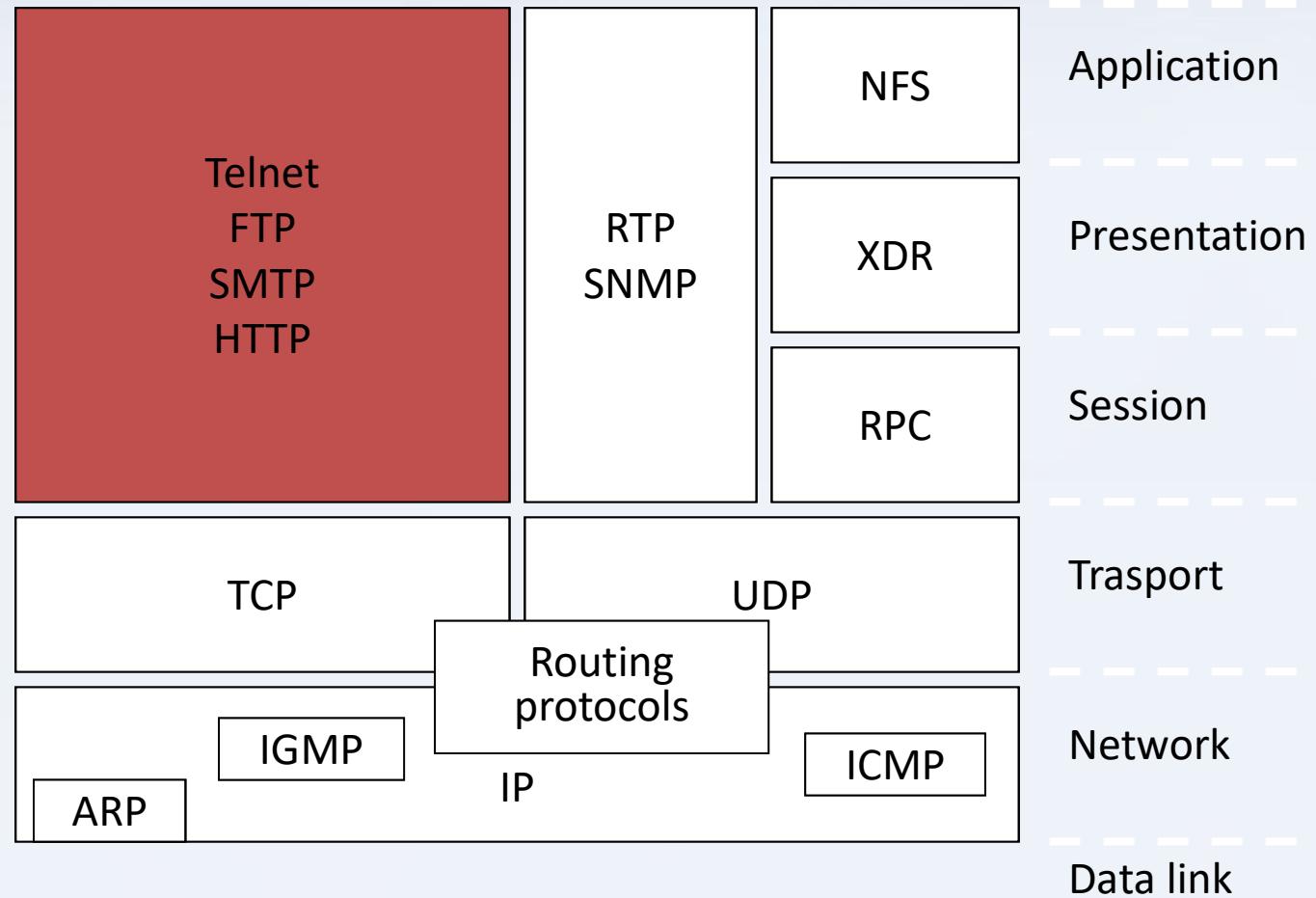
# **Normes et Protocoles**

## **Chapitre 05**

### **Les protocoles Internet**



# L'architecture protocolaire



# Protocoles de couche d'application

Les protocoles de couche d'application importants sont :

- Domain Name Service (DNS)
- Hyper Text Transfer Protocol (HTTP)
- Simple Mail Transfer Protocol (SMTP)
- Post Office Protocol (POP)
- IMAP (Internet Message Access Protocol)
- File Transfer Protocol (FTP)

# Hyper Text Transfer Protocol (HTTP)



# Uniform Resource Locator (URL)

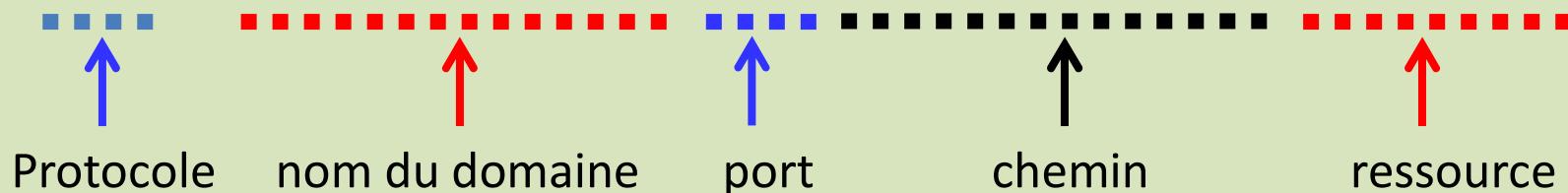
Couramment appelée **adresse web** permet d'identifier une ressource du *World Wide Web* par son **emplacement** et de préciser le **protocole** internet pour la récupérer.

`http://www.mysite.com/folder1/myfiles/index.html`



- L'URL peut également inclure **le port** qui est masqué par le navigateur, mais on peut l'inclure manuellement :

`http://www.mysite.com:8080/folder1/myfiles/index.html`



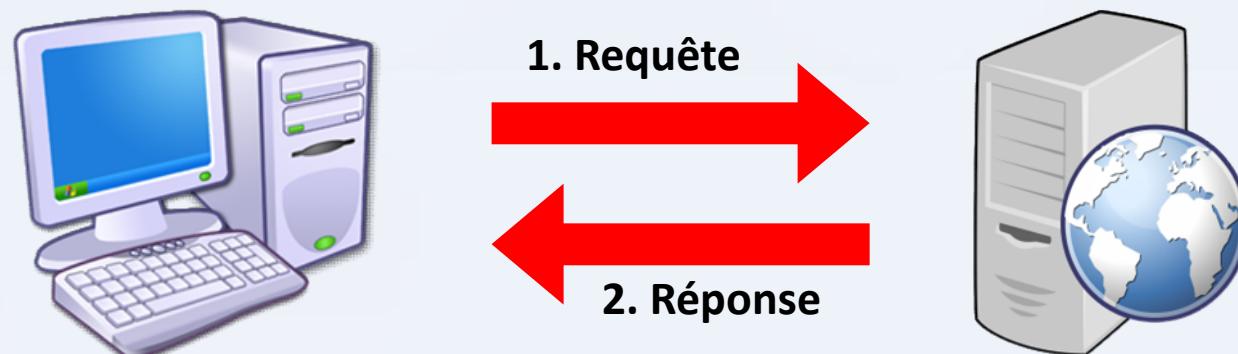
# Le HTTP : Hyper Text Transfer Protocol

- C'est un protocole de communication de la couche application, basé sur TCP/IP,
- Conçu au début des années 90,
- utilisé pour transférer des données sur le Web (fichiers HTML, fichiers image, résultats de requête, etc.) ,
- Le port par défaut est TCP 80, mais d'autres ports peuvent également être utilisés,
- Il fournit un moyen normalisé pour les ordinateurs de communiquer entre eux,
- La spécification HTTP spécifie comment les données de requête des clients seront construites et envoyées au serveur,
- et spécifie comment les serveurs répondent à ces requêtes....

## Modèle client-serveur

HTTP est un protocole client-serveur :

- Les requêtes sont envoyées par un client (navigateur web, ou mandataire en son nom, proxy),
- Une réponse est envoyée par le serveur pour chaque requête.



- Une ressource peut être une page HTML, un fichier CSS, une police, une image ou un fichier avec un code JavaScript.

# Exemple de résultat de requête

The screenshot shows a browser window displaying the homepage of the University of Saida. Below the browser is the developer tools Network tab interface.

**Network Tab Headers:**

- Inspecteur
- Console
- Débogueur
- Éditeur de style
- Réseau (highlighted)

**Filter Options:**

- Filtrer les URL
- Désactiver le cache
- Aucune limitation de la bande passante

**Request Table Headers:**

- Tout
- HTML
- CSS
- JS
- XHR
- Polices
- Images
- Médias
- WS
- Autre

**Request Table Data:**

État	Mét...	Domaine	Fichier	Initiateur	Type	Transfert	Taille
204	POST	www....	collect?v=2&tid=G-1SGCRL1Q57&gtm=2	js:49 (beacon)	plain	566 o	0 o
200	GET	www.univ...	cropped-logo-univ-saida2020-192x192.pi	FaviconLoad...	png	mis en cache	54,6...
200	GET	www.univ...	cropped-logo-univ-saida2020-32x32.png	FaviconLoad...	png	mis en cache	2,61 ...
204	POST	www....	collect?v=2&tid=G-1SGCRL1Q57&gtm=2	js:49 (beacon)	plain	566 o	0 o
200	GET	www.univ...	الرزنامة-البيداغوجية.png	rs6.min.js:37 ...	png	mis en cache	46,2...

**Summary Metrics:**

- 24 requêtes
- 1,23 Mo / 320,60 Ko transférés
- Terminé en : 54,75 s
- DOMContentLoaded: 1,40 s
- load: 1,48 s

# Navigateurs Web

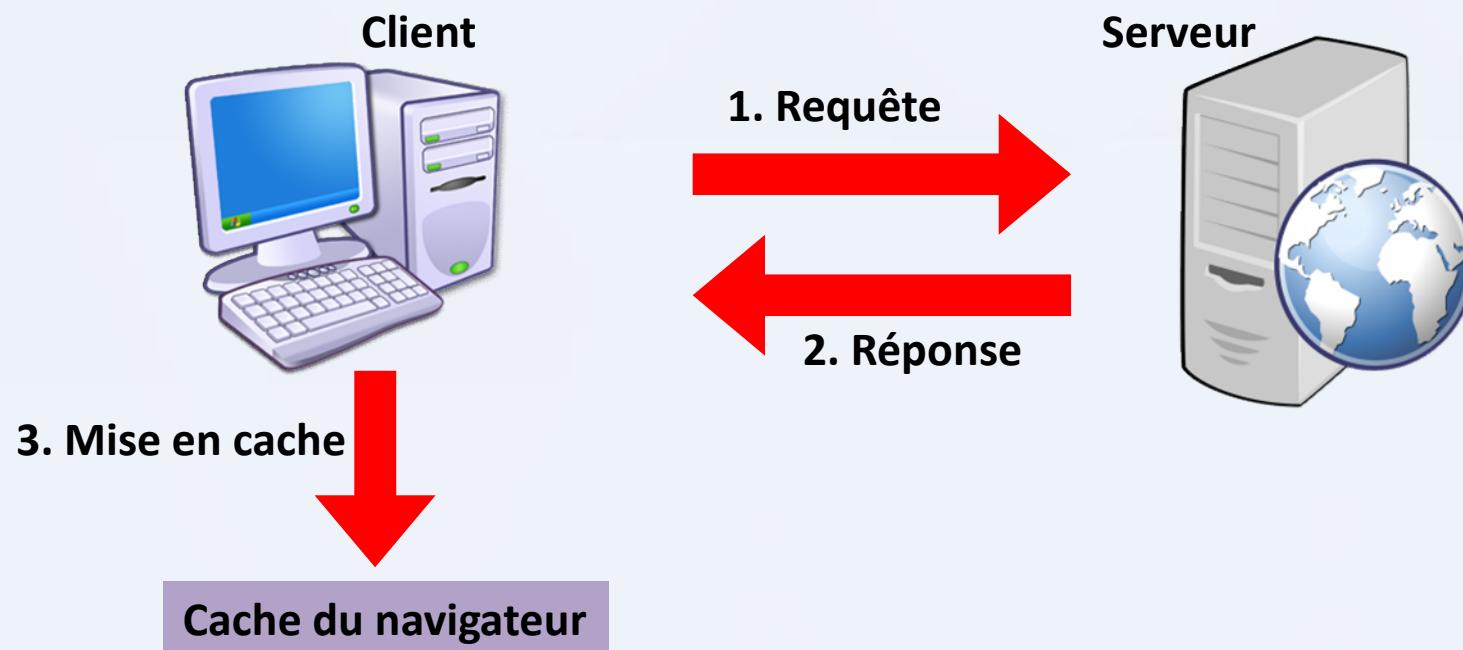
Le client peut être un navigateur web, utilisé pour :

- Visualiser les pages,
- Télécharger par un clic (liens),
- Plusieurs protocoles : HTTP, FTP, SIPn
- Types d'objects : Images, video, Audio...



# Qu'est-ce que le cache ?

- Le cache est un mécanisme qui permet aux pages Web de se charger plus rapidement,
- Certaines ressources sont stockées dans la mémoire du navigateur. Et cette mémoire est appelée cache,
- La mise en cache doit être programmé dans le code.



## Qu'est-ce que le cache ?

- Voici une requête HTTP avec la mise en cache **désactivée**.

82 requests | 622 KB transferred | 2.1 MB resources | Finish: 5.45 s |

- Voici une requête HTTP avec la mise en cache **activée**.

73 requests | 34.8 KB transferred | 2.0 MB resources | Finish: 3.10 s |

- Comme on peut le voir, avec le cache activé, il y a 9 requets de moins et la page se charge 2,35 secondes plus rapidement.

 Remember!!!

**Une requête pour une page HTML peut être suivie par plusieurs requêtes (images, polices....etc.)**



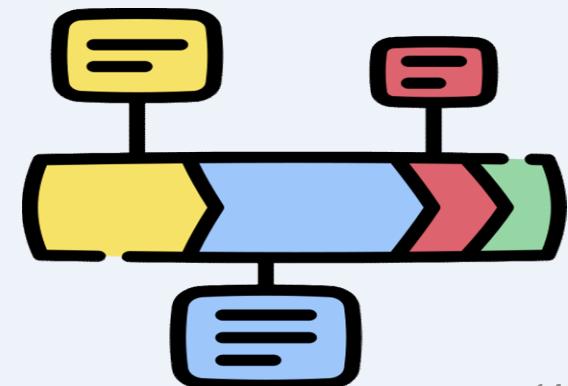
## Caractéristiques de base

Il existe trois fonctionnalités de base qui font de HTTP un protocole simple mais puissant :

- **HTTP est sans connexion** (HTTP/1.0): le client HTTP lance une requête HTTP et après qu'une requête est faite, le client se déconnecte du serveur et attend une réponse.
- **HTTP est indépendant du média** : cela signifie que tout type de données peut être envoyé par HTTP si le client et le serveur savent comment gérer le contenu des données.
- **HTTP est sans état** : HTTP est sans connexion et résulte directement du fait que HTTP est un protocole sans état. Le serveur et le client ne se connaissent que pendant une requête en cours. Après, les deux s'oublient...

## Versions HTTP

- HTTP/0.9 : la première version, n'est plus utilisé, (1991),
- HTTP/1.0 utilise une nouvelle connexion pour chaque échange de requête/réponse, (1996),
- La connexion HTTP/1.1 peut être utilisée pour un ou plusieurs échanges requête/réponse, (1997),
- HTTP/2.0. En février 2015, le groupe de travail HTTP de *l'Internet Engineering Task Force* (IETF) a révisé HTTP et développé la deuxième version...



## Méthodes HTTP

Les méthodes HTTP aident à distinguer les requêtes adressées au serveur, les plus utilisées sont :

- **la méthode GET** : est une requête basique, responsable de l'affichage de la représentation actuelle de la ressource (pages Web ou des formulaires). Les paramètres sont passés dans une adresse URL.
- **la méthode POST**: est utilisée lorsqu'on souhaite ajouter de nouvelles ressources (créer un nouveau compte ou envoyer des fichiers). Les paramètres sont passés dans le corps.
- **la méthode PUT**: est utilisée lorsqu'on souhaite mettre à jour une ressource existante.
- **la méthode DELETE**: est responsable de la suppression des ressources.

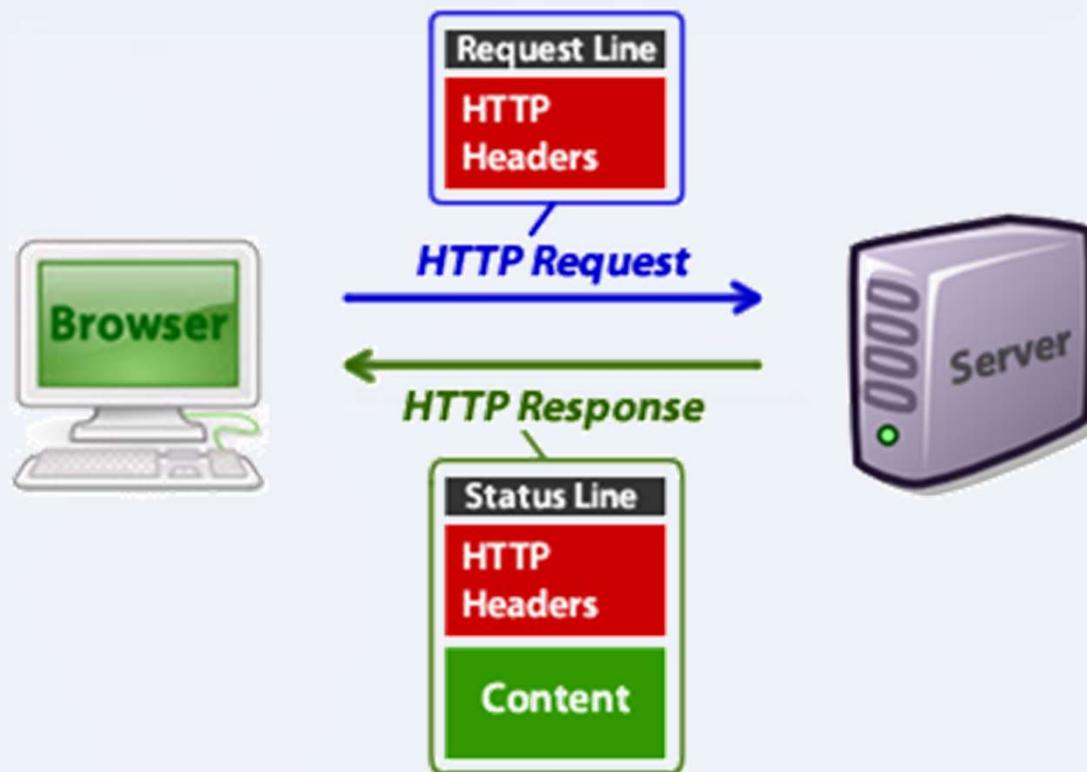
## Les 5 principaux groupes de statuts HTTP

- 1xx : Ce sont des codes informatifs.
- 2xx La demande a été traitée avec succès. **200-ok, 201-created,**
- 3xx : Cela signifie que la demande doit être dirigée vers une autre adresse ou un autre serveur. Par exemple, saisir une ancienne l'URL (**301 – Moved permanently** )
- 4xx : Ceux-ci apparaissent lorsque le problème réside du côté client. Par exemple, vous n'êtes pas autorisé à demander la ressource ou faute dans l'URL (**401 – Unauthorized, 403 – Forbidden, 404 – Not found**)
- 5xx : Codes d'erreur du serveur. Ces codes sont un problème sérieux. Parce que cela peut signifier que quelque chose ne va pas avec le serveur et qu'il ne peut pas traiter la demande du client ( **502 – Bad gateway, 503 – Service unavailable** )

## Format des messages

- Les requêtes HTTP et les réponses HTTP utilisent un format de message générique de RFC 822 pour transférer les données requises.
- Ce format de message générique se compose des quatre éléments suivants :
  - ✓ Une ligne de départ,
  - ✓ Zéro ou plusieurs champs d'en-tête suivis de CRLF,
  - ✓ Une ligne vide (c'est-à-dire une ligne sans rien précédant le CRLF) , indiquant la fin des champs d'en-tête,
  - ✓ En option, un corps de message.

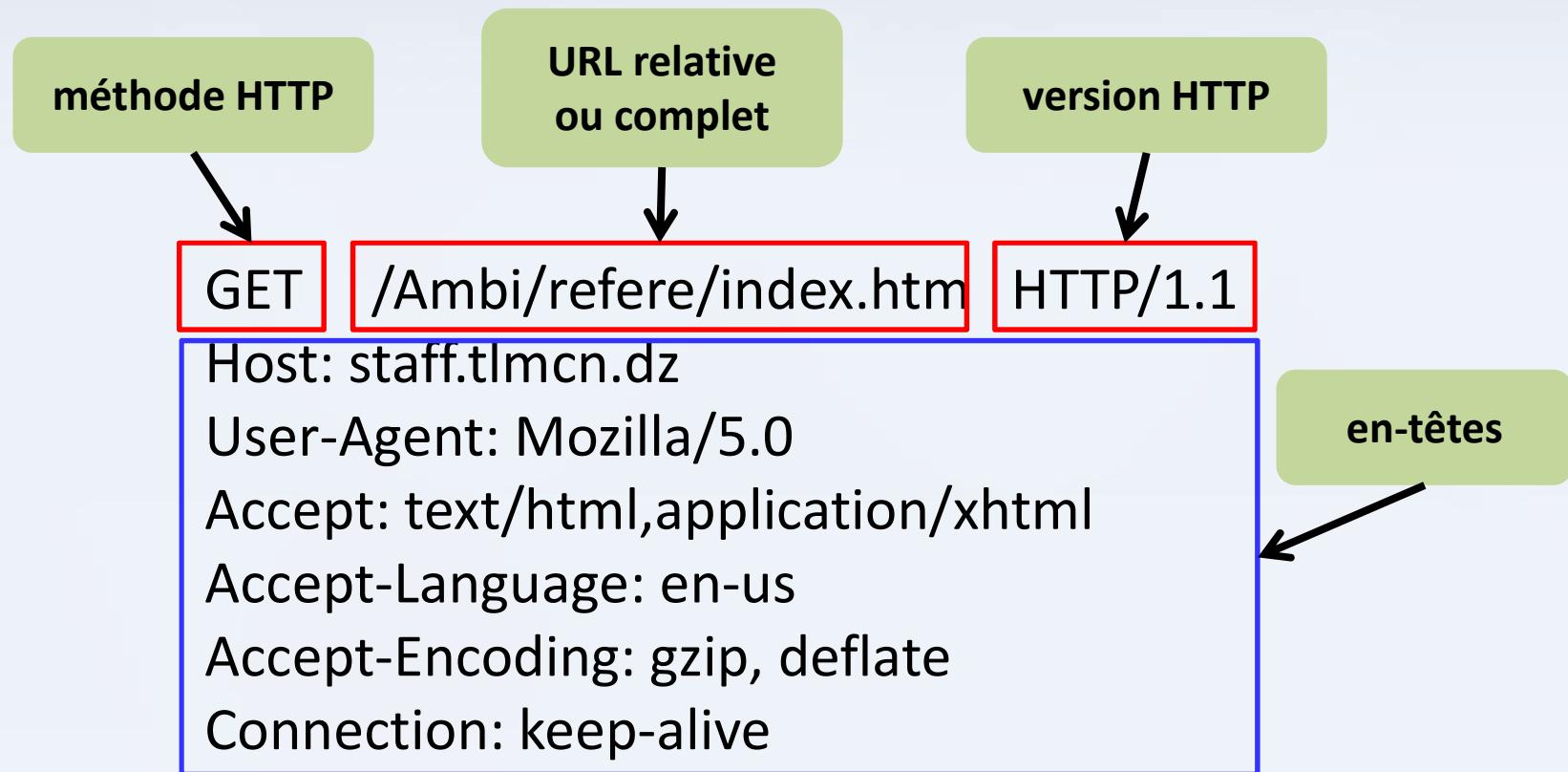
# Format des messages



## La ligne de départ du message HTTP

- Ligne de départ en cas de requête : commence par une **méthode** HTTP, généralement un verbe comme GET, POST, ou un nom comme OPTIONS ou HEAD qui définit l'opération que le client veut effectuer, puis le **chemin** de la ressource à récupérer et la **version** du protocole:  
**GET /hello.htm HTTP/1.1**
- Ligne de départ en cas de réponse : est constituée de la **version** du protocole HTTP qu'ils suivent, un **code d'état**, indiquant si la demande a réussi ou non, et pourquoi, puis un **message d'état**.  
**HTTP/1.1 200 OK**

# Message de requête HTTP



# Message de réponse HTTP

Après avoir reçu et interprété un message de requête, un serveur répond avec un message de réponse HTTP :

```
HTTP/1.1 200 OK
Date: Mon, 27 Jul 2009 12:28:53 GMT
Server: Apache/2.2.14 (Win32)
Last-Modified: Wed, 22 Jul 2009 19:15:56 GMT
Content-Length: 88
Content-Type: text/html
Connection: Closed
<html>

<body>

<h1>Hello, World!</h1>

</body>

</html>
```

# Message de réponse HTTP

**HTTP/1.1 200 OK**

Date: Sun, 08 Feb xxxx 01:11:12 GMT  
Server: Apache/1.3.29 (Win32)  
Last-Modified: Sat, 07 Feb xxxx  
ETag: "0-23-4024c3a5"  
Accept-Ranges: bytes  
Content-Length: 35  
Connection: close  
Content-Type: text/html

<h1>My Home page</h1>

Status Line

Response Headers

Response Message Header

A blank line separates header & body

Response Message Body

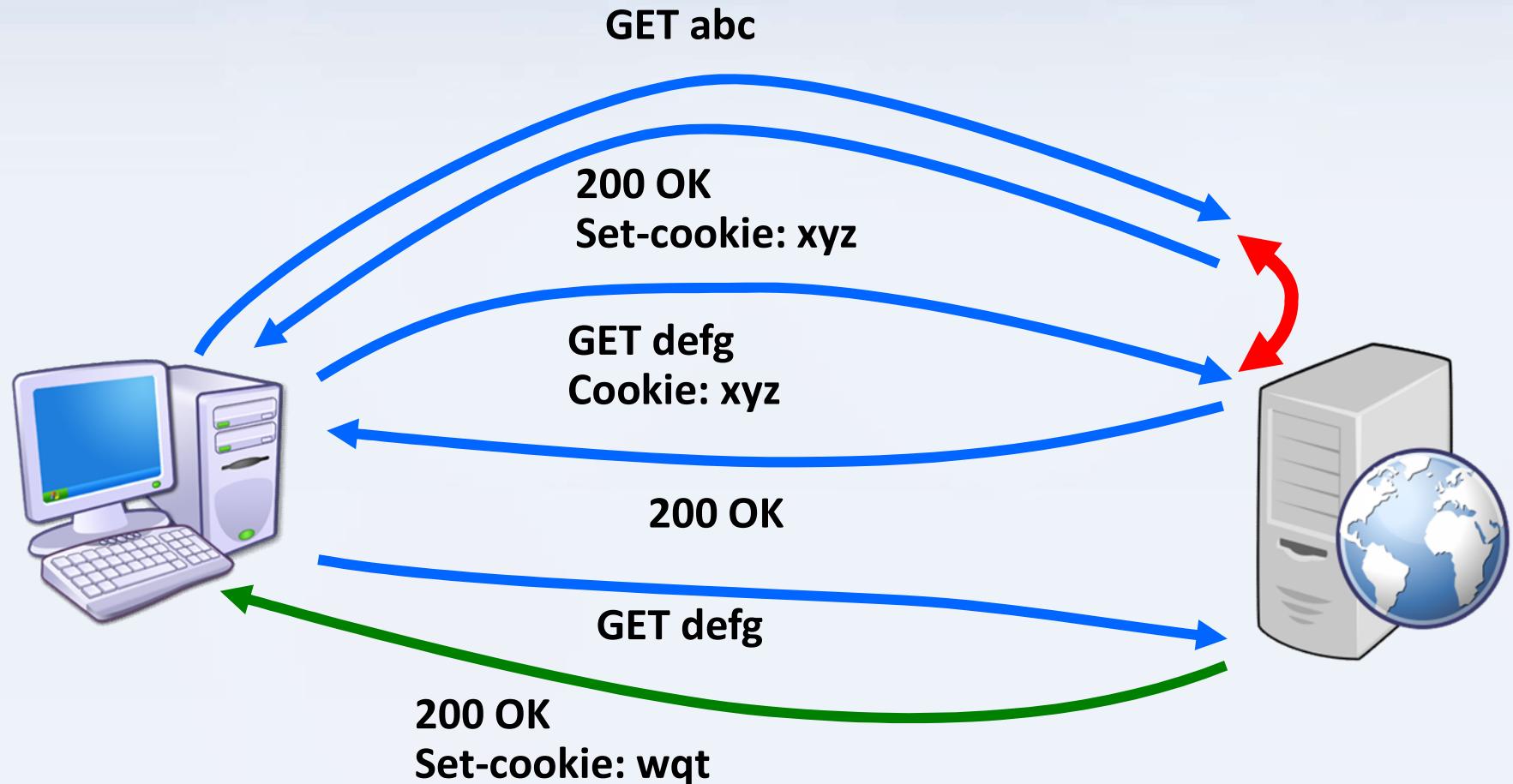
# Les cookies



## Les cookies

- Comme mentionné précédemment, HTTP est un protocole sans état. Mais les cookies sont une solution à ce problème.
- À l'aide de cookies, un serveur peut lier une demande client en un seul package.
- Si un utilisateur coche la case « **Remember me** ». Le serveur envoie un en-tête (set-cookie : cookie-value) au navigateur en réponse, avec un cookie.
- Cela signifie que pour la prochaine visite au site le navigateur enverra une demande à ce domaine avec un cookie (cookie : cookie-value) et le serveur autorisera l'utilisateur sur la base de ce cookie.

# Les cookies



# HTTPS

- Lorsqu'on connecte à un site, les identifiants de connexion sont faciles à intercepter s'ils ne sont pas cryptés avec HTTPS.
- Le champ « mot de passe » peut n'afficher que des cercles dans le navigateur Web, mais le mot de passe réel est transmis « en clair » sur Internet pour que tout le monde puisse le voir.
- Ainsi, un nouveau protocole a été introduit pour gérer des données sensibles précieuses. Ce protocole est connu sous le nom de SSL (Secured Socket Layer).
- HTTPS= HTTP + SSL (protocole HTTP fonctionnant en tandem avec SSL)

# Protocoles des services de messagerie (**SMTP, POP, IMAP**)



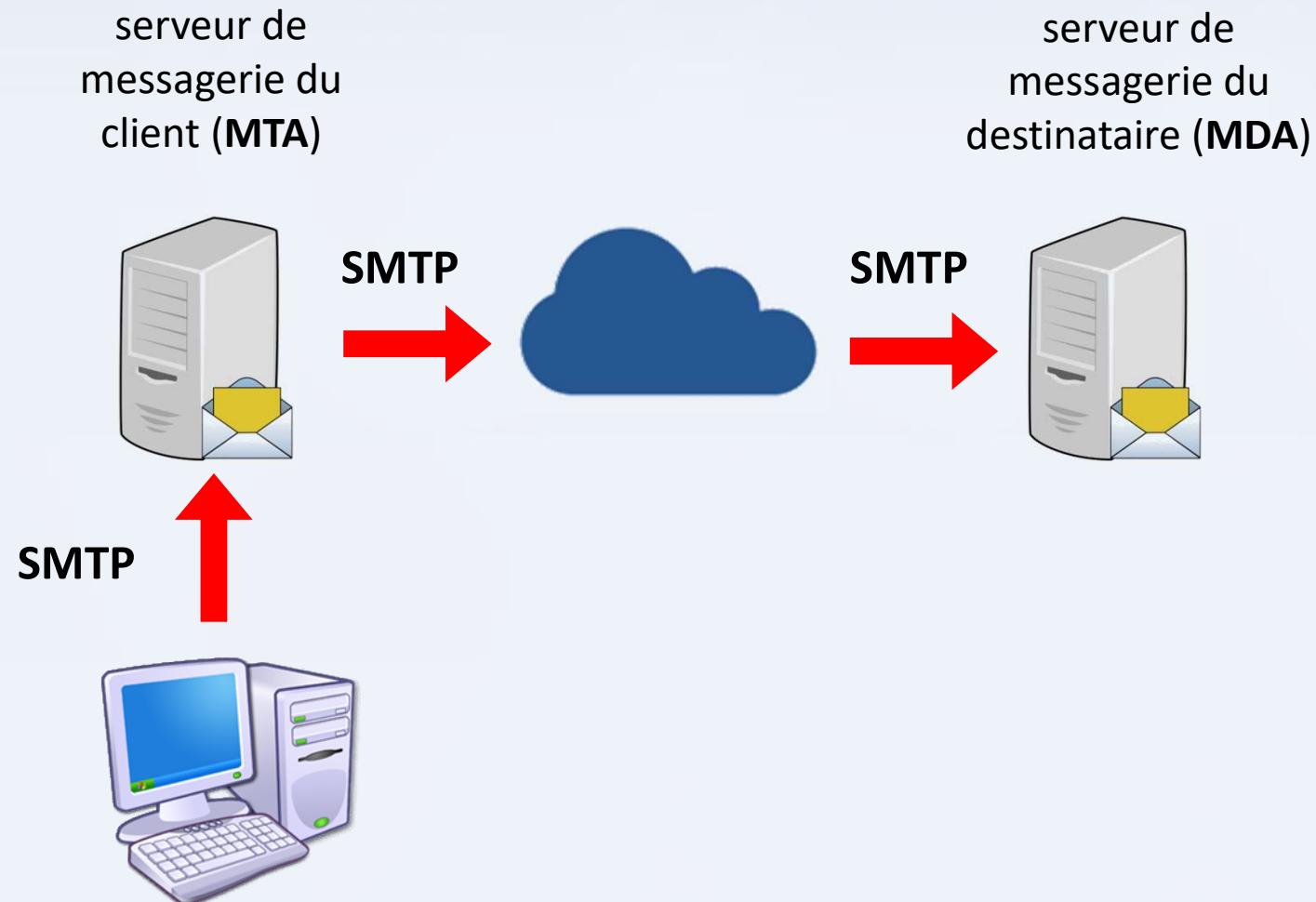
## Le protocole SMTP

- Simple Mail Transfer Protocol , est spécifiquement responsable de l'envoi et de la transmission des emails d'un expéditeur à un destinataire.
- SMTP a été développé pour la première fois au début des années **1980** par le très sérieux groupe de travail (IETF), **RFC 821 et RFC 2821**,
- Depuis sa sortie, SMTP est devenu le protocole standard pour **l'envoi** d'emails.
- Ce protocole fonctionne selon le mode client/serveur avec des connexions TCP...

## Terminologie SMTP

- Pour envoyer un mail, on utilisez un **MUA**. (**Mail User Agent**), est en général de 2 types :
  - ✓ un webmail (lorsque vous vous connectez en ligne)
  - ✓ un client de messagerie (logiciel installé sur le PC tel que Outlook, application de Smartphone, ...)
- Les serveurs de messagerie du client, appellés également **MTA** (**Mail Transfer Agent**), vont faire transiter les e-mails.
- Le **Mail Delivery Agent MDA**, c'est le service de remise des mails dans les boîtes aux lettres (les espaces mémoires réservés) des destinataires, il intervient donc en fin de la chaîne d'envoie d'un mail...

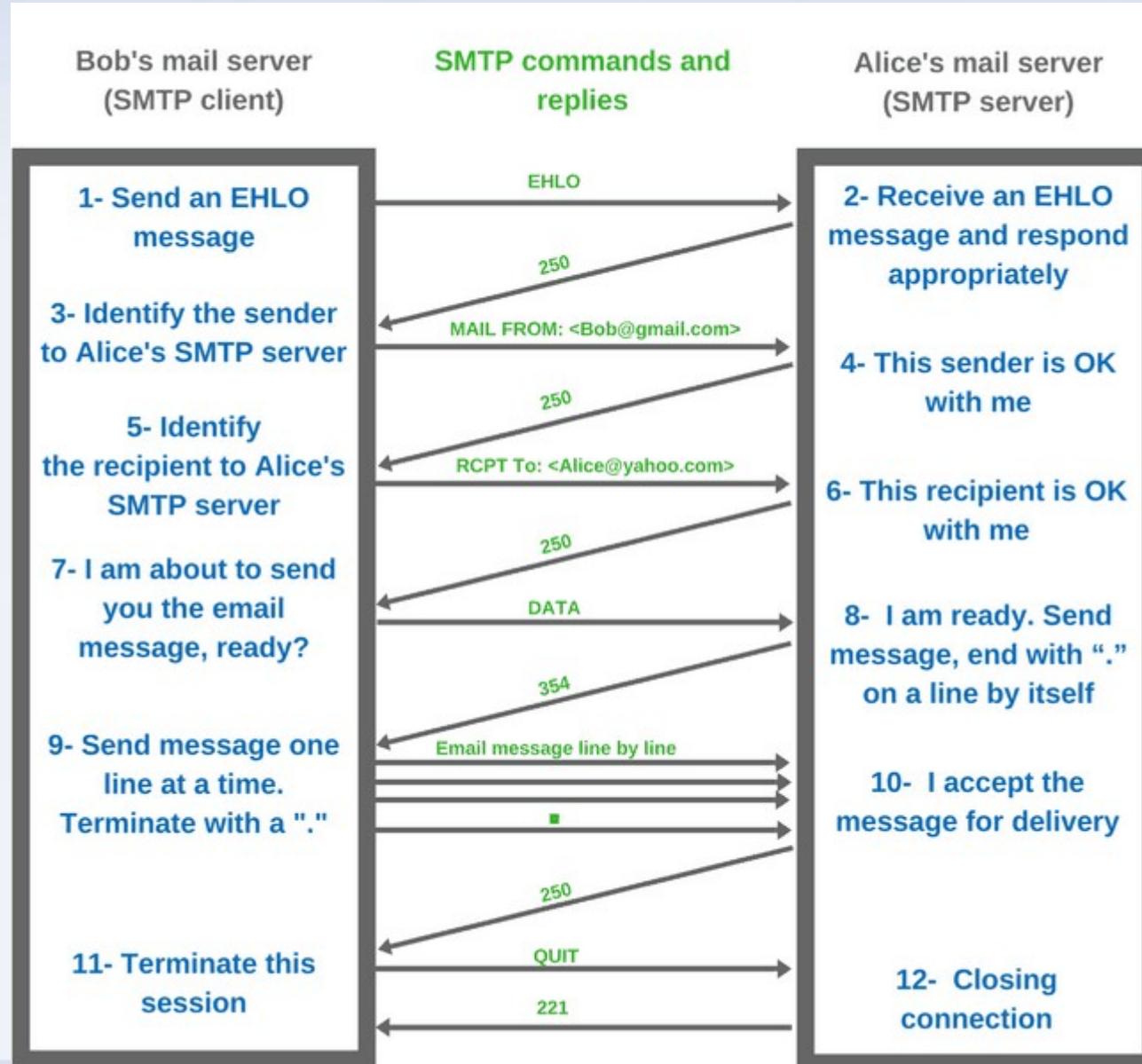
# Comment fonctionne le processus SMTP ?



## Comment fonctionne le processus SMTP ?

- L'e-mail est envoyé avec SMTP via un MUA au serveur de messagerie (MTA),
- Pour trouver à quel serveur de messagerie l'e-mail doit être envoyé, le serveur SMTP va s'appuyer sur le DNS et consulter l'enregistrement MX associé au domaine : cet enregistrement indique l'adresse du serveur de messagerie à contacter,
- Ensuite, le serveur de messagerie va l'envoyer via SMTP au serveur de messagerie du destinataire (MDA),
- Le serveur SMTP de destination (cible) stocke l'email à son niveau...

# Comment fonctionne le processus SMTP ?



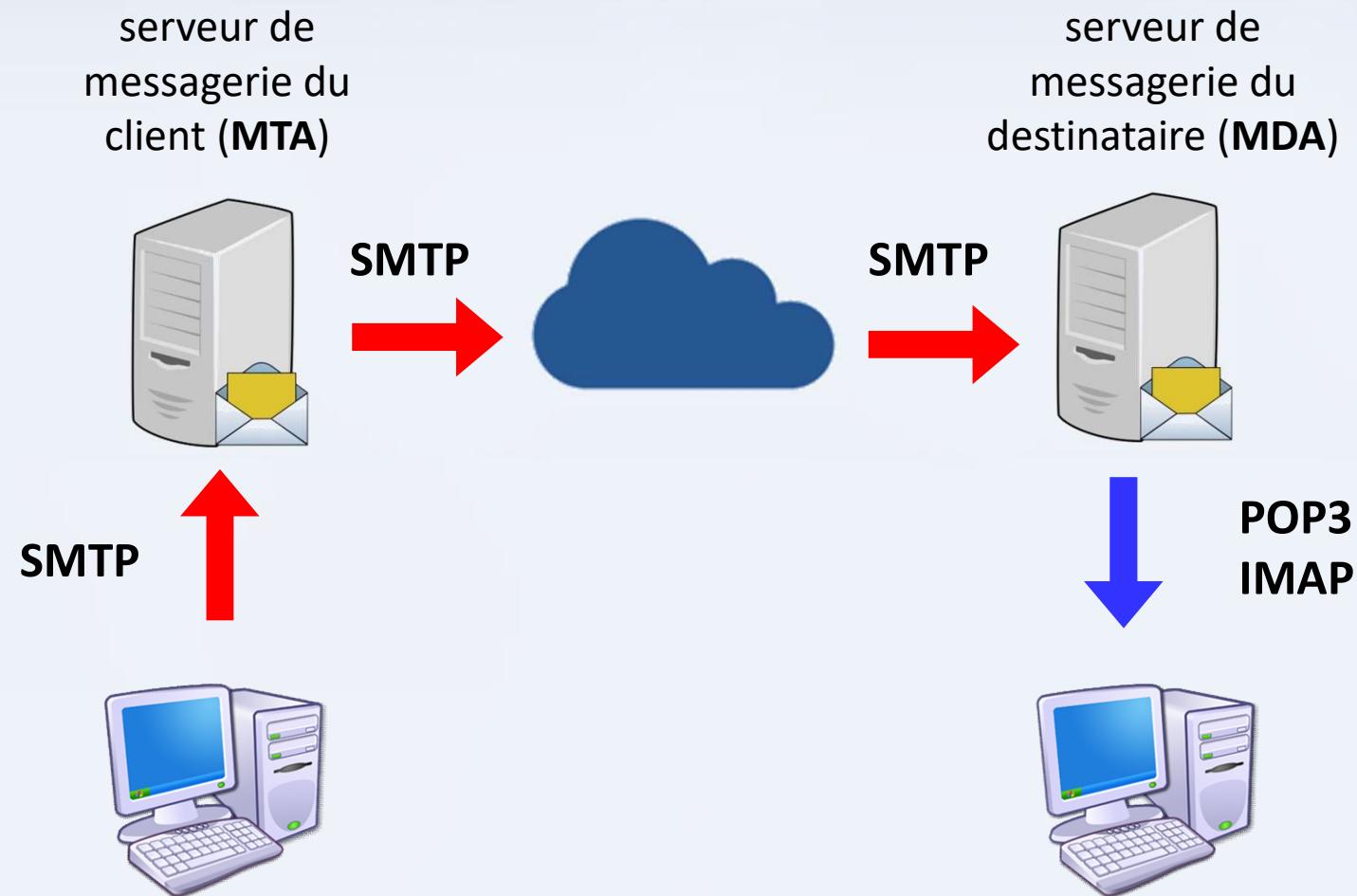
# Les commandes les plus couramment utilisées

Commande SMTP	Signification
HELO	« Hello » – Le client se connecte avec son nom d'ordinateur et démarre la session avec.
MAIL FROM	Le client nomme l'expéditeur de l'email.
RCPT TO	« Recipient » – Le client nomme le destinataire de l'email.
DATA	Le client initie la transmission de l'email.
RSET	Le client interrompt la transmission initiée, mais maintient la connexion entre le client et le serveur.
VRFY/EXPN	« Verify »/ « Expand » – Le client vérifie si une messagerie est disponible pour la transmission du message.
NOOP	Le client demande une réponse du serveur pour éviter une déconnexion due à un délai d'attente.
QUIT	Le client termine la session.

## Protocoles d'accès au courriel

- Le serveur MDA va vérifier que l'utilisateur destinataire existe bien dans sa liste d'utilisateurs.
- Il va ensuite placer le mail dans l'espace mémoire accordé à ses mails sur le serveur. Le mail est ainsi arrivé à destination. L'objectif du protocole SMTP est atteint.
- Ensuite c'est le protocole POP ou IMAP qui est utilisé par le destinataire pour consulter son email...

# Comment fonctionne le processus SMTP ?



## Multipurpose Internet Mail Extensions (MIME)

- À l'origine, SMTP avait été prévu pour ne transférer que des fichiers textes (codés en ASCII). Cela limite les courriels aux messages qui n'incluent que ces caractères, soit un petit nombre de langages comme l'anglais.
- Les autres langages qui ne sont pas supportés par l'ASCII ne peuvent donc pas être correctement représentés dans des courriels basiques.
- Aussi pour les données binaires (dont des fichiers contenant des images, des sons, ou des programmes informatiques).
- MIME définit des mécanismes pour l'envoi d'autres sortes d'informations, donc les types de contenus définis par le standard MIME peuvent être utilisés à d'autres fins que l'envoi de courriels.

## Multipurpose Internet Mail **Extensions (MIME)**

MUA va convertir votre mail au format texte (même les pièces jointes seront converties en texte).

MIME-Version: 1.0

Content-Type: image/png; name="image001.png"

Content-Description: image001.png

Content-Transfer-Encoding: base64

iVBORw0KGgoAAAANSUhEUgAAAKgAAABDCA  
xAAADsQBISSOGwAAABI0RVh0U29mdHdhcm  
EEQXBBxR19URQF3OEzRo0rKvoeCYm4xJen

## Le protocole POP

- Il s'appuie sur le port 110 par défaut, et pour la déclinaison chiffrée, **POP over SSL**, le port est le 995, on parle donc aussi de POP3S,
- Son objectif, c'est de permettre de télécharger les e-mails de la boîte aux lettres sur un serveur de messagerie, à partir du client de messagerie (Outlook ...)
- Lorsque l'e-mail est téléchargé sur le PC par l'intermédiaire du protocole POP, il n'est plus stocké sur le serveur.
- Un e-mail téléchargé sur le PC ne sera pas accessible sur le Smartphone, et vice-versa...

## Le protocole IMAP

- Internet Message Access Protocol a pour objectif est de récupérer les e-mails de la boîte aux lettres sur un serveur de messagerie. Néanmoins, il fonctionne différemment.
- Ce protocole **synchronise en permanence** les e-mails sur le client (exemple, PC) à partir du serveur de messagerie.
- Autrement dit, il crée une copie du message sur le PC ou le Smartphone grâce à la synchronisation. Le message d'origine reste sur le serveur de messagerie, ce qui va permettre de centraliser l'ensemble des boîtes aux lettres.
- En complément, il gère également la **synchronisation** des dossiers que vous créez pour organiser votre boîtes aux lettres.

## Le protocole IMAP

- La synchronisation permet d'avoir une boîte aux lettres dans le même état sur l'ensemble de vos appareils,
- Par exemple, si sur votre Smartphone vous passez un message en « non lu », ce même message sera aussi dans l'état « non lu » sur votre PC.
- POP présente l'avantage de permettre un accès hors ligne à vos messages puisqu'il les télécharge sur le PC. C'est également vrai avec le protocole IMAP grâce à **la mise en cache des messages** dans un fichier de données, que ce soit sur ordinateur, tablette ou mobile.

## Ports utilisés dans la messagerie

Une adresse IP permet d'identifier un ordinateur. Un port identifie une application/service spécifique s'exécutant sur cet ordinateur :

- Par défaut, les ports POP3 sont les suivants:
  - Port 110 – port non chiffré
  - Port 995 – Port SSL / TLS, également appelé POP3S (sécurisé)
- Ports IMAP par défaut:
  - Port 143 – port non crypté
  - Port 993 – Port SSL / TLS, également appelé IMAPS (sécurisé)
- Ports SMPT
  - 25 –
  - 587 (sécurisé)
  - 465 TLS

## Session SMTP

- L'authentification SMTP est une autre extension du protocole SMTP. Cela permet aux clients de messagerie de s'authentifier lors de la connexion à un serveur SMTP à l'aide d'un nom d'utilisateur et d'un mot de passe. Bref, cela empêche les utilisateurs non autorisés d'envoyer des courriers électroniques via un serveur SMTP
- Chaque session se compose d'une séquence de commandes SMTP provenant du client et de réponses sous forme de codes d'état provenant du serveur...

Inbox (1) - mehdi.m.rouissat@g...

https://mail.google.com/mail/u/0/#inbox?compose=new

New Message

To  
Cc  
Bcc |  
Subject

Compose

Inbox

Starred

Snoozed

Important

Sent

Drafts

Categories

Exposés

Private call

sendsms

Meet

New meeting

Join a meeting

Hangouts

Mehdi

No recent ch... Start a new

Sans Serif

B I U A

Send

EDAS

Password reset - You can reset your EDAS login credentials for user name mehdi.m.rouissat@...

8°C 20:00 FRA 05/01/2022

*Exercices –*

*Normes et*

*Protocoles*

## **Exercices – Normes et Protocoles**

### **I. QCM – Choisissez la bonne réponse**

1. 1. Quelle norme Wi-Fi permet un débit maximal de 9,6 Gbps ?

- a) 802.11n
- b) 802.11ac
- c) 802.11ax
- d) 802.11g

***Réponse : c) 802.11ax***

---

2. 2. Quelle modulation est utilisée par le Bluetooth classique ?

- a) QAM
- b) GFSK
- c) BPSK
- d) OFDM

***Réponse : b) GFSK***

---

3. 3. Le protocole utilisé pour transférer des fichiers sur Internet est :

- a) HTTP
- b) FTP
- c) SMTP
- d) DNS

***Réponse : b) FTP***

---

## **II. Exercices avec application**

### **Exercice 1 : Modèles OSI et TCP/IP**

Question : Comparez les couches des modèles OSI et TCP/IP. Identifiez les équivalences et les différences entre les deux modèles.

*Solution : Le modèle OSI comporte 7 couches, tandis que le modèle TCP/IP en comporte 4. Les couches Application, Présentation et Session de l'OSI sont fusionnées en une seule couche Application dans TCP/IP. Le modèle TCP/IP est plus pratique et utilisé sur Internet.*

---

### **Exercice 2 : Analyse de la technique FHSS**

Question : Expliquez le principe de la technique FHSS utilisée dans les réseaux sans fil IEEE 802.11. Donnez un exemple de fonctionnement.

*Solution : La technique FHSS (Frequency Hopping Spread Spectrum) consiste à faire sauter rapidement la fréquence de transmission entre différents canaux selon une séquence pseudo-aléatoire. Cela permet de réduire les interférences et améliorer la fiabilité des communications. Exemple : saut de fréquence toutes les 625 µs entre 79 canaux dans le Bluetooth.*

---

### **III. Questions de cours**

4. 1. Citez trois rôles principaux d'un protocole de communication.

*Réponse : Détection d'erreurs, synchronisation des communications, gestion de session.*

---

5. 2. Quelle est la différence entre norme et standard ?

*Réponse : Une norme est approuvée par un organisme officiel et est souvent contraignante, tandis qu'un standard est un accord ou une convention plus souple, souvent adopté par l'industrie.*

---

6. 3. Quels sont les avantages de la normalisation ?

*Réponse : Interopérabilité, réduction des coûts, sécurité, protection du consommateur, qualité.*

---

# *Conclusion*

## *Générale*

## Conclusion Générale

Le cours « Normes et Protocoles » constitue une composante essentielle dans la formation des étudiants en réseaux et télécommunications. Il offre une vision globale, structurée et approfondie des mécanismes de communication qui régissent les échanges d'informations dans les systèmes numériques modernes.

À travers l'étude des organismes de normalisation, des principes de standardisation, et des différents types de protocoles — qu'ils soient liés à la transmission analogique ou numérique, aux réseaux filaires ou sans fil, ou encore aux services Internet — l'étudiant acquiert une compréhension claire de l'architecture des réseaux et des règles d'interopérabilité. Le cours met également en lumière l'importance des modèles de référence OSI et TCP/IP dans la classification des protocoles, tout en abordant des aspects concrets comme les normes IEEE 802.11, les technologies Bluetooth, ou encore les protocoles applicatifs tels que HTTP, FTP, SMTP et DNS.

Cette formation ne se limite pas à une approche théorique : elle invite l'étudiant à analyser, comparer, et appliquer les normes et protocoles dans des contextes technologiques réels. En maîtrisant ces éléments, il devient capable de concevoir, évaluer et optimiser des systèmes de communication fiables, sécurisés et conformes aux standards internationaux.

Ainsi, ce cours prépare les futurs ingénieurs à relever les défis liés à l'évolution rapide des technologies de l'information, tout en les dotant des compétences nécessaires à l'innovation et à la conformité dans le domaine des réseaux et des télécommunications.