Cours de Réseaux

M1 informatique

1998-2018

Zoubir Mammeri

Chapitre 1

Tendances en réseaux

Quelques éléments pour comprendre le contexte des réseaux actuels et futurs

1. Principales évolutions et quelques chiffres

1. Principales évolutions et quelques chiffres

Age de pierre	Age de bronze	Age de fer
2,5 M années	8000 années	3000 années

Imprimerie

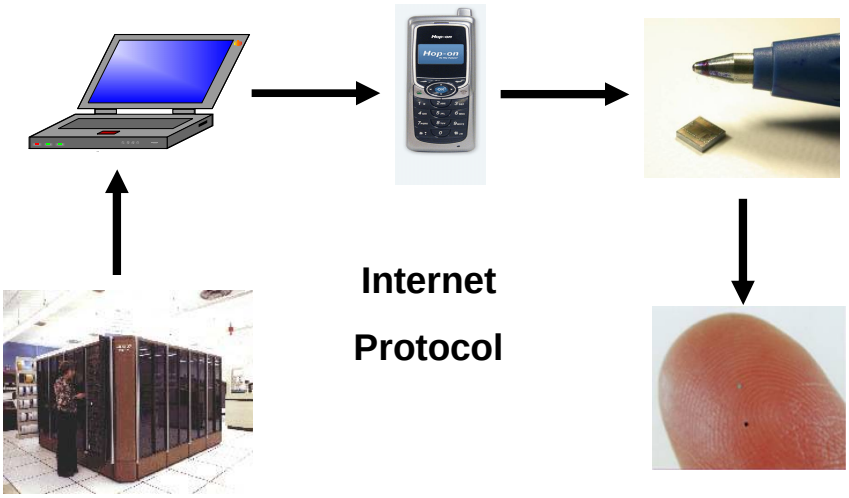
Age de pierre	Age de bronze	Age de fer
1440	1850	1930

Internet

Age de pierre	Age de bronze	Age de fer
1970	2010	2030

1. Principales évolutions et quelques chiffres

Evolution des équipements connectés

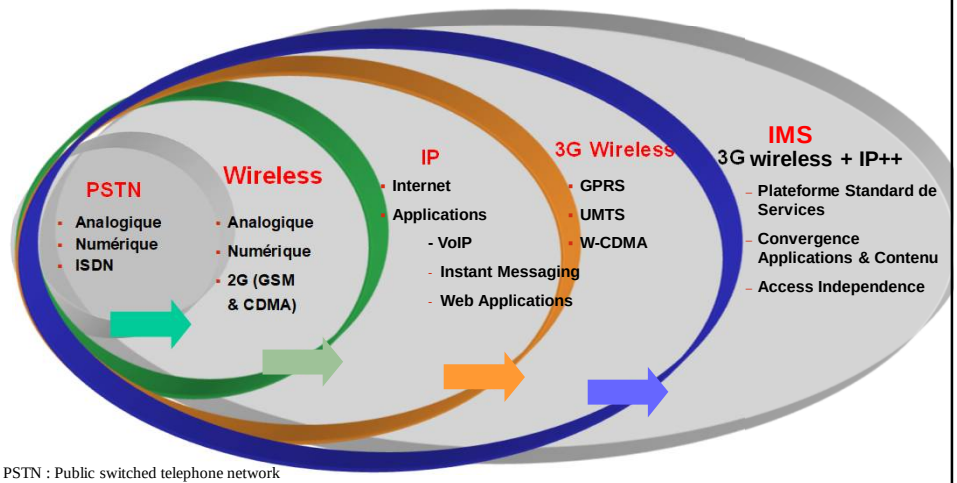


1. Principales évolutions et quelques chiffres

Diversité des équipements

1. Principales évolutions et quelques chiffres

Evolution des technologies de réseaux



PSTN : Public switched telephone network
ISDN : Integrated Services Digital Network
GPRS: General Packet Radio Service
CDMA : Code Division Multiple Access
W-CDMA : Wideband CDMA
IMS : IP Multimedia Subsystem
UMTS : Universal Mobile Telecommunication System

1. Principales évolutions et quelques chiffres

NGN (Next Generation Networks)

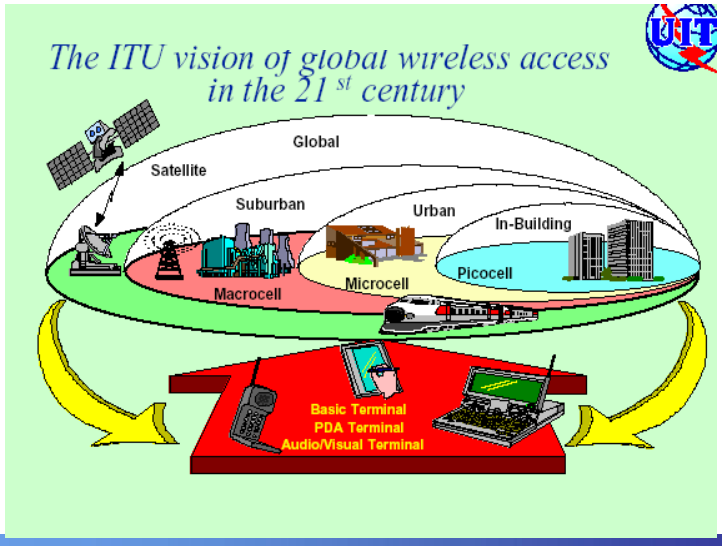
- **Internet aujourd'hui**
  - Des millions d'utilisateurs
  - Web, email, qualité plutôt médiocre de l'audio & vidéo
  - Les applications sont adaptées à la technologie sous-jacente
- **NGN Internet : les attentes**
  - Des milliards d'utilisateurs, de machines et de choses
  - Convergence des applications et des services
  - Convergence entre filaire et sans fils, entre fixe et mobile
  - Les nouvelles technologies mènent à de nouvelles applications
  - Société de l'information dans laquelle les clients sont 'Always-on Network'
  - Faire que le "Global village" devienne une réalité
  - Applications avec qualité de service garantie
  - Garantie de sécurité et protection de la vie privée

1. Principales évolutions et quelques chiffres

Evolution des modes d'accès et connexion

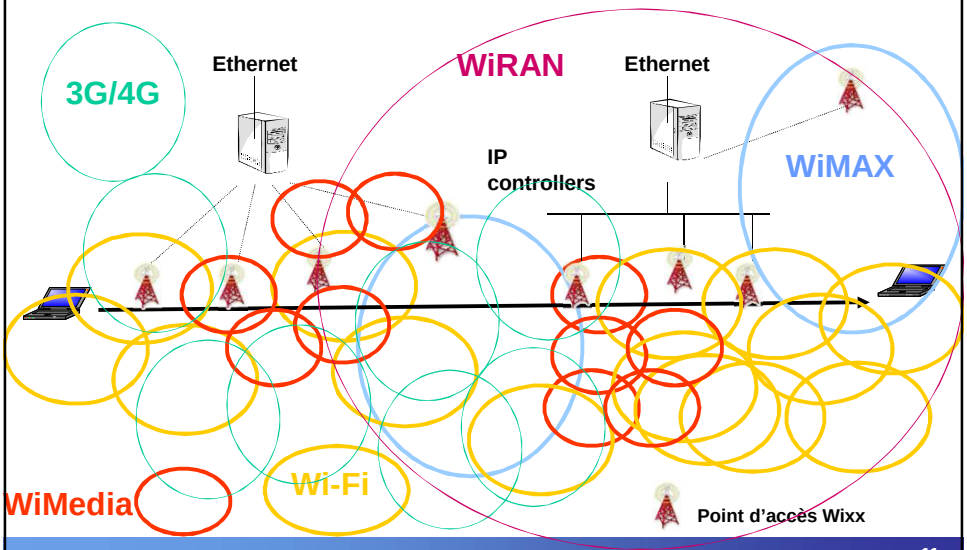
1. Principales évolutions et quelques chiffres

Portée/étendue des réseaux



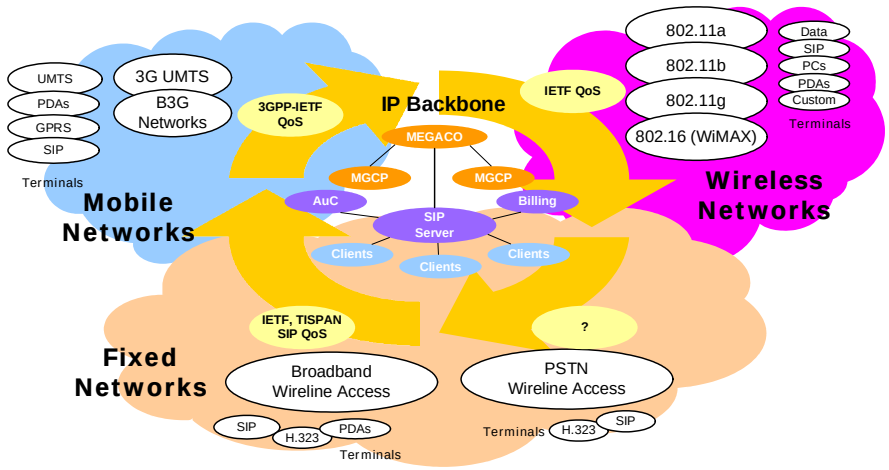
1. Principales évolutions et quelques chiffres

Cohabitation de différents réseaux



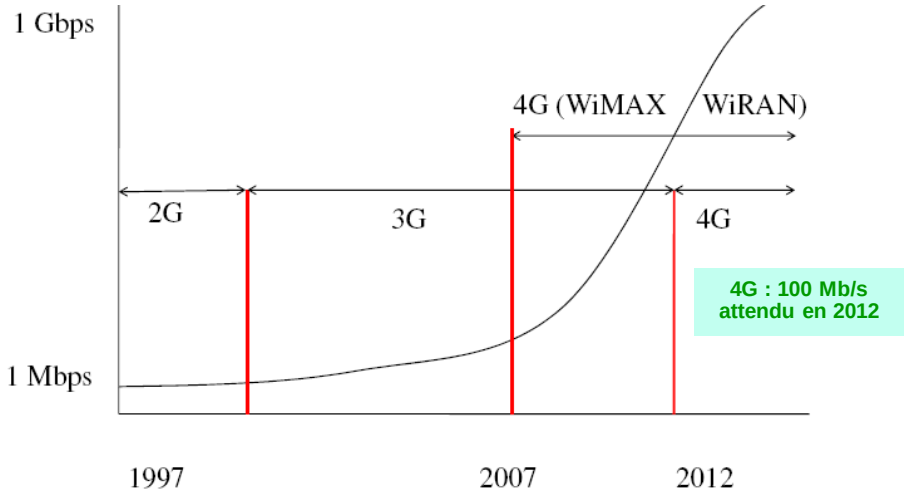
1. Principales évolutions et quelques chiffres

Cohabitation de différents protocoles



1. Principales évolutions et quelques chiffres

Evolution des débits des réseaux de télécom



4G : 100 Mb/s attendu en 2012

1. Quelques caractéristiques en chiffres

Puissance, débit, temps de transfert

File Transfer in megabytes: 5,000	Bluetooth	802.11b	802.11a/g	WiMedia
Rx power consumption, mW	70	350	700	405
Effective throughput (Mbps)	0.75	6.0	25	170
Time to transfer file (minutes)	889	111	26.7	3.9
Ratio to WiMedia time	227	28	7	1
Battery consumed @ 3.3V (mAh)	314	196	94	8.0
Ratio to WiMedia power	39	24	12	1

1. Quelques caractéristiques en chiffres

Coût du bit selon les applications

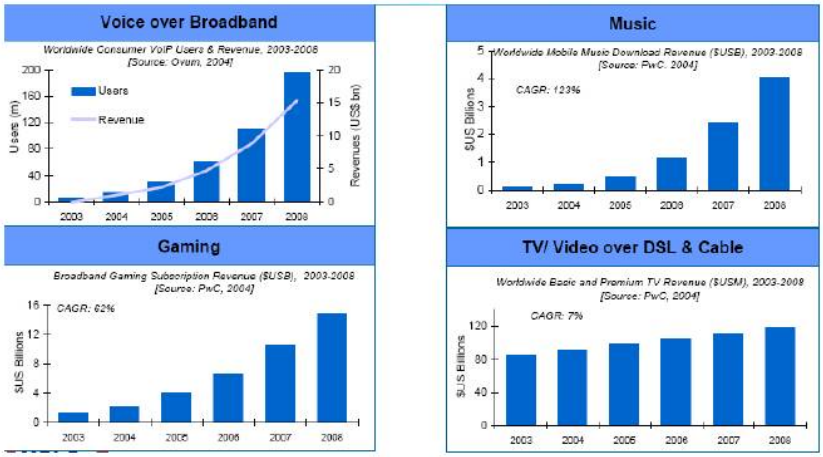
Service	kB	Pricing	$ per MB
Film 90 Min	691 MB	$ 10	$ 0.01
Fixed Call 1 Min	480 kB	$ 0.175	$ 0.12
MP3 4 Min	1850 kB	$ 1.89	$ 1.02
Web on 3G 5 Min	425 kB	$ 1.41	$ 3.33
Mobile Call 1 Min	144 kB	$ 0.84/min	$ 5.86
MMS	20 kB	$ 0.50	$ 25.00
SMS	0.1 kB	$ 0.25	$ 2,500
Ringtone	0.2 kB	$ 3.95	$ 19,750

Document Alcatel

2. Applications

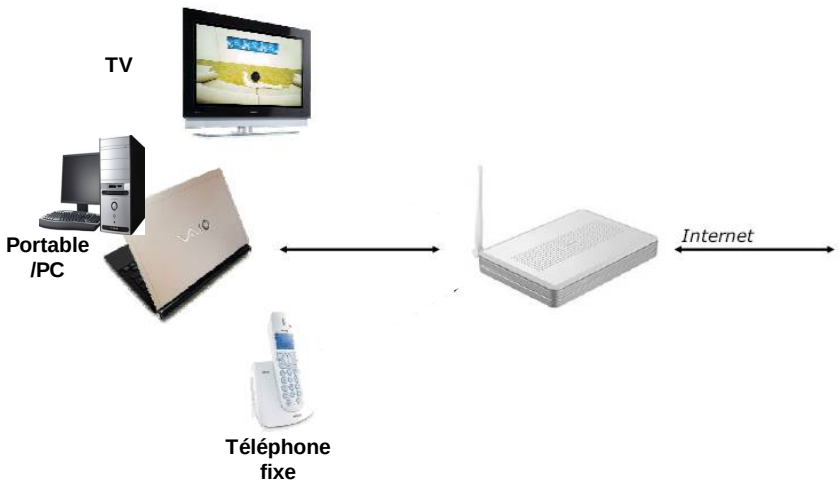
2. Applications

Principales applications sur Internet



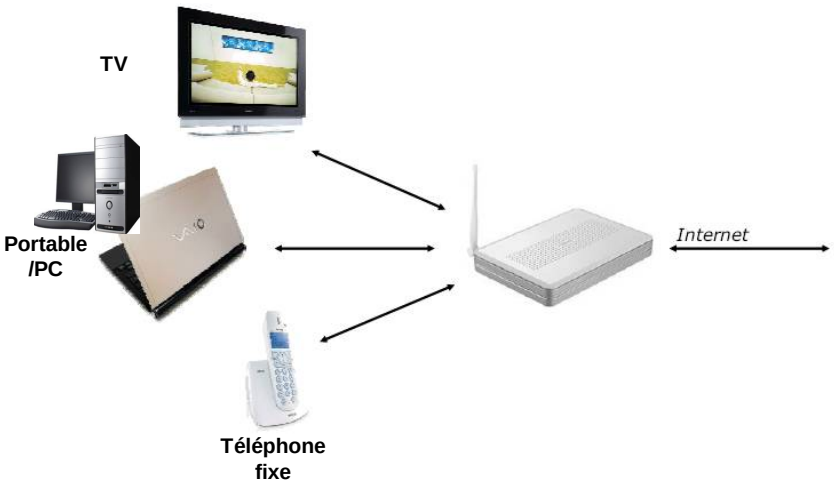
2. Applications

One-play



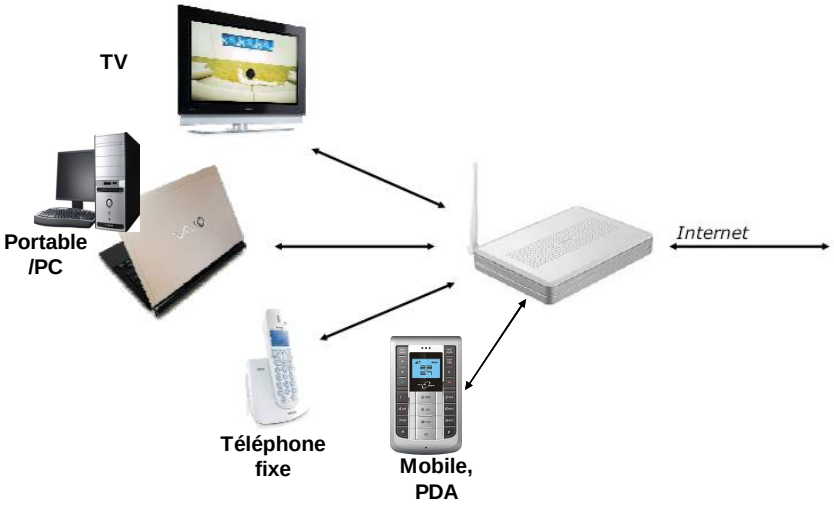
2. Applications

Triple-play



2. Applications

Quadruple-play



2. Applications

Penta-play : « tout en un »

2. Applications

Développement des applications et services

- **Applications vs Services**
  - Service = aspect particulier (ex. Localisation, temps synchronisé…)
  - Application = un tout pour répondre à un besoin global
  - Application = *N* services + autres
- **Applications**
  - De plus en plus de demandes
  - Tous les secteurs (téléachat, médical, transport, loisirs…)
  - Secteur de recrutement des informaticiens

2. Applications

Développement des applications et services

- Services directement « commercialisables »
  - Utilisés par les entreprises et personnes pour développer leurs applis
  - Exemples : Localisation par satellite, Stockage de données, Facilités d'accès à Internet …
  - Secteur de création d'entreprises
- Services « à la demande », spécifiques, bas niveau
- Challenges pour le développement des applications et services
  - Conception/design de contenus attractifs et rentables
  - Maîtrise de la complexité logicielles des applications/services
  - Maîtrise du business

3. Internet des choses
Internet of the things

3. Internet des choses

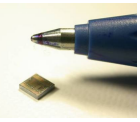





RFID

Réseau de domicile

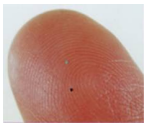
100 Milliards de choses en 2010-2015



1 % des connexions actuelles

99% des nouvelles connexions

Capteur sans fil



Nanotechnologie




3. Internet des choses

Internet et les nanotechnologies









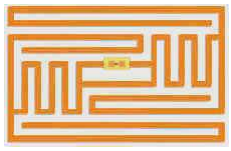


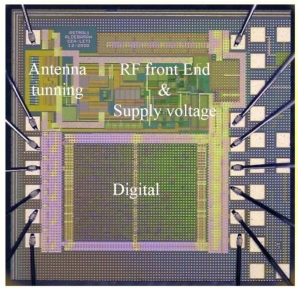


3. Internet des choses

RFID (Radio Frequency Identification)

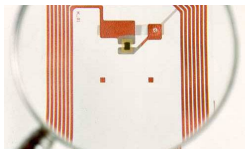
- **But**
  - Identification
  - Traçabilité
- **Régulation**
  - Fréquence : 865-868 MHz
  - Puissance : de 1 W à 4 W
- **Modes**
  - Passif
    - Pas d'énergie dans un RFID
    - Lecteur (quelque mm à quelques m)
  - Active
    - Diffusion de balise
    - Portée : 10 mètres
    - Temps de vie : 10 ans

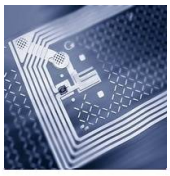


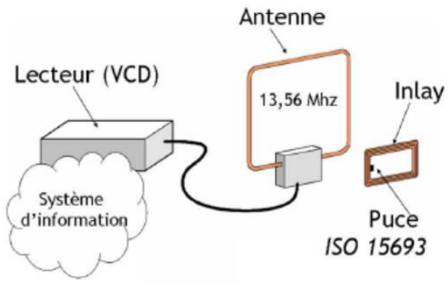


3. Internet des choses

Tags et lecteurs RFID



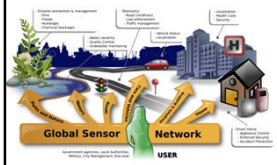




3. Internet des choses

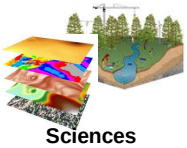
Domaines d'applications

Maintenance prédictive



Smart City

Industrie automatisée



Sciences

Défense

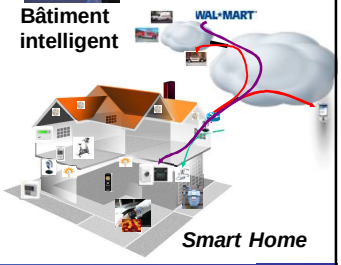
Economie d'énergie

Santé

Bâtiment intelligent

Amélioration de productivité

Agriculture



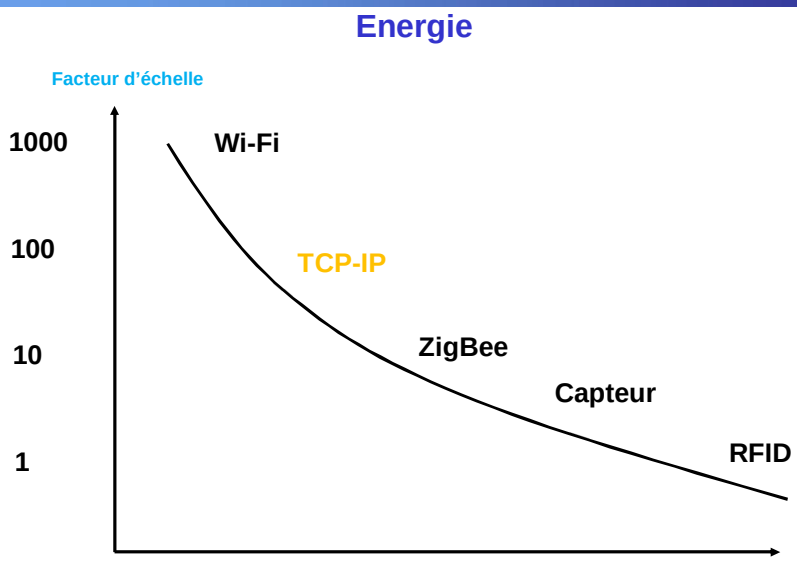
Smart Home

3. Internet des choses

De nombreux défis

- Énergie des équipements/choses
- Adressage (~~IPv4~~ | IPv6 | …) : des Gigas d'@IP
- Sécurité
- Qualité de service
- Autopilotage
- Communications T2T (Thing to Thing)

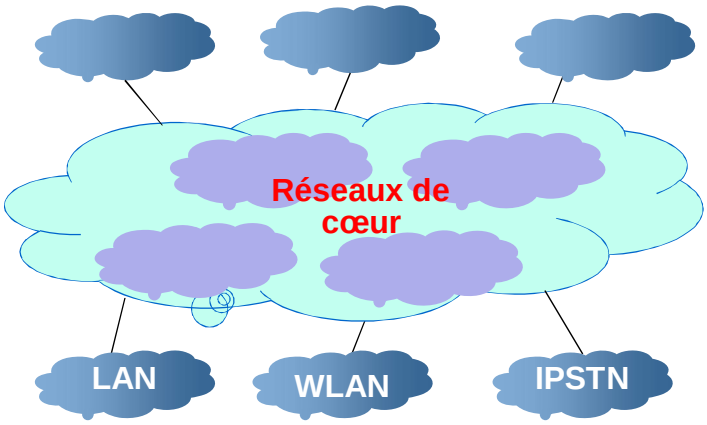
3. Internet des choses



4. Réseaux d'accès

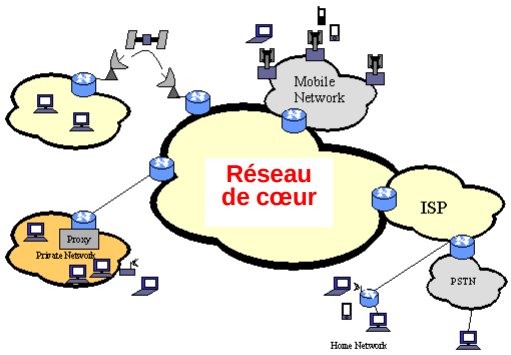
4. Réseaux d'accès

Internet = réseaux de cœur + réseaux d'accès (vue 1)



4. Réseaux d'accès

Internet = réseaux cœur + réseaux d'accès (vue 2)



4. Réseaux d'accès

Réseaux d'accès filaires – Les supports

Paire métallique

Câble coaxial

Fibre optique

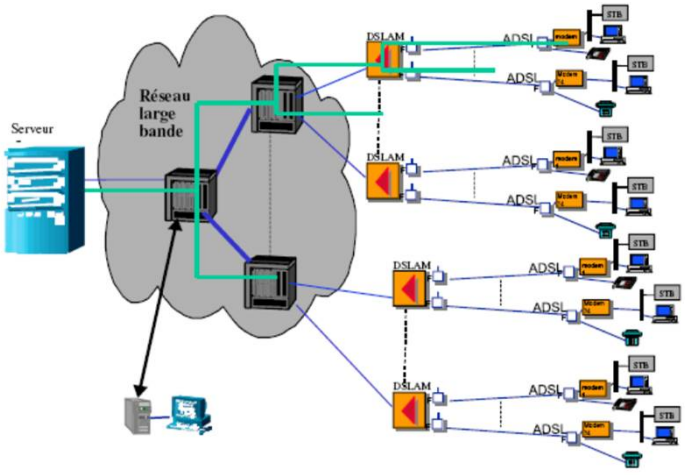
USB

RJ45

PLC
(Power Line Communication)

4. Réseaux d'accès

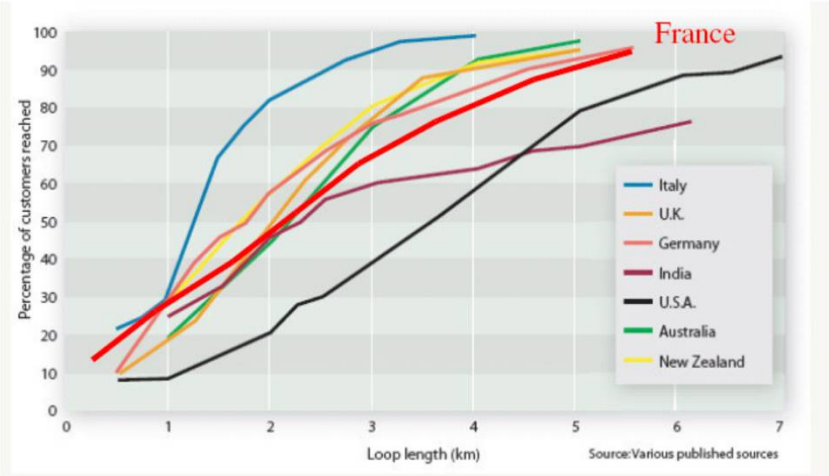
Réseaux d'accès filaires – Architecture typique



DSLAM: Digital subscriber line access multiplexer

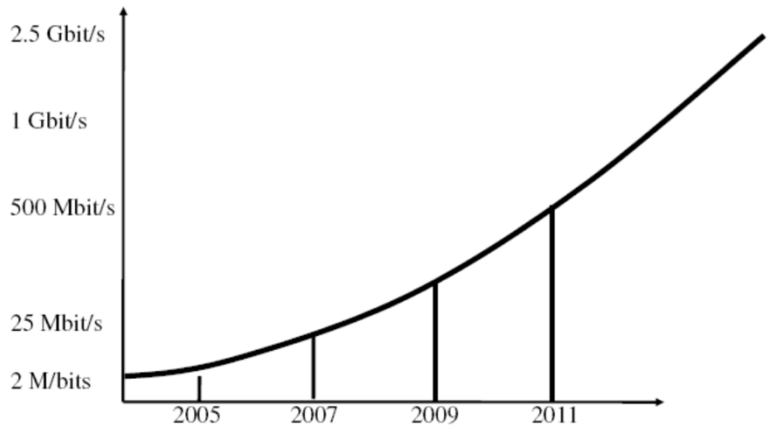
4. Réseaux d'accès

Réseaux d'accès filaires – Boucle locale



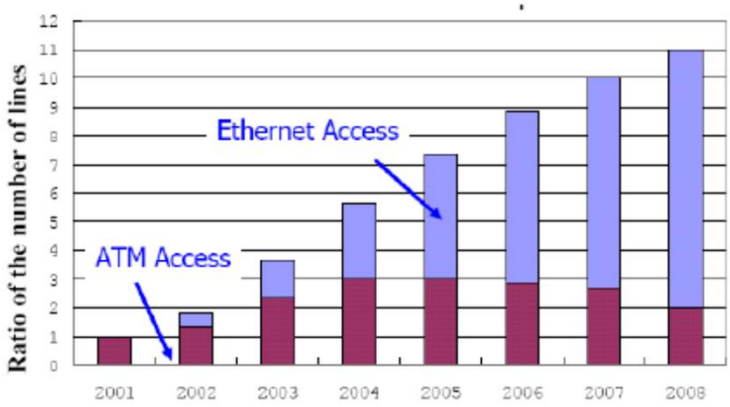
4. Réseaux d'accès

Réseaux d'accès filaires – Débit des internet-boxes



4. Réseaux d'accès

Réseaux d'accès filaires – ATM vs Ethernet

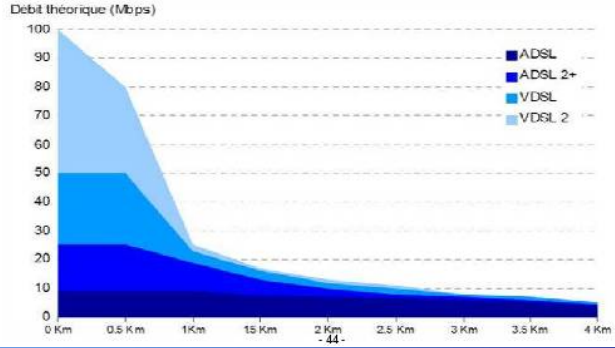


4. Réseaux d'accès

Réseaux d'accès filaires – xDSL

paires métalliques + modem xDSL (*x Data Subscriber Line*)

- ADSL (*Asymmetric Digital Subscriber Line*)
- SDSL (*Symmetric DSL*)
- HDSL (*High-bit-rate DSL*)
- VDSL (*Very-high-bit-rate DSL*)



4. Réseaux d'accès

Réseaux d'accès filaires – Fibre optique (en France)

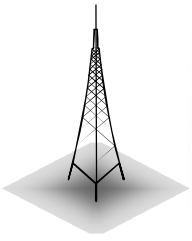
La fibre optique FITL (*Fiber In The Loop*)

- jusqu'au quartier FTTQ
- jusqu'au trottoir FTTC
- jusqu'au bâtiment FTTB
- jusqu'à la prise FTTH

4. Réseaux d'accès

Réseaux d'accès sans fils – les antennes

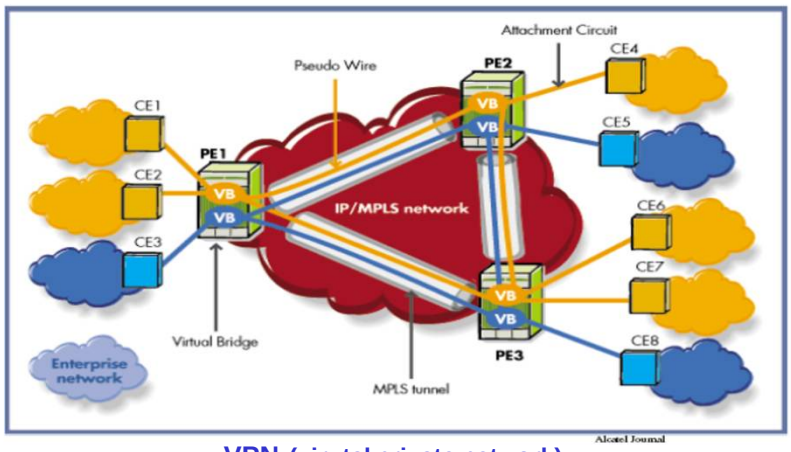
Antennes intégrées (invisibles)



Antennes visibles

4. Réseaux d'accès

Réseaux d'accès pour les entreprises – VPN



VPN (virutal private network)

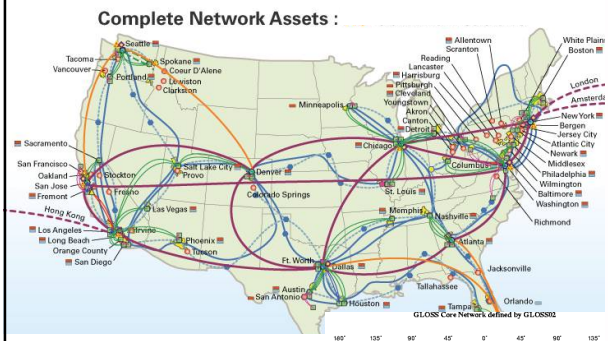
VPN = en W | WL | W + WL W : wired , WL : wireless

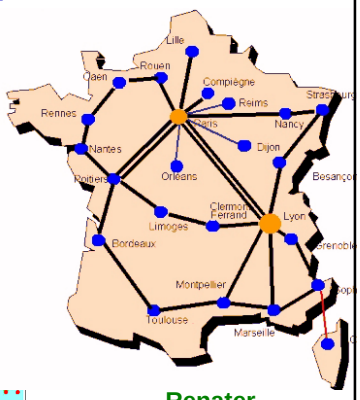
VPN = partie propriétaire + partie louée

5. Réseaux de cœur

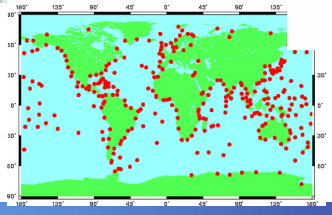
5. Réseaux de cœur

Vue géographique



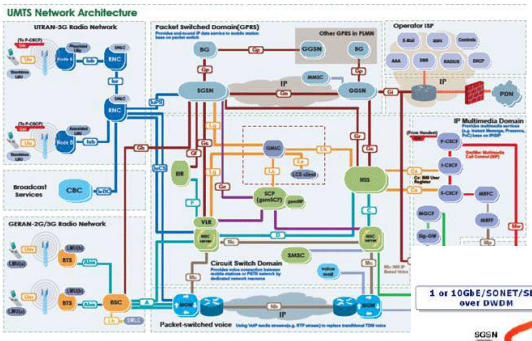


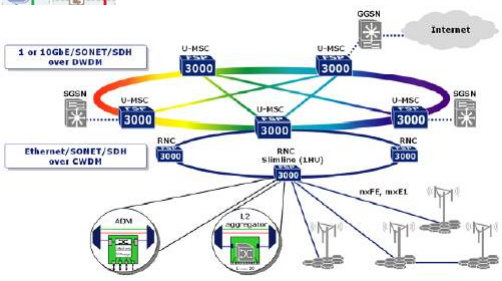
Renater



5. Réseaux de cœur

Vues Composants





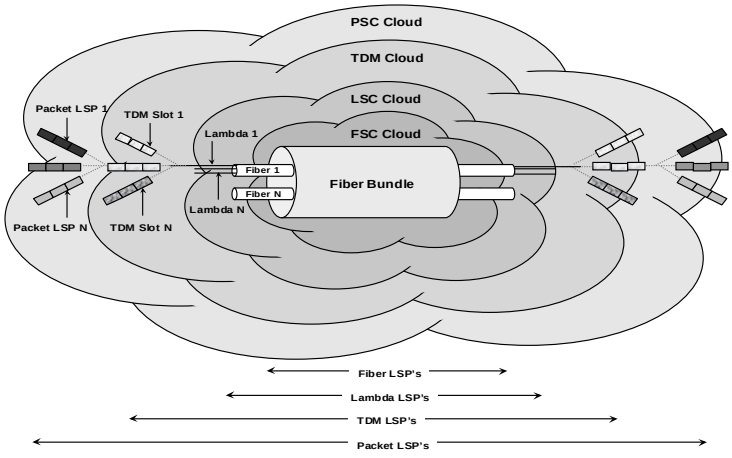
5. Réseaux de cœur

Technologies pour les réseaux de cœur

- **Besoins : rapidité, rapidité, rapidité**
- **Contrôle de trafic : en bordure des réseaux de cœur**

- **Technologies pour les réseaux de cœur**
  - **ATM**
  - **Ethernet (Ethernet carrier grade,** Ethernet Generalized VLAN, Metro Ethernet Forum, … **)**
  - **MPLS, GMPLS**
  - **?**

ATM : Asynchronous Transfer Mode MPLS : Multi Protocol Label Switching
GMPLS : Generalized MPLS



Commutation rapide

6. Réseaux dédiés

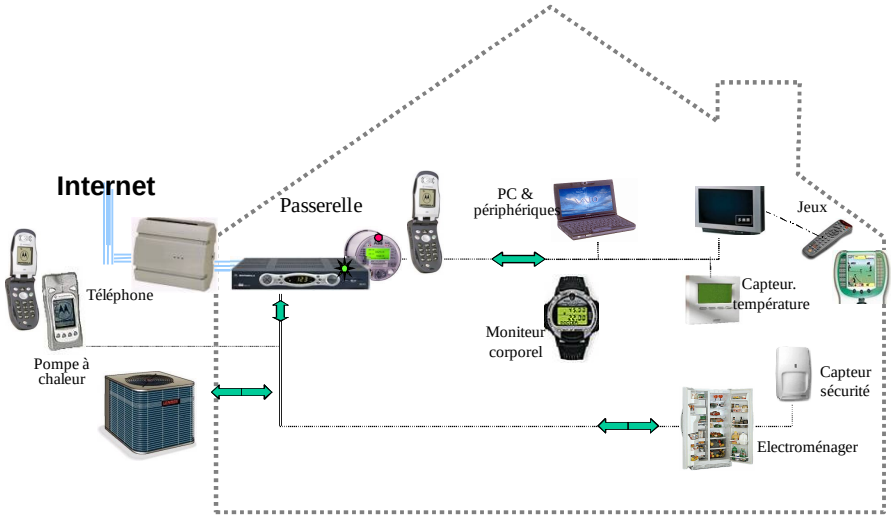
Réseaux domotiques

Réseaux embarqués

Réseaux de véhicules (VANETs)

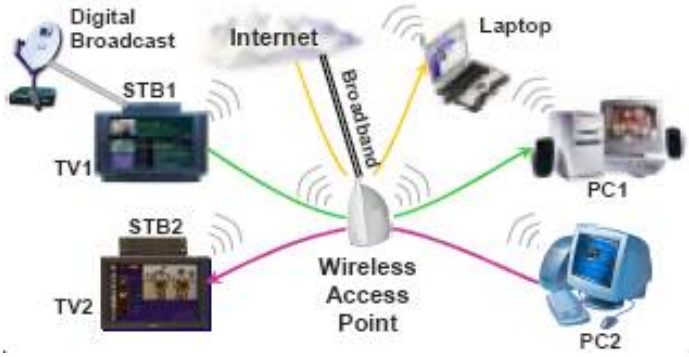
6. Réseaux dédiés - Réseaux domotiques

Panoplie d'équipements à connecter



6. Réseaux dédiés - Réseaux domotiques

Topologie (à court terme)



- Desserte de l'utilisateur par une Internet box unique
- Augmentation des débits de façon quasi-exponentielle
- Marché important

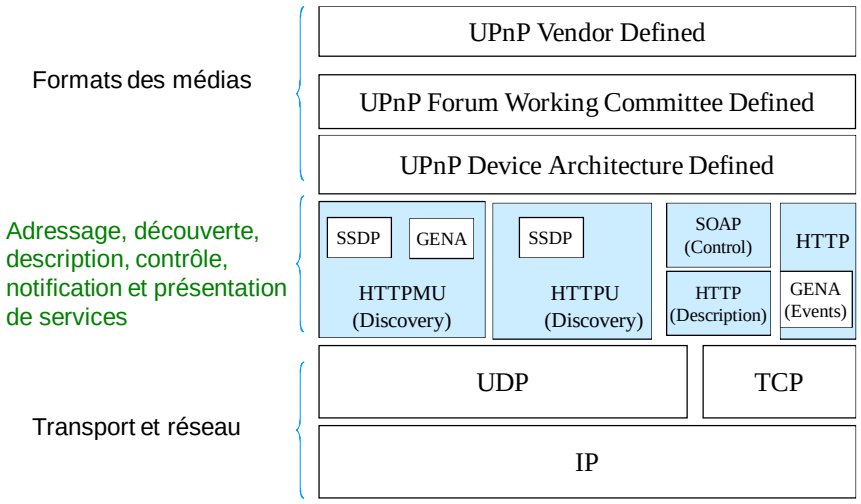
6. Réseaux dédiés - Réseaux domotiques

Architectures

- Architectures pour réseaux domestiques
  - UPnP (Universal Plug and Play)
  - DLNA (Digital Living Network Alliance)
  - HGI (Home Gateway Initiative)

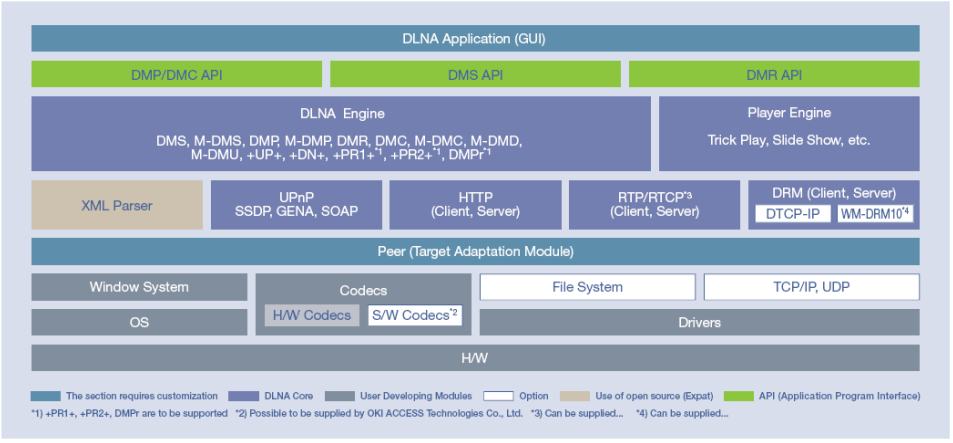
6. Réseaux dédiés - Réseaux domotiques

Architecture UPnP



6. Réseaux dédiés - Réseaux domotiques

Architecture DLNA



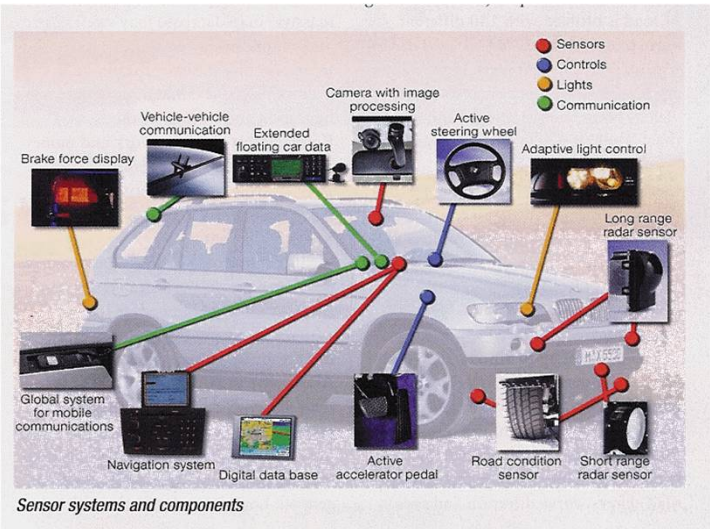
6. Réseaux dédiés - Réseaux embarqués

Secteurs d'utilisation des réseaux embarqués

- Réseaux dans l'automobile
- Réseaux avioniques
- Réseaux dans les trains, à la SNCF
- Réseaux dans les robots
- Réseaux de corps (BAN : body area networks)
- …

6. Réseaux dédiés - Réseaux embarqués

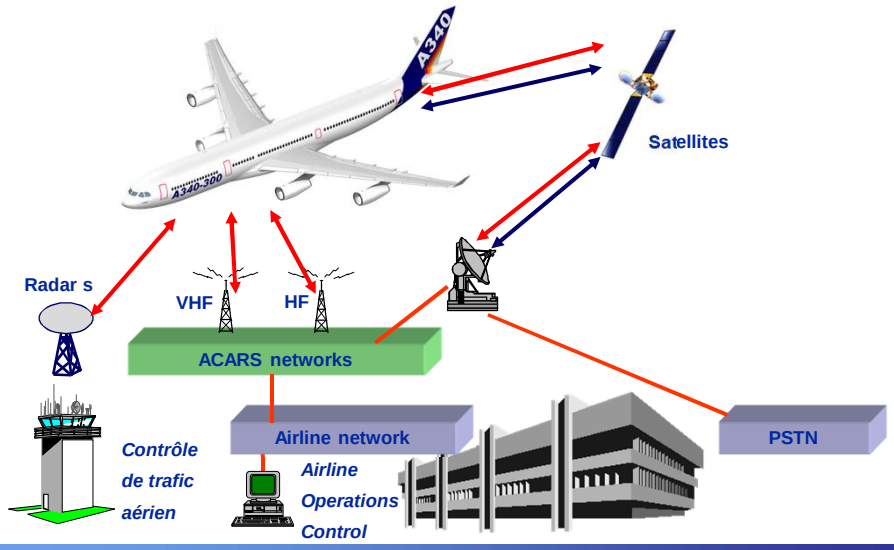
Réseaux embarqués – Automobile



Sensor systems and components

6. Réseaux dédiés - Réseaux embarqués

Réseaux embarqués – avionique et aérien



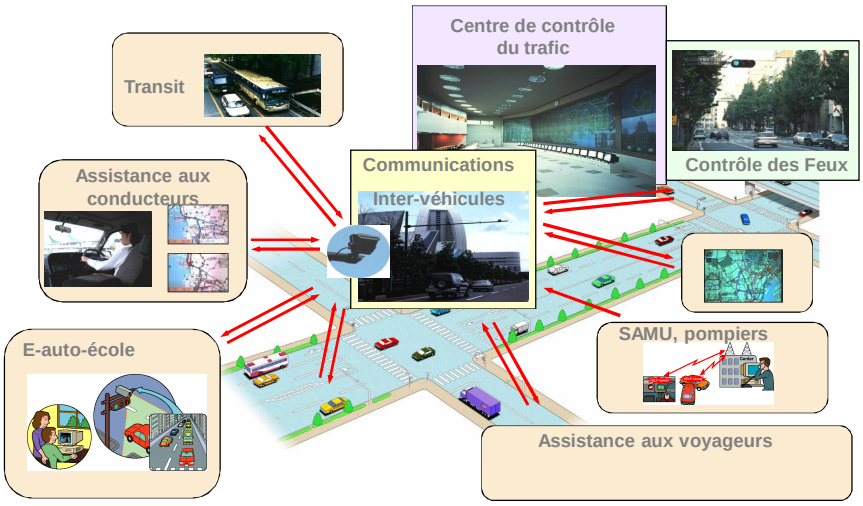
6. Réseaux dédiés - Réseaux de véhicules

Réseaux VANETs pour la gestion du transport

- Applications
  - Sécurité des usagers
  - Gestion de trafic/circulation
  - Informations aux conducteurs/voyageurs
  - Gestion de fret et transport de marchandises
  - Autres
- Bénéfices escomptés
  - Réduction des accidents
  - Circulation fluide
    - Réduction de la pollution
    - Réduction des temps et coût des déplacements

6. Réseaux dédiés - Réseaux de véhicules

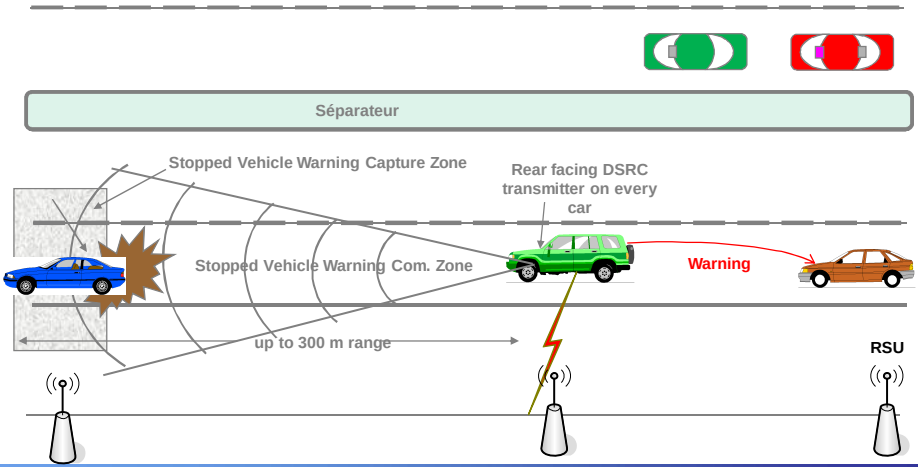
Gestion automatisée du trafic urbain et routier



6. Réseaux dédiés - Réseaux de véhicules

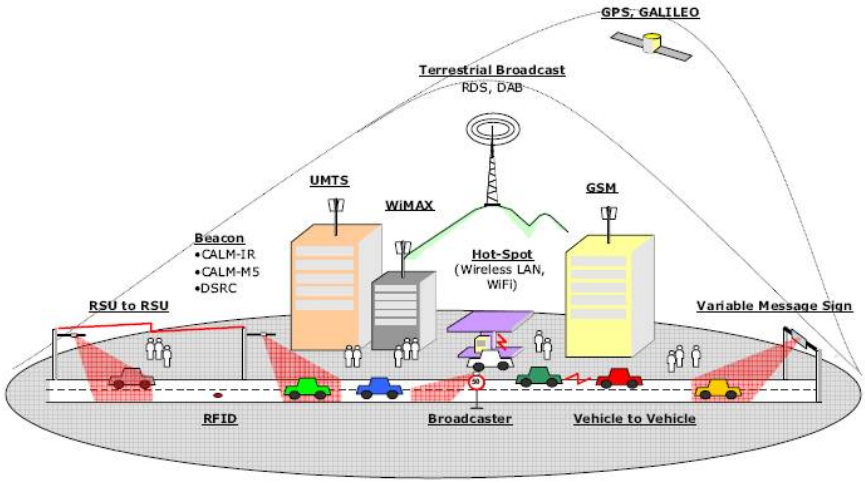
Infrastructure pour VANETs

- Utilisation d'infrastructure dans les véhicules et les bords des routes : capteurs, routeurs…



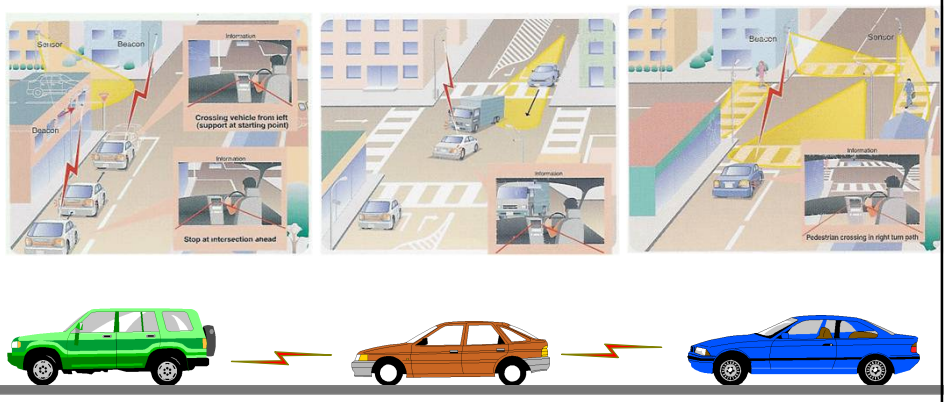
6. Réseaux dédiés - Réseaux de véhicules

Infrastructure pour VANETs



6. Réseaux dédiés - Réseaux de véhicules

- **Réseau de diffusion d'Informations sur les accidents, obstacles, bouchons, piétons….**



7. Sécurité

7. Sécurité

- ***Anytime Anywhere connected*** **+ malveillances ⇨ Besoins de protection**
- **Modèles de vulnérabilités et attaques**
- **Contre-attaques et anticipation des attaques : mécanismes de sécurité**

- ***Besoins de base en sécurité***
  - **Intégrité**
  - **Confidentialité**
  - **Disponibilité**

7. Sécurité

- *Challenges*
  - Mécanismes de sécurité robustes
  - Mécanismes de sécurité avec surcoût faible
  - Gestion de clés efficace
  - Etablissement de confiance et anonymat (tout le monde veut communiquer avec tout le monde, de n'importe où, et tout le monde se méfie de tout le monde !)
  - Administration de la sécurité à faible coût

8. Autopilotage des réseaux et Virtualisation

8. Autopilotage des réseaux et virtualisation

Pilotage automatique des réseaux

- **Problèmes**
  - **Complexité croissante des réseaux (en nombre de réseaux, de protocoles, de contraintes à respecter, de nœuds, d'utilisateurs…)**
  - **Ajout/changement de protocoles, services, clients, utilisateurs, machines…**
  - **Difficulté de configuration et adaptation dynamique et rapide**
  - **Interventions humaines**
    - **Sources d'erreurs**
    - **Temps de réaction élevés face à des changements rapides**
    - **De nombreux ingénieurs réseaux sont nécessaires**

8. Autopilotage des réseaux et virtualisation

Pilotage des réseaux

< 1950

< 2000

8. Autopilotage des réseaux et virtualisation

Pilotage automatique des réseau

1980-2020

2000-2020

8. Autopilotage des réseaux et virtualisation

Pilotage automatique des réseau

Réseaux autonomes

Quand ?

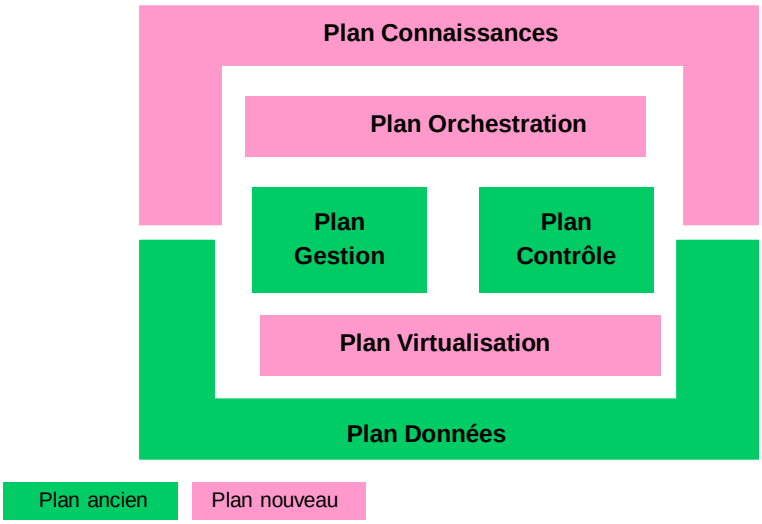
> 2020

Propriétés du pilotage automatique

- Gestion distribuée et autonome
- Basé sur des algorithmiques avancées (IA, analyse de données, sciences cognitives…)
- Temps de réponse aux changements : qq ms

8. Autopilotage des réseaux et virtualisation

Nouvelles architectures multi-plans



8. Autopilotage des réseaux et virtualisation

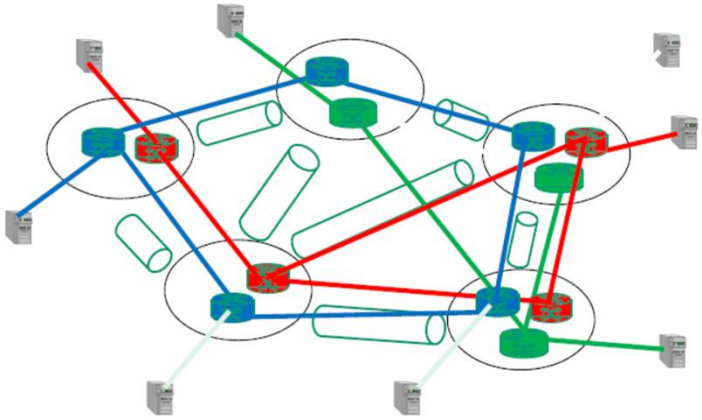
Virtualisation

- **Virtualisation classique**
  - Virtualisation des ressources d'une machine (CPU, Mémoire…)
  - Bénéfices : plus d'utilisateurs et de programmes sur une seule machine
- **Pourquoi virtualiser les réseaux**
  - Pouvoir réutiliser plusieurs fois un même composant logiciel/matériel
  - Permettre et faciliter le partage de ressources
  - Augmenter la sécurité des routeurs (car ils sont virtuels)
  - Isolation du trafic réseau dans les machines virtuelles

8. Autopilotage des réseaux et virtualisation

Virtualisation – Plusieurs réseaux virtuels sur un même réseau physique

- Chaque administrateur croit qu'il gère son propre réseau
- Un hyper administrateur gère le réseau physique



8. Autopilotage des réseaux et virtualisation

Virtualisation

- **Virtualisation des réseaux**
  - Concept de partage nouveau
  - Probablement plus de création de services réseau (les ISP)
  - Méfiance : sécurité pas totalement maîtrisée aujourd'hui
- **Challenges**
  - Modèles de virtualisation (abstraction) acceptés par tous
  - Garanties quant à la sécurité
  - Former de nouvelles génération d'administrateurs Réseaux

9. Développement des réseaux et services

9. Développement des réseaux et services

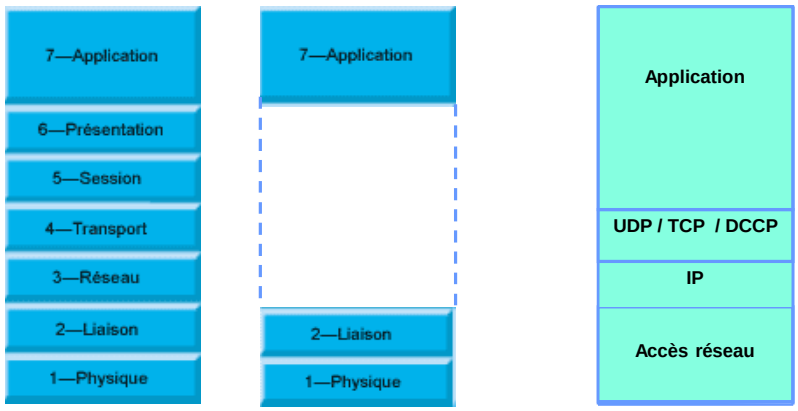
- Réseaux et services = Matériel et Logiciel
- Développement des réseaux et services
  - Méthodes de génie logiciel
    - Cycle de vie du logiciel (analyse des besoins, …, codage,…, maintenance)
    - Modularité, UML, types, objets,…
    - Langages de programmation (Java, C++, …)
    - Validation de programmes (preuve, test, simulation)
  - Autres disciplines
    - Informatique : Bases de données, IA
    - Mathématiques : théorie des graphes…
    - Automatique
    - Economie
    - Droit
    - …

9. Développement des réseaux et services

- Analyse de performances des réseaux et services
  - Méthodes de simulation
  - Méthodes analytiques (preuves de théorèmes)
  - Méthodes d'analyse de données statistiques
  - Théorie des files d'attente

10. Modèles en couches

Modèles de base

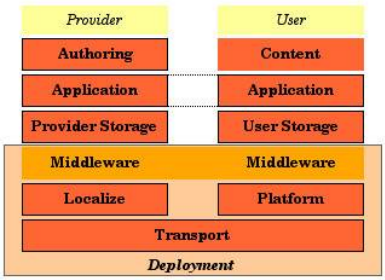


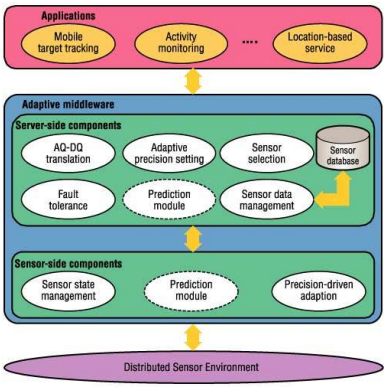
Modèle de référence OSI | Modèle IEEE (pour LAN) | Modèle TCP/IP

10. Modèles en couches

Nécessité d'avoir d'autres modèles

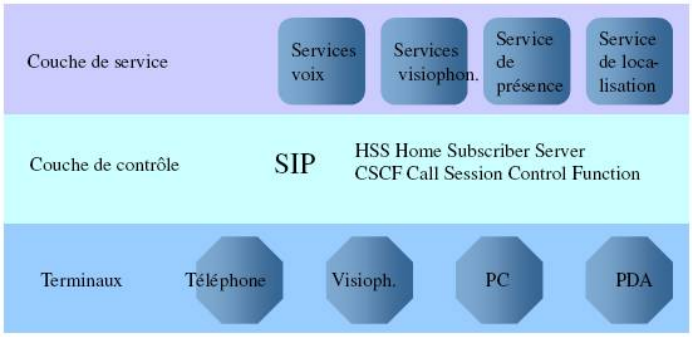
- Modèles OSI : couches peu représentatives de la complexité des réseaux et applications actuelles et futures
- Utilisation d'autres modèles





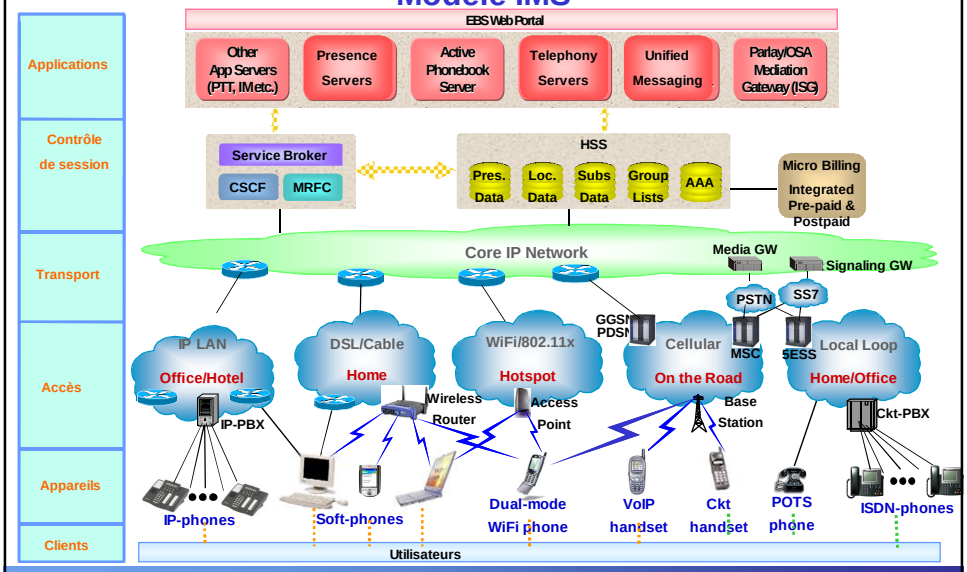
10. Modèles en couches

Modèle IMS (IP Multimedia Subsystem) – vue simplifiée



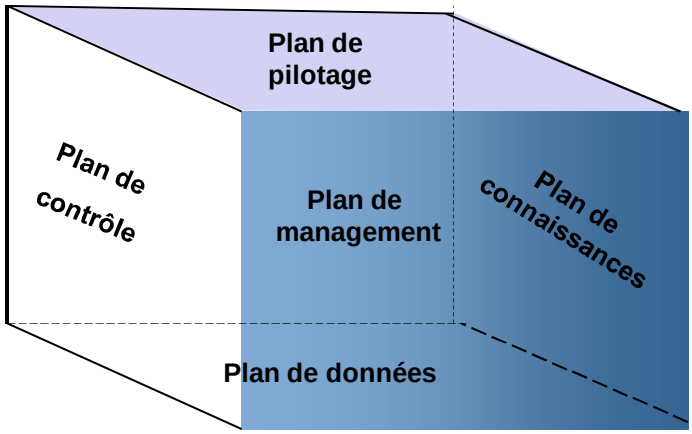
10. Modèles en couches

Modèle IMS



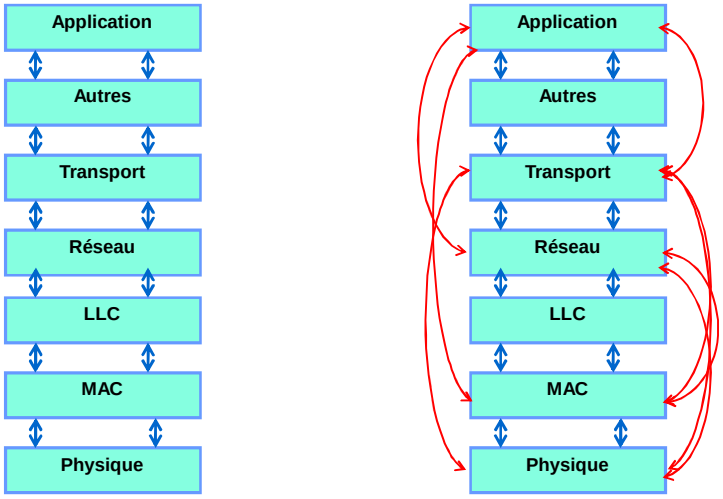
10. Modèles en couches

Modèles à *n* plans



10. Modèles en couches

Approche *cross-layer*



11. Organismes de standardisation

ISO IEC

IETF

IEEE

3G

Industriels influents

hp invent, NOKIA, Panasonic, Huawei Technologies, IBM, ST, FUJITSU, SAMSUNG, PHILIPS, lenovo, SONY, KENWOOD, NEC, intel, Pioneer, TOSHIBA, SHARP, THOMSON, Texas Instruments, MOTOROLA

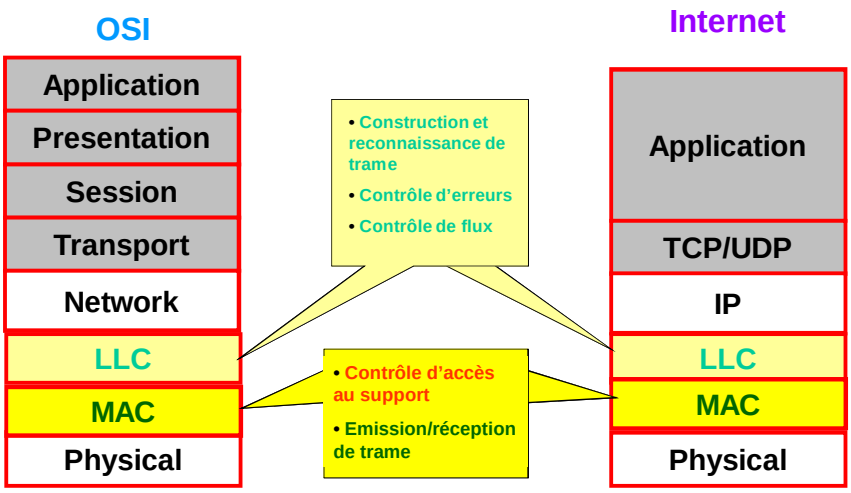
Chapitre 2

Méthodes d'accès au support de transmission dans les réseaux filaires et sans fil

(MAC : Medium Access Control)

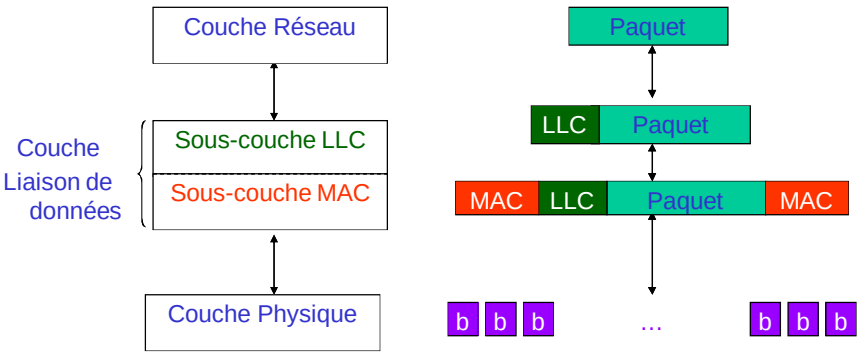
1. Généralités

Sous-couche MAC



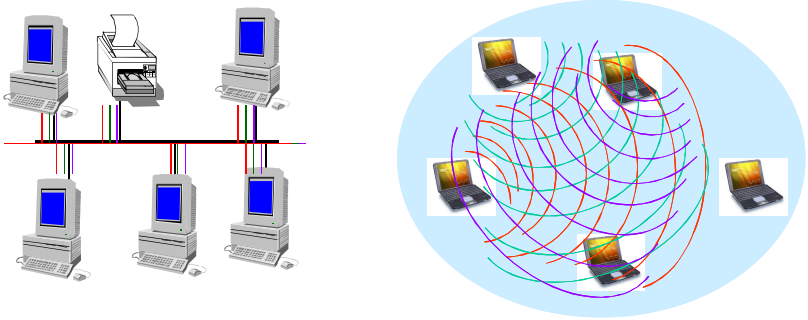
1. Généralités

Sous-couche MAC



1. Généralités

Accès au canal



Canal partagé par toutes les stations du réseau ➔ conflit d'accès

Choix de méthode d'accès appropriée

1. Généralités

Méthodes d'accès : 1ère classification

- Méthodes d'allocation statique (ou pseudo-statique)
  - Chaque émetteur a une part fixe du canal
  - Exemples : TDMA, FDMA, CDMA
- Méthodes d'allocation dynamique
  - Accès aléatoire (par compétition)
    - Chaque émetteur émet quand il peut
    - Exemples : ALOHA, CSMA/xx
  - Accès à tour de rôle :
    - Exemples : jeton, maître-esclave

1. Généralités

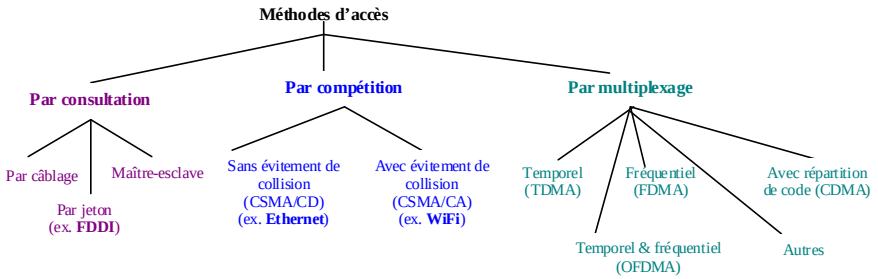
Méthodes d'accès : 2ème classification

- Méthodes accès par compétition (ou aléatoire)
  - Chaque émetteur essaie de prendre le contrôle du canal quand il le peut
  - Exemples : ALOHA, CSMA/xx
- Méthodes accès par accès ordonné
  - Chaque émetteur accède au canal quand son tour arrive
    - Exemples : Méthodes à jeton, TDMA, maître-esclave
  - Chaque émetteur accède au canal en utilisant la bande passante qui lui a été allouée
    - Exemple : FDMA

1. Généralités

Méthodes d'accès : 3ème classification

- Méthodes accès par compétition (ou aléatoire)
- Méthodes par consultation (dynamique)
- Méthodes par multiplexage



1. Généralités

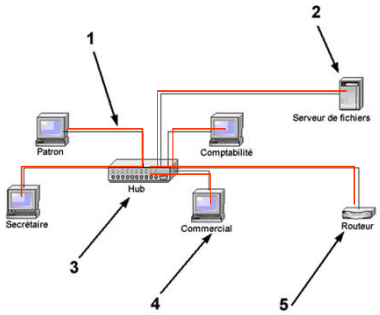
Choix de méthode d'accès

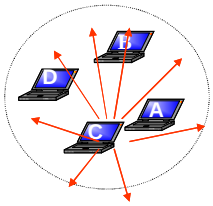
- **Monde Internet, bureautique, …**
  - Communications aléatoires, peu connues a priori
  - Pas de station centralisatrice des décisions (d'allocation du canal, de configuration des nœuds…)
  - Pas de contraintes de temps de réponse
  - Méthodes utilisées : CSMA/CD, CSMA/CA
- **Monde de la téléphonie ou multimédia en local**
  - Communications aléatoires mais périodiques
  - Contraintes de temps de réponse
  - Méthodes utilisées : TDMA, FDMA, CDMA
- **Monde Industriel et Embarqué**
  - Communications prévisibles (capteurs, actionneurs)
  - Fortes contraintes de temps de réponse (déterminisme exigé)
  - Méthodes utilisées : Jeton, Maître-esclave, CSMA/CR

2. Eléments sur la transmission sur un canal

Transmission sur un canal filaire

- **Transmission sur un réseau filaire**





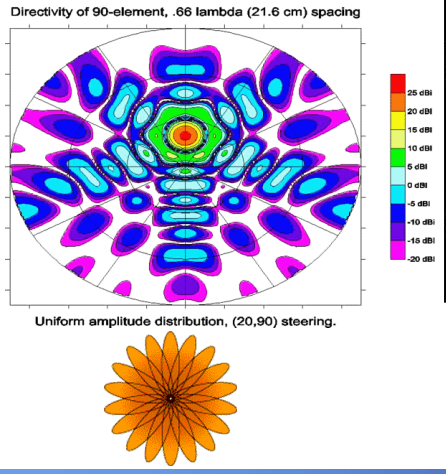
Cas idéal
(C transmet – tous les nœuds l'entendent)

- **Toutes les stations reçoivent le signal**
  (sauf cas particulier : collision, bruit…)

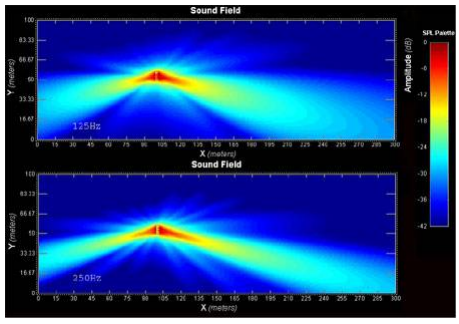
2. Eléments sur la transmission sur un canal

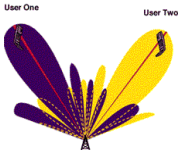
Transmission sur un canal sans fil - Antennes

Antenne non directionnelles
(omnidirectionnelles)



Antennes directionnelles

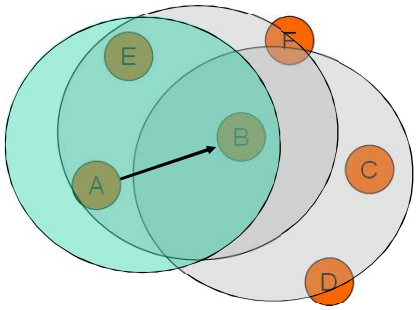




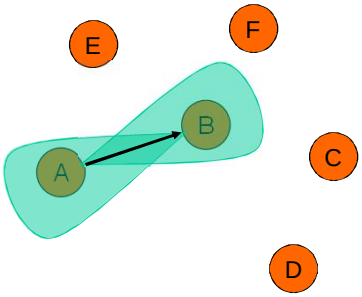
2. Eléments sur la transmission sur un canal

Transmission sur un canal sans fil - Antennes

Antenne non directionnelles (omnidirectionnelles)



Antennes directionnelles

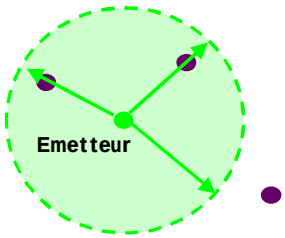


2. Eléments sur la transmission sur un canal

Transmission sur un canal sans fil

Portée/rayon de transmission

- Etendue où un paquet est reçu avec succès s'il n'y a pas d'interférence



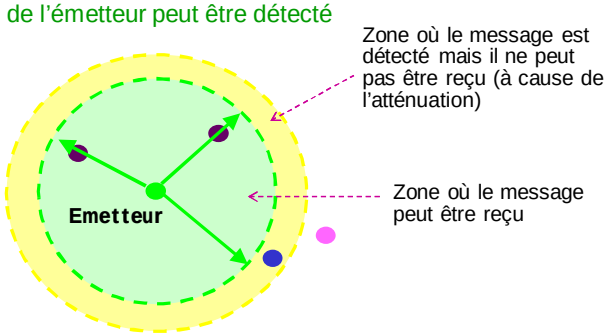
- Dépend de la puissance de transmission et atténuation de signal

2. Eléments sur la transmission sur un canal

Transmission sur un canal sans fil

Portée/rayon de détection de porteuse

- Etendue où le signal de l'émetteur peut être détecté



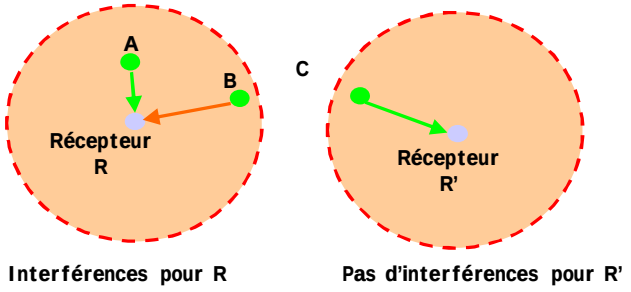
- Dépend de la sensibilité de l'antenne

2. Eléments sur la transmission sur un canal

Transmission sur un canal sans fil

Portée/rayon d'interférence

- Etendue où les signaux reçus par un récepteur peuvent interférer les uns sur les autres conduisant à des pertes



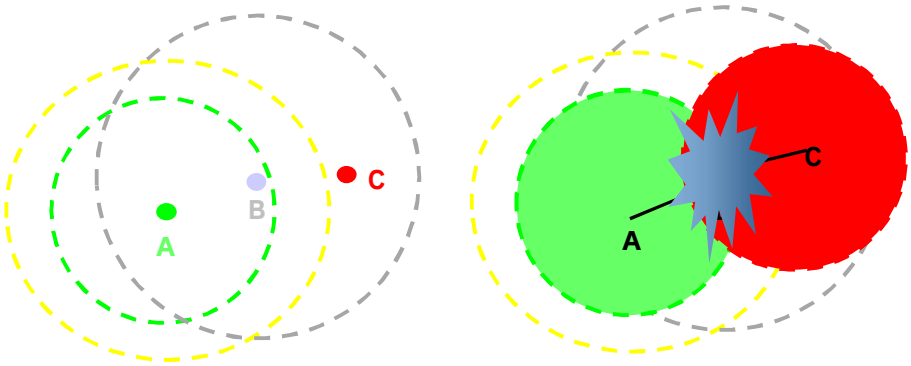
- Dépend de la sensibilité de l'antenne

2. Eléments sur la transmission sur un canal

Transmission sur un canal sans fil

Station cachée

- Toute station dans le rayon d'interférence d'un émetteur peut être une station cachée vis-à-vis de cet émetteur



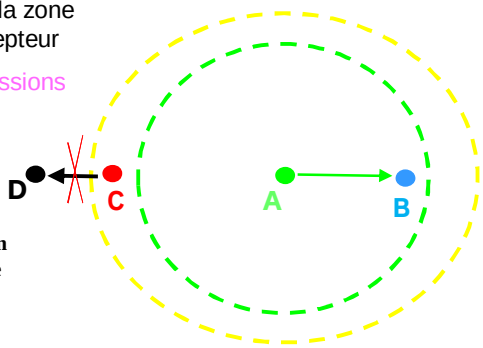
C est dans la zone d'interférence de B et elle est hors de la zone de détection de porteuse de A

2. Eléments sur la transmission sur un canal

Transmission sur un canal sans fil

Station exposée

- Toute station dans la zone de détection de porteuse de l'émetteur et hors de la zone d'interférence du récepteur
- Empêche les transmissions simultanées



C est dans la zone de détection de la porteuse de A et hors de la zone d'interférence de B.

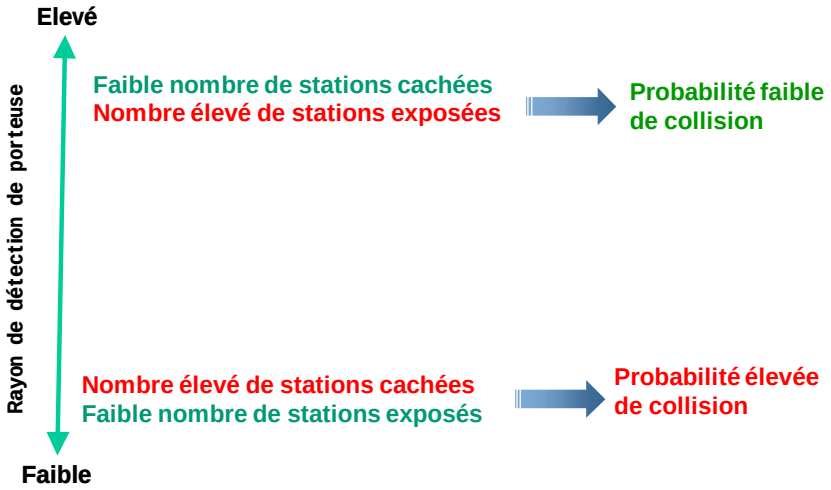
Si elle transmet en même temps que A, B ne sera pas gênée par sa transmission

C se prive de transmettre en même temps que A

2. Eléments sur la transmission sur un canal

Transmission sur un canal sans fil

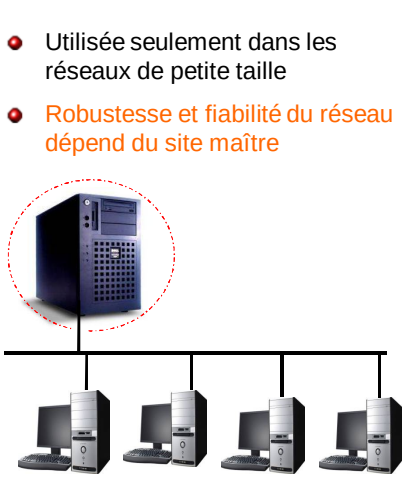
Performance d'un réseau sans fils

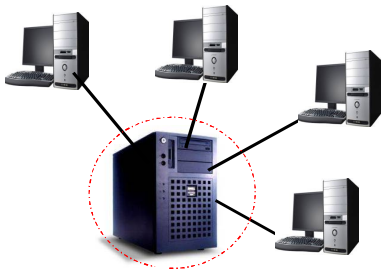


3. Méthodes par consultation

Méthode Primaire-secondaire (maître-esclave)

- Utilisée seulement dans les réseaux de petite taille
- Robustesse et fiabilité du réseau dépend du site maître





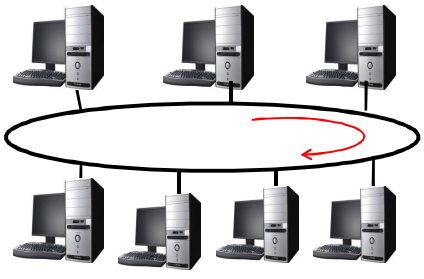
3. Méthodes par consultation

Méthode Primaire-secondaire – Principe général

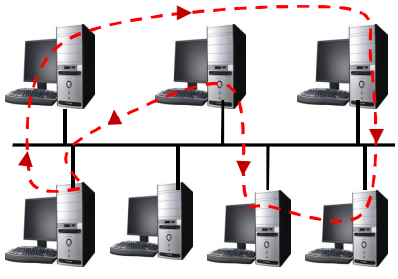
- **Passage du droit à transmettre**
  - Le maître donne le droit à transmettre au secondaire
  - Le secondaire transmet ses données
- Comment donner le droit de parole?
  - À tour de rôle (scrutation périodique)
  - Selon un ordre connu par le maître (eg. Système embarqués)
- Comment le secondaire rend t-il la main?
  - Implicitement : à la fin de transmission de sa trame
  - Explicitement : par une trame spéciale envoyée au maître (danger !)
- Comment le maître est-il choisi (élu) ?
  - De manière statique (par reconfiguration du réseau)
  - Dynamiquement (par une procédure d'élection)

3. Méthodes par consultation

Méthode à jeton circulant



Boucle à jeton



Anneau à jeton

Entête	Bits jeton	CRC

Jeton

Entête	@Dest	@Src	Bits jeton	CRC

Jeton

3. Méthodes par consultation

Méthode à jeton circulant

- **Principe général**
  - Les stations sont organisées en anneau
  - Un jeton passe de station en station
  - La station qui détient le jeton peut transmettre ses trames
  - La station qui finit de transmettre ses données libère le jeton
- Types de jeton
  - Simple (transmettre ce que l'on veut tant qu'on a le jeton)
  - Temporisé : transmettre pendant un laps de temps connu à l'avance
  - A priorité : transmettre des trames avec une priorité supérieure ou égale à celle du jeton reçu
- Aspects qui affectent les performances de la méthode
  - Création et maintenance de l'anneau
  - Surveillance et régénération du jeton

3. Méthodes par consultation

Méthode à jeton circulant

- **Avantages**
  - Garantie de bande passante pour chaque station
  - Garantie de délais bornés (pour les jetons temporisés)
- Inconvénients
  - Une station qui fonctionne mal peut monopoliser le jeton (famine !)
  - Effets négatifs de périodes transitoires de perte de jeton
  - Inefficacité en cas de charge faible (on consomme plus de la bande passante pour le passage du jeton que pour transmettre des données)
- Domaines d'utilisation
  - Réseaux locaux et PABX
  - Réseaux industriels et embarqués

4. Méthodes par compétition

- **Méthodes accès par compétition (accès aléatoire)**
  - ALOHA
  - CSMA (Carrier Sense Multiple Access)
    - CSMA/CD (CSMA with Collision Detection)
    - CSMA/CA (CSMA with Collision Avoidance)
    - CSMA/CR (CSMA with Collision Resolution)
    - CSMA/DCR (CSMA with Deterministic Collision Resolution)
  - CDMA

4. Méthodes par compétition

Méthode ALOHA

- La plus ancienne des Méthodes d'accès (début des 70's)
- Ancêtre de tous les protocoles CSMA/xx
- Deux variantes : ALOHA pure et ALOHA à tranches (Slotted ALOHA)

- **ALOHA pure**
  - Toute station peut transmettre dès qu'elle le souhaite (sans aucune précaution)
  - Après transmission, la station attend un Ack
  - Si l'Ack ne lui parvient pas au bout d'un délai fixé, elle retransmet sa trame
  - Inconvénient :
    - Rendement très mauvais en cas de charge élevée

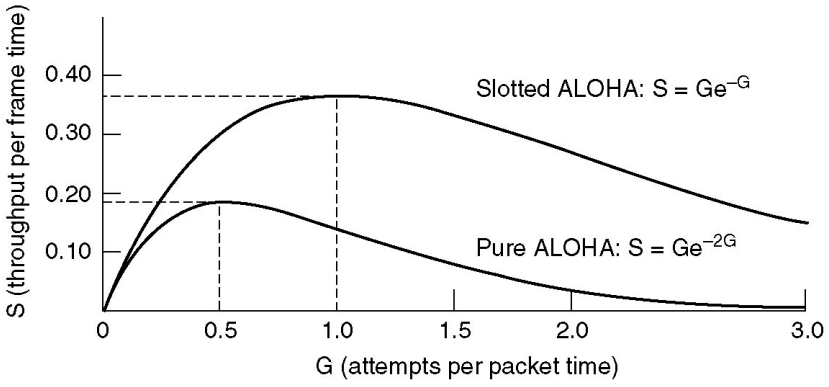
4. Méthodes par compétition

Méthode ALOHA

- **Slotted ALOHA**
  - Le temps est découpé en slots (la durée de slot a un impact sur les performances)
  - Toute station peut transmettre dès qu'elle le souhaite, mais elle doit commencer sa transmission au début d'un slot.
  - Inconvénients :
    - ♦ Nécessite une synchronisation des horloges pour repérer les débuts de slots
    - ♦ Rendement très mauvais en cas de charge élevée

4. Méthodes par compétition

Pure ALOHA vs Slotted ALOHA



Taux d'utilisation Max de ALOHA pure = 18%

Taux d'utilisation Max de Slotted ALOHA pure = 37%

4. Méthodes par compétition

Méthodes CSMA

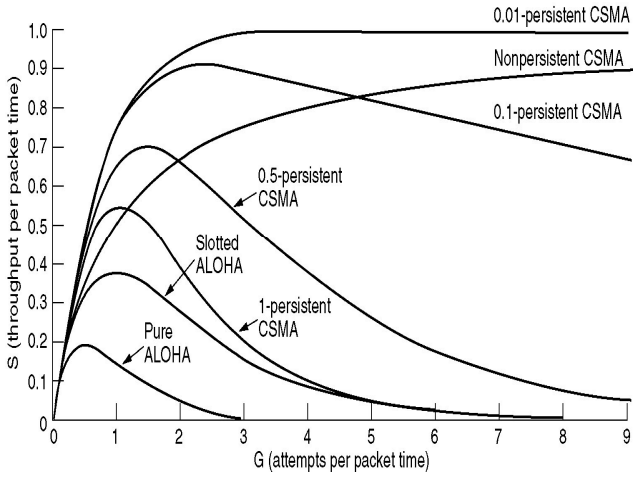
- **Améliorer ALOHA :** ne pas transmettre si le support est déjà occupé
- Analogie avec l'Homme : ne pas couper la parole aux autres

- **Variantes de CSMA**
  - 1-persistant : si le canal est libre, la station transmet immédiatement (proba = 1). Si le canal est occupé, elle attend qu'il redevienne libre (le test de l'état du canal est fait en continu). En cas de collision, la station attend une durée aléatoire avant de retenter sa transmission
  - *p*-persistant : si le canal est libre, la station transmet avec une probabilité *p*. Si le canal est occupé, elle attend le début du prochain slot et transmet ou pas avec une probabilité *p*.
  - Non-persistant : Si le canal est libre, la station transmet. Si le canal est occupé, elle ne teste pas en continu l'état du canal. Elle attend une durée aléatoire avant de le tester à nouveau.

4. Méthodes par compétition

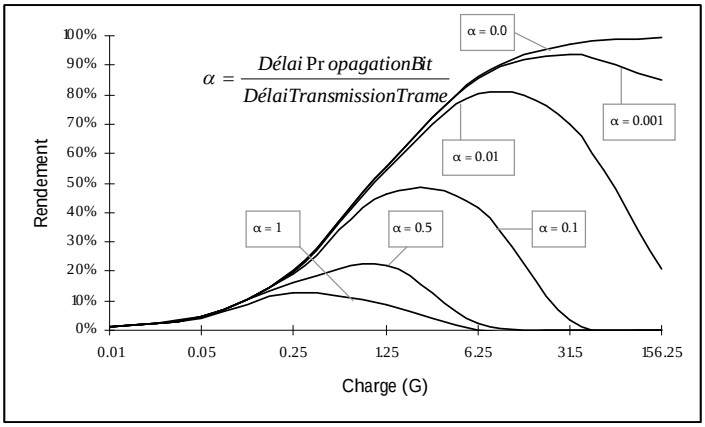
Comparaison de performance

(utilisation du canal vs charge)



4. Méthodes par compétition

Performance de CSMA
(utilisation du canal vs longueur)



Le taux d'utilisation dépend de la longueur du câble et de trame

4. Méthodes par compétition

Méthode CSMA - Backoff

- CSMA/xx sont des protocoles à *backoff* (protocoles à retrait)
- *Backoff* = ajourner d'une période calculée de manière aléatoire comprise entre *Vmin* et *Vmax* (*Vmin* est généralement = 1)

- Méthodes de calcul de la valeur max du backoff (Vmax)
  - Binaire exponentiel : après K tentatives de retransmission, **Vmax = 2^K**
  - Linéaire : après K tentatives, **Vmax = Vinit + K*incrément**
  - **Autres**

4. Méthodes par compétition

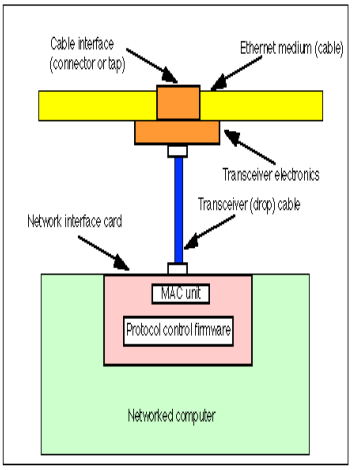
Méthode CSMA/CD

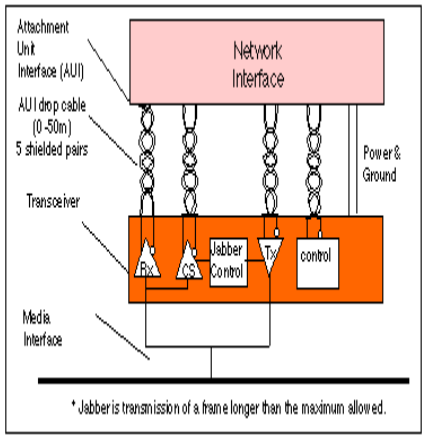
- **C'est la méthode la plus utilisée au monde**
- C'est la méthode d'Ethernet
- Standard IEEE 802.3 (ISO 8802.3)

- **Principe**
  - Si le canal est libre, transmettre immédiatement (1-persistant)
  - S'il est occupé attendre qu'il redevienne libre
  - Tester l'état du canal en même temps que la transmission. S'il y a une différence entre ce que transmet une station et ce qu'elle reçoit, il y a collision.
  - En cas de collision, envoyer des données de bourrage et arrêter la transmission. Attendre une durée aléatoire et tenter à nouveau la retransmission
- Détection de collision : facile dans les réseaux filaires, difficile (impossible) dans les réseaux sans fils

4. Méthodes par compétition

Méthode CSMA/CD – Détection de collision

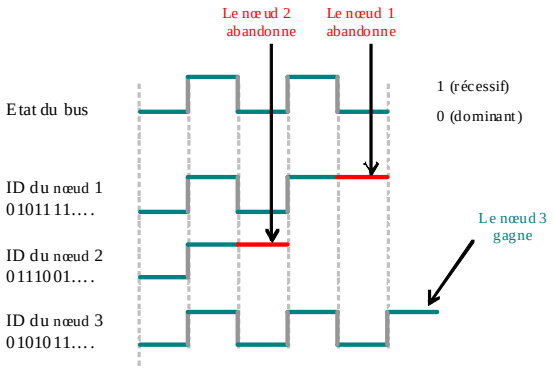




4. Méthodes par compétition

Méthode CSMA/CR

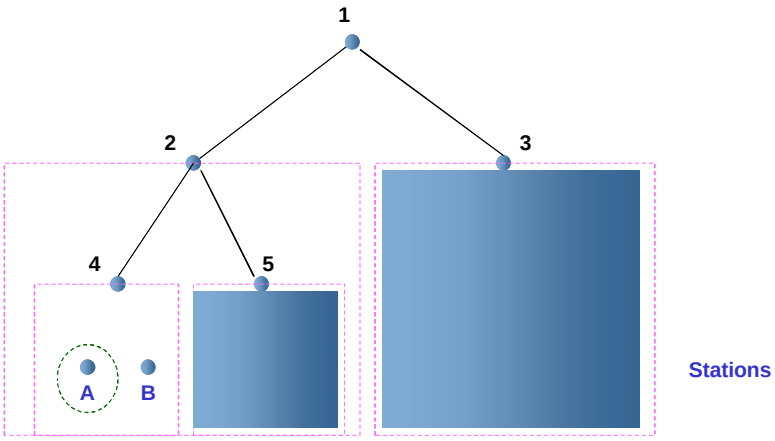
- **L'arbitrage se fait bit à bit**
- Les collisions ne sont pas destructrices
- Utilisé par le réseau CAN (un standard dans l'automobile)



4. Méthodes par compétition

Méthode CSMA/DCR

- **Utilisation d'un algorithme basé sur l'arborescence des adresses pour résoudre les collisions : une station finit par s'imposer**



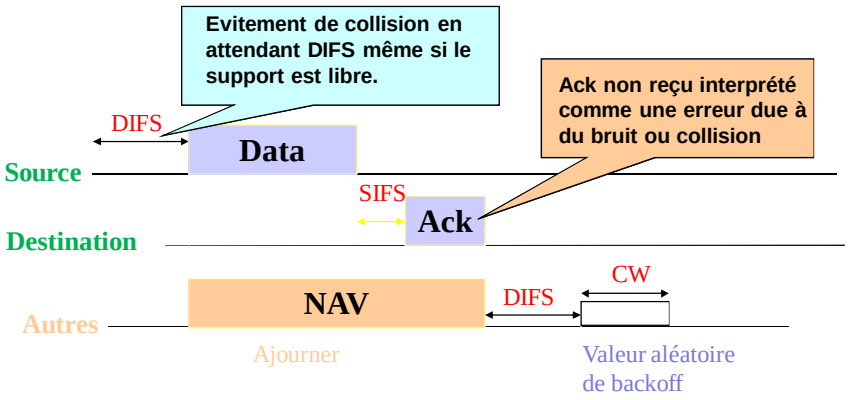
4. Méthodes par compétition

Méthode CSMA/CA – Pour réseaux sans fils

- **CSMA/CD n'est pas utilisable dans les réseaux sans fils**
- **Causes :** Détection de collisions pendant la transmission
  - Très coûteuse (voire impossible)
    - Les liaisons radio ne sont pas en full duplex
    - La puissance en émission est différente de celle en réception
    - Les signaux sont affaiblis (d'où difficulté de comparer)
  - Inefficace : existence de stations cachées ou exposées
- **CSMA/CA : méthode du Wifi – std IEEE 802.11**
- **Plusieurs protocoles en CSMA/CA**
  - CSMA/CA (simple) basé sur les acquittements
  - CSMA/CA basé sur la réservation
  - Autres : plus complexes

4. Méthodes par compétition

Méthode CSMA/CA – simple



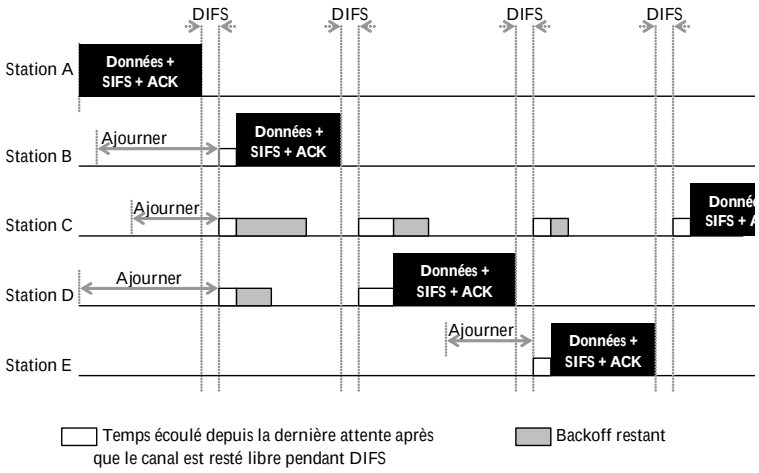
DCF : Distributed Coordination Function PCF : Point Coordination Function

IFS : interFrame Space DIFS : DCF IFS SIFS : Short IFS PIFS : PCF IFS

Problème: ne prend pas en compte les stations cachées

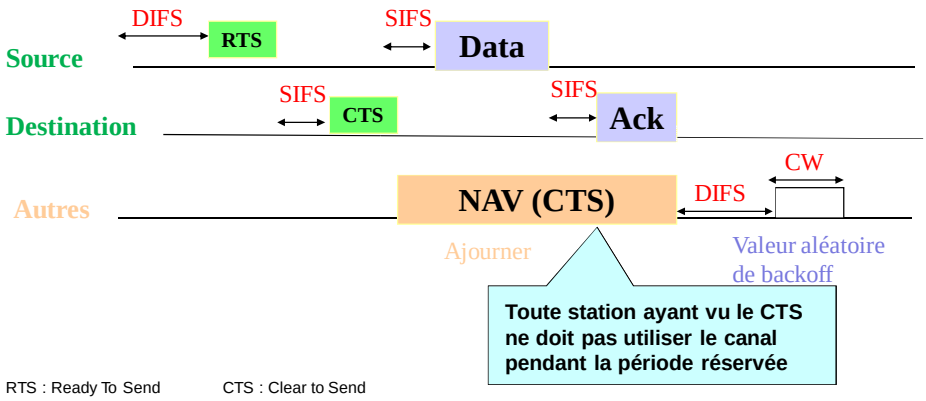
4. Méthodes par compétition

Méthode CSMA/CA – simple (exemple)



4. Méthodes par compétition

Méthode CSMA/CA – Avec réservation

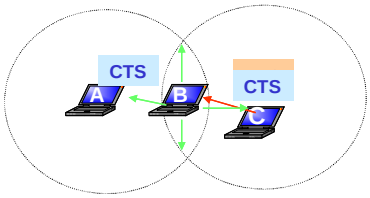


RTS : Ready To Send CTS : Clear to Send

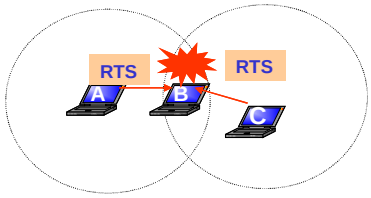
4. Méthodes par compétition

Méthode CSMA/CA – Avec réservation

- Le mécanisme RTS/CTS prend en compte le problème de la station cachée



A, B et C savent que le canal est réservé



B ne répond pas par un CTS

- Il a un surcoût
- Utilisé surtout quand les trames de données ont une taille importante (pour les trames de petites tailles, il faut envoyer directement la trame sans passer par la réservation)

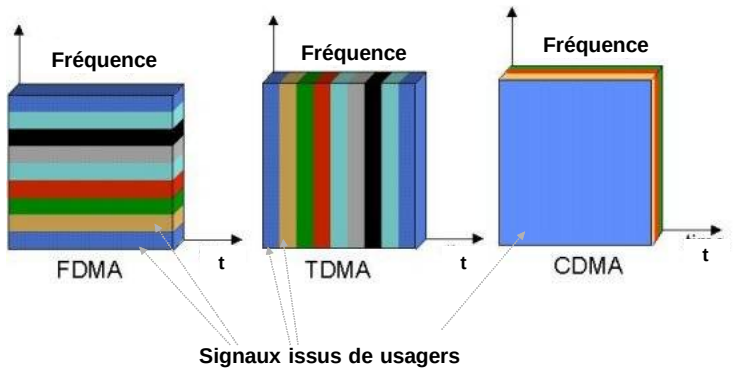
5. Méthodes par multiplexage

Multiplexage – "International Cocktail Party"

- Des personnes (nombreuses) se retrouvent à un cocktail pour discuter deux à deux.
- Comment peuvent-elles parler et se comprendre ?
- Solutions avec une seule pièce
  - Chaque paire de personnes parle à son tour pendant x sec (TDMA)
  - Plusieurs paires (qui utilisent des langues différentes) peuvent parler en même temps (CDMA) – parler à voix basse (sinon les autres ne s'entendent plus)
- Solutions avec plusieurs petites pièces
  - Chaque paire prend une petite pièce pour discuter (FDMA, OFDM)
  - Plusieurs paires partagent une même pièce et parlent à tour de rôle (OFDMA)
  - Plusieurs paires partagent une pièce et utilisent des langues différentes pour parler en même temps (COFDMA)

5. Méthodes par multiplexage

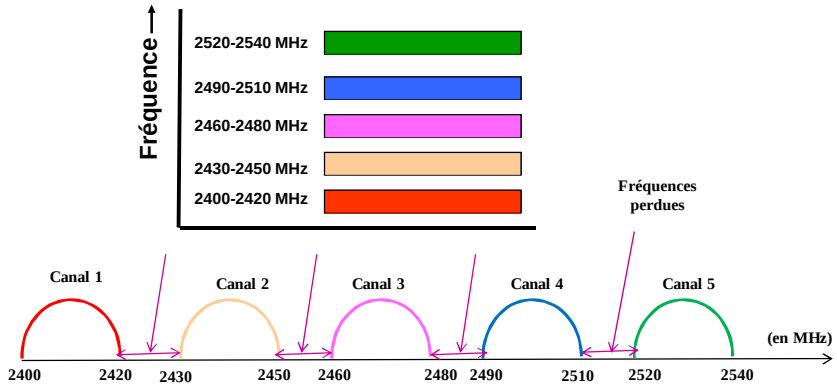
Formes de multiplexage



5. Méthodes par multiplexage

FDMA (Frequency Division Multiple Access)

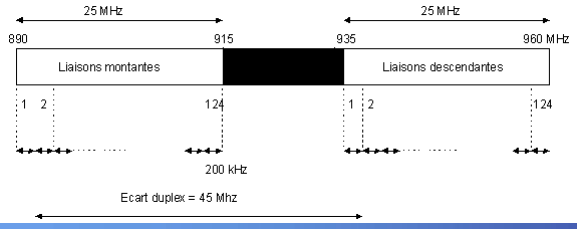
- **Le spectre de fréquences est subdivisé en canaux (dits aussi sous-canaux)**
- Chaque émetteur utilise la bande de fréquences qui lui allouée le temps d'un appel (connexion)

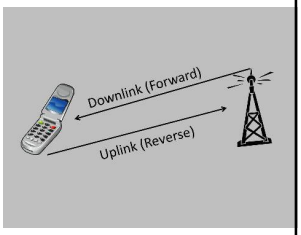


5. Méthodes par multiplexage

FDMA – Exemple GSM (Bande des 900 MHz)

- La bande est subdivisée en canaux
  - 2 fois 25 MHz de bande ont été alloués (*uplink* et *downlink*)
  - Largeur des canaux étant de 200 kHz
  - On obtient 124 canaux duplex qui ont été répartis entre les opérateurs (ex. SFR utilise 63 à 124)
  - Les bandes des deux liaisons sont séparées par 20 MHz, ce qui porte à 45 MHz l'écart duplex
  - L'écart duplex entre fréquences émission et réception du mobile est de 45 Mhz





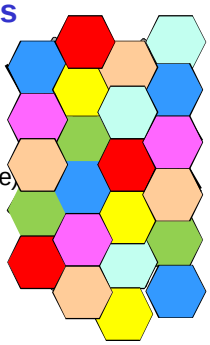
5. Méthodes par multiplexage

FDMA – Exemple GSM (Bande des 900 MHz)

- Capacité théorique du réseau
  - Bande disponible 915 – 890 MHz = 25 MHz
  - Sous Bandes disponibles 25 / 0,2 = 125 bandes
  - Nombre d'intervalles de temps 125x8 IT =1000 ➔
    soit 1000 utilisateurs simultanés par zone

5. Méthodes par multiplexage

FDMA – Avantages et inconvénients



- **Avantages**
  - Simple au niveau algorithmique
  - Réutilisation de fréquences dans les systèmes cellulaires
  - Equitable quand le trafic est uniforme/constant (eg. Téléphonie)
  - Pas besoin de synchroniser les horloges des stations
  - Adaptée à n'importe quel type de modulation
- **Inconvénients** :
  - Les sous-bandes utilisées pour séparer les canaux (i.e. de garde) sont perdues
  - Le débit max dépend de la largeur des canaux
  - Nécessite plus de capacités de filtrage pour s'adapter à différents canaux et éviter les perturbations venant des canaux voisins
  - Une bande allouée ne peut plus être utilisée même si la station à laquelle elle a été allouée est silencieuse

5. Méthodes par multiplexage

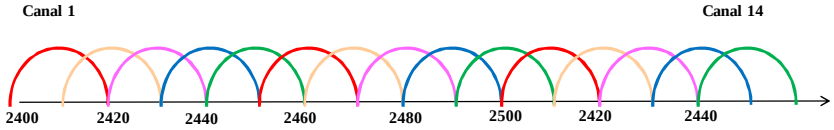
Variantes de FDMA : OFDM et OFDMA (1)

- **Répondre au problème de canaux de garde de FDMA**
- **Deux méthodes**
  - OFDM (Orthogonal Frequency Division Multiplexing)
  - OFDMA (Orthogonal FDM Access)
  - Utilisées dans les réseaux Wifi, WiMAX et UMTS
  - Utilisées pour la transmission de TNT et Radio NT

5. Méthodes par multiplexage

Variantes de FDMA : OFDM (2)

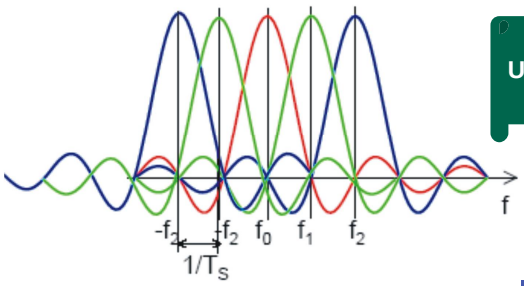
- **OFDM**
  - Découpage du spectre de fréquences en canaux (comme FDM) sans perte de fréquences due à l'espacement entre sous-canaux
  - La transmission s'effectue Symbole par Symbole (un symbole = plusieurs bits)
  - Chaque symbole commence par un préfixe connu
  - La réception se fait Symbole par Symbole
  - Les symboles sont transmis en parallèle sur des canaux orthogonaux (les signaux émis sur deux sous-canaux orthogonaux sont toujours distingués à la réception)



5. Méthodes par multiplexage

Variantes de FDMA : OFDM (3)

- OFDM = Orthogonal FDM
- La transmission de symboles s'effectue sur de multiple porteuses dont les fréquences sont orthogonales
- ORTHOGONALITE : la puissance maxi d'une fréquence est nulle sur les fréquences voisines.
- Les fréquences porteuses sont séparées par 1/Ts (Ts : Temps de transmission d'un symbole)

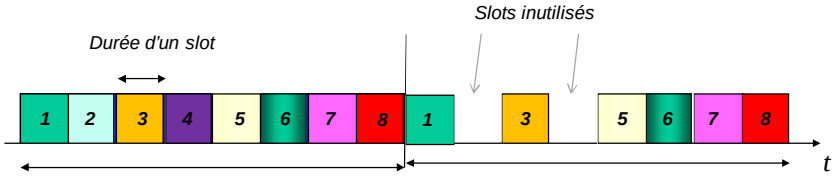


Utilisation des FFT

5. Méthodes par multiplexage

TDMA

- **Principes de base**
  - Le temps est découpé en supertrames (trames temporelles) de même taille
  - Chaque supertrame est découpée en slots de taille fixe
  - Dans chaque supertrame, chaque station *i* a le droit d'utiliser N_i slots
  - Technique de service : Round Robin
  - Tout slot laissé libre par une station ne peut être utilisé par les autres stations



Durée de la supertrame

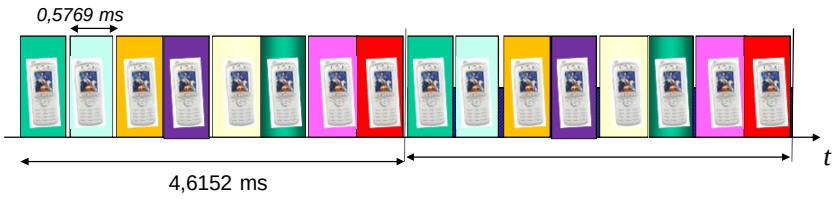
5. Méthodes par multiplexage

TDMA – Exemple du GSM

- **Parole (voix téléphonique)**
  - La parole occupe une bande de {300 Hz ; 3400 Hz }
  - La parole est échantillonnée à 8 kHz et chaque échantillon est représenté sur 8 bits, ce qui donne un débit de 64 kbit/s
  - Le signal est découpé en intervalles de 20 ms
  - Chaque intervalle est numérisé puis comprimé
  - Le codec de parole transforme des segments de 20 ms de parole en blocs de 260 bits, ce qui correspond à un débit de 13 kbps
- **Application de TDMA dans le GSM**
  - Le temps de chaque canal est découpé en supertrames de 8 slots
  - Un *slot* dure *de* 0,5769 ms. La supertrame dure 4,6152 ms
  - Chaque mobile accède au réseau de manière discontinue dans le temps. Il envoie des rafales d'informations d'une durée de 156 bits
  - Sur chaque canal de 200 kHz, la transmission s'effectue à 270.833 kb/s, en utilisant la modulation GMKS (Gaussian minimum-shift keying)

5. Méthodes par multiplexage

TDMA – Exemple du GSM



Limite d'une cellule

Meilleur des cas : 124 canaux utilisés (par tous les opérateurs)

Nombre max de communications simultanées : 124*8 = 992

5. Méthodes par multiplexage

TDMA – Variantes

- **Deux formes de TDMA**
  - TDMA synchrone
    - Toutes les stations ont droit au même nombre de slots
    - Inefficace en présence de trafics diversifiés
    - Adaptée aux réseaux d'acquisition de données
  - TDMA statistique
    - Chaque station a droit a un nombre de slots qui répond à ses besoins
    - Plus équitable
    - Plus difficile à mettre en œuvre

5. Méthodes par multiplexage

TDMA

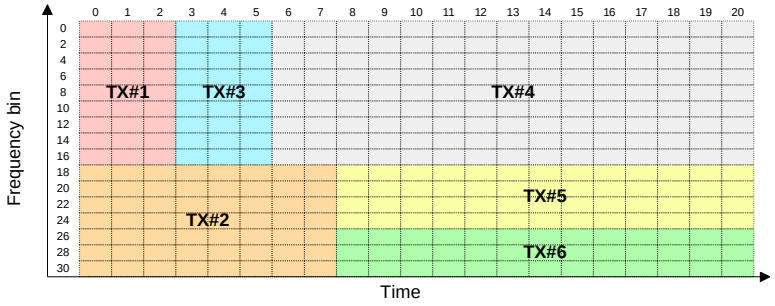
- **Avantages**
  - Débit flexible (avec TDMA statistique seulement)
  - Pas de fréquences de garde perdues
  - Filtre de fréquence simple (pas besoin de s'adapter à différentes bandes de fréquences)
  - Durée de batterie plus élevée
  - Autres
- **Inconvénients**
  - Nécessité d'horloges synchronisées tout le temps
  - Autres (distorsion quand les signaux se propagent sur plusieurs chemins…)

TDMA non adaptée aux réseaux de grande taille à cause des problèmes de synchronisation d'horloges

5. Méthodes par multiplexage

Variantes de FDMA : OFDMA

- **OFDMA = OFDM + TDMA (à l'intérieur des canaux)**



TX#i : désigne la station i

5. Méthodes par multiplexage

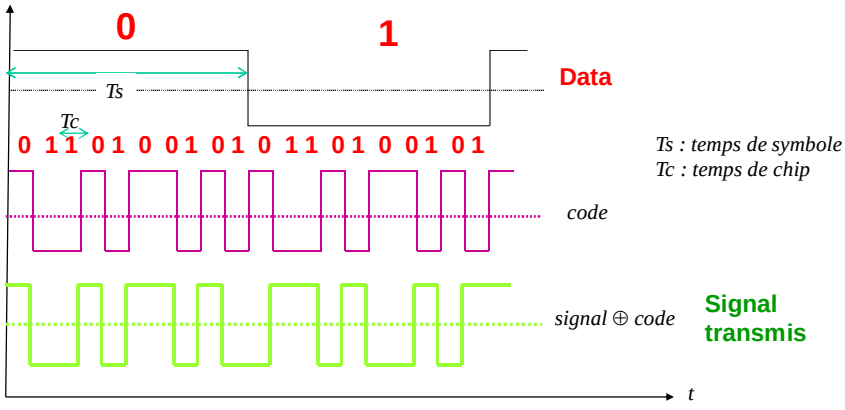
CDMA (code division multiple access)

- **Principes de base**
  - Méthode développée à l'origine par les militaires
  - Résiste aux brouillage et interférences
  - Plusieurs stations utilisent une même bande de fréquence et peuvent transmettre en même temps
  - Chaque station utilise son code propre pour transmettre
  - La quasi-totalité des réseaux 3G ont adopté CDMA (dans les réseaux UMTS, on parle de W-CDMA)

5. Méthodes par multiplexage

CDMA

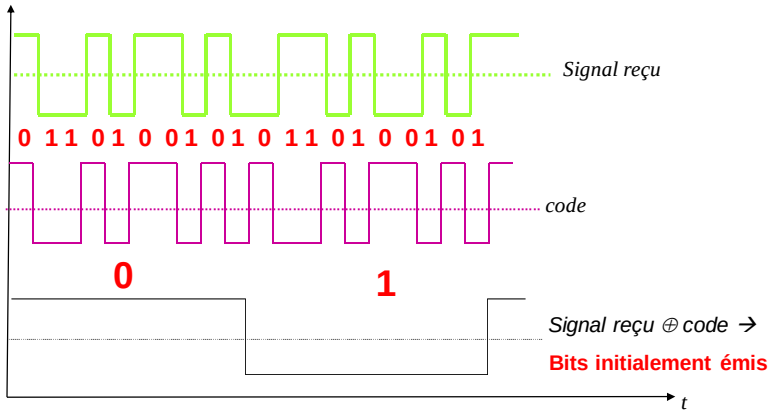
- Code = une suite de *n* bits connue de l'émetteur et récepteur
- Chaque bit (1 ou 0) à transmettre est multiplié par le code et on transmet n bits. On parle d'étalement de spectre.



5. Méthodes par multiplexage

CDMA

- Réception : on multiplie le signal reçu par le code



5. Méthodes par multiplexage

CDMA

- Les codes utilisés par *m* stations partageant la même bande de fréquences doivent être orthogonaux deux à deux

- Deux codes C_A et C_B sont orthogonaux ssi leur produit scalaire est nul :

$$C_A \bullet C_B = \sum (C_{A,i} \times C_{B,i}) = 0$$

Exemple : C_A = **<1, -1, -1, 1, -1, 1>** et C_B = **<1, 1, -1, -1, 1, 1>**

1	-1	-1	1	-1	1
1	1	-1	-1	1	1
1	-1	1	-1	-1	1

→ **Somme = 0**

5. Méthodes par multiplexage

CDMA

- **Transmissions simultanées**
  - Les signaux s'additionnent sur le canal
  - Les récepteurs reçoivent une sorte de 'bruit'
  - Le récepteur cible (qui connaît le code d'émission) retrouve les bits émis (sauf en cas d'erreur de transmission) en faisant la corrélation entre le code et le signal reçu sur le canal

- **Exemple**
  - Source A :
    - Data transmise = D_A = 100 représentée par < 1 -1 -1 >
    - Code de A = C_A = < 1 -1 -1 1 >
  - Source B :
    - Data transmise = D_B = 001 représentée par < -1 -1 1 >
    - Code de B = C_B = < 1 -1 1 -1 >

5. Méthodes par multiplexage

CDMA

- $D_A \times C_A$ = <1 -1 -1> × <1 -1 -1 1> = { <1 -1 -1 1>, <-1 1 1 -1>, <-1 1 1 -1> }
- $D_B \times C_B$ = <-1 -1 1> × <1 -1 1 -1> = { <-1 1 -1 1>, <-1 1 -1 1>, <1 -1 1 -1> }
- $D_A \times C_A$ et $D_B \times C_B$ sont transmis simultanément
- Les récepteurs reçoivent : $D_A \times C_A + D_B \times C_B$ = { <0 0 -2 2>, <-2 2 0 0>, <0 0 2 -2> }
- Récepteur légitime du message A
  - $C_A \times (D_A \times C_A + D_B \times C_B)$ = { <0 0 2 2>, <-2 -2 0 0>, <0 0 -2 -2> }
  - il retient la moyenne des signaux reçus sur la durée d'un bit initial : (0+0+2+2)/4 = 1, (-2-2+0+0)/4 = -1, (0+0-2-2)/4 = -1. Ce qui permet de retrouver la séquence <1 -1 -1> et ensuite la chaîne initiale '100'.

5. Méthodes par multiplexage

CDMA – Avantages et inconvénients

- **Avantages**
  - Plusieurs stations peuvent transmettre en simultané sur la même bande de fréquences
  - Plus de résistance aux interférences
  - Ajout de nouveaux utilisateurs plus facile
  - Sécurité au niveau physique (quasi-impossibilité d'intercepter les signaux)
  - Les handovers sont facilités
- **Inconvénients**
  - L'étalement de spectre est très consommateur en bande passante
  - Plus il y a d'utilisateurs, plus de codes distincts doivent être utilisés
  - Autres

5. Méthodes par multiplexage

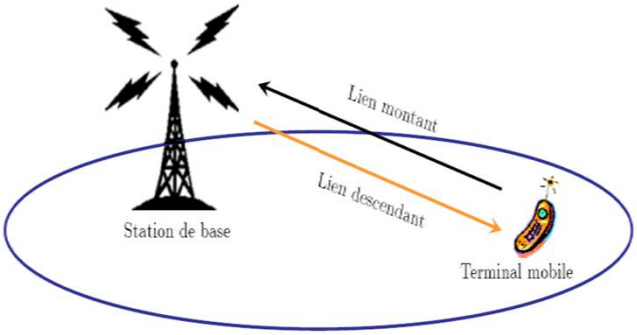
Contrôle d'allocation dans TDMA, FDMA et CDMA

- **Comment allouer les fréquences (dans FDMA), les slots (dans TDMA) et les codes (dans CDMA) ?**
- **Solutions statiques** (***Fixed-assignment multiple access*** **: FAMA**)
  - Chaque émetteur est configuré manuellement ou préconfiguré pour utiliser une bande, un code ou des slots fixes
  - Peuvent conduire à une sous-utilisation (en cas de silence) du réseau
  - Ne réagissent pas à la variation des demandes des utilisateurs
  - Ne sont utilisées que pour les configurations statiques (ex. les satellites et leurs stations au sol)

5. Méthodes par multiplexage

Contrôle d'allocation dans TDMA, FDMA et CDMA

- **Solutions dynamiques** **(Dynamic-assignment multiple access : DAMA)**
  - Un ou plusieurs canaux ou des slots sont laissés libres.
  - Une station connue (station de base, point d'accès..) contrôle les allocations
  - Chaque station qui démarre utilise ces canaux ou slots (en compétition) pour acquérir une bande de fréquences, des slots ou un code



6. Conclusion

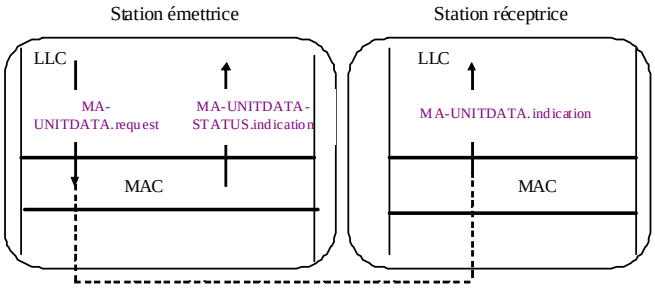
Autres mécanismes des Méthodes d'accès

- **Méthodes d'accès sensibles à l'énergie**
  - Energie = facteur important pour les réseaux mobiles
  - Consommation d'énergie
    - Mode transmission : consommation très élevée
    - Mode réception : consommation faible
    - Mode veille : consommation très faible
  - Le protocole MAC doit gérer les transitions entre les modes de consommation (tâche complexe)
- **Méthodes d'accès sensibles à la qualité de service**
  - Applications multimédia exigeantes en termes de QoS (délai et débit)
  - Le protocole doit garantir (ou aider à garantir) la QoS

6. Conclusion

Primitives de niveau MAC

- MA-UNITDATA.request
- MA-UNITDATA.indication
- MA-UNITDATA-STATUS.indication



Chapitre 3

Réseau Ethernet

1. Introduction

Ethernet en bref

- Introduit par Metcalfe au début des années 70 (73-74)
- Commercialisé par Intel, Xeroc et Dec en 1976
- Premier réseau local « opérationnel » au monde
- Le réseau d'accès à Internet le plus utilisé au monde (+95 %)
- Basé sur la méthode d'accès CSMA/CD (i.e. CSMA 1-persistant)
- Initialement introduit pour fonctionner sur un bus en câble coaxial à 1-10 Mb/s
- Etendue souvent limitée (point faible)
- Le plus robuste et le plus équitable (point faible pour la QoS)

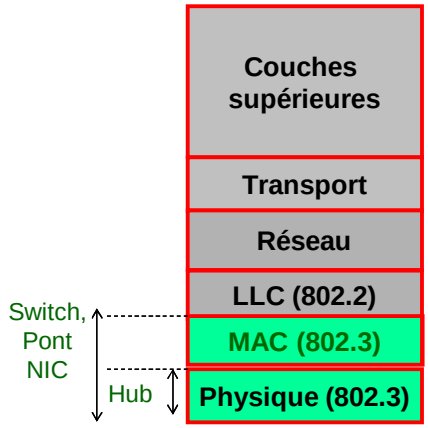
1. Introduction

Ethernet en bref

- Aujourd'hui :
  - Tous les supports : coaxial, fibre optique, paire métallique
  - Bus, étoile, arbre
  - Débits de 10 Mb/s à 10 Gb/s et même 100 Gb/s (std IEEE P802.3ba approuvé en juillet 2008)
  - de quelques dizaines de mètres à des dizaines de Km
- Demain : Ethernet partout (Réseau MAN … Réseau de cœur)
- Evolution du standard :
  - Environ 200 pages début des années 80 → des milliers de pages pour couvrir différents débits, différentes topologies, fonctionnalités et contraintes (énergie…)
  - Des dizaines de standards

1. Introduction

Ce que couvrent les standards Ethernet



NIC : Network Interface Card

1. Introduction

Exemples de NIC Ethernet

Carte NIC Ethernet - RJ45

Ethernet 10/100 BaseT RJ45

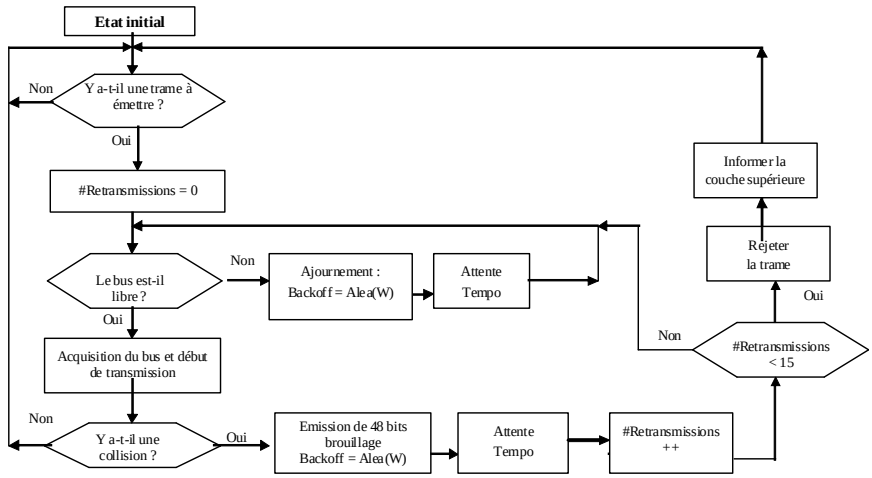
MAC
+ Physique

Adaptateur USB Ethernet

Carte Ethernet Gigabit

2. Sous-couche MAC

Principe de CSMA/CD



Le signal de brouillage (1 et 0 alternés) sert à s'assurer que toutes les stations détectent la collision

2. Sous-couche MAC

Calcul de la valeur de backoff

- Backoff = *R*Temps_de_base*

  R = Random(0, 2^L)

  L = min(K, 10)

  K : nombre de transmissions déjà effectuées

- *Temps_de_base = temps de transmission de 512 bits (64 octets)*

  = Temps de transmission d'une trame de longueur min

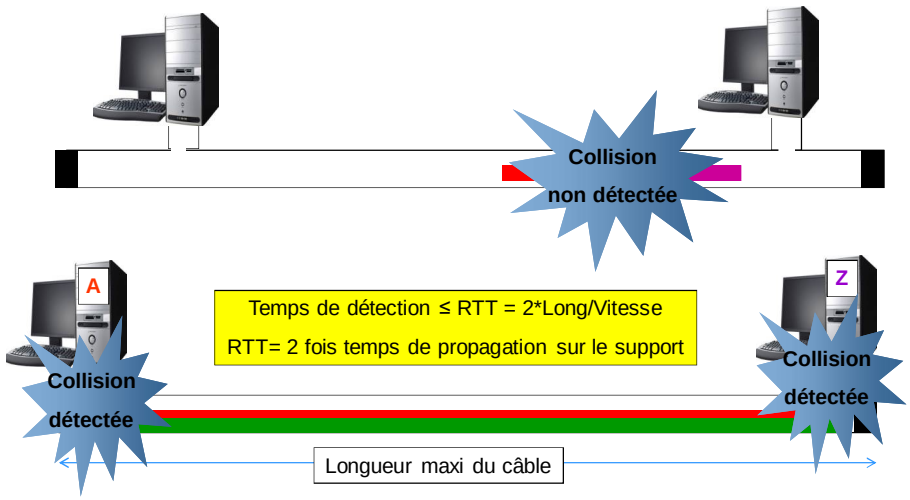
  ≥ Temps maximum d'aller-retour du signal sur tout le réseau

  (i.e. 51.2 µs à 10 Mb/s et 0,512 µs à 1 Gb/s)

- Le temps d'attente maxi est borné par 2^{10} ➔ pas d'attente infinie
- Le nombre maxi de retransmissions borné ➔ informer la couche supérieure, ne pas saturer le réseau inutilement

2. Sous-couche MAC

Détection de collision



2. Sous-couche MAC

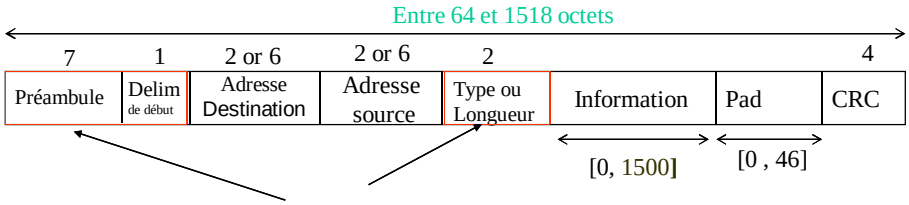
Valeurs par défaut des paramètres de configuration

	1, 10 et 100 Mb/s	1 Gb/s	10 Gb/s
Temps de base	≈ 512 bits	≈ 4096 bits	Non applicable
Gap inter-trames	96 bits	96 bits	96 bits
Nombre de bits de brouillage	32	32	32
Nombre de retransmissions	16	16	Non applicable
Taille maximale de trame	1518 octets	1518 octets	1518 octets
Taille minimale de trame	64 octets	64 octets	64 octets

Ces valeurs ont des impacts sur les performances du réseau

2. Sous-couche MAC

Format de trame Ethernet



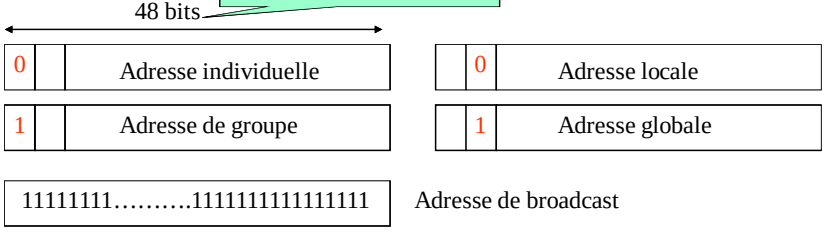
IEEE 802.3 : 7 +1 octets et *Longueur*
Ethernet : 8 octets et *Type*

GIT : Gap interTrame : silence pendant l'équivalent de 96 bits
(permet aux stations de se préparer pour recevoir la trame suivante)

2. Sous-couche MAC

Format des adresses Ethernet

Les adresses sur 16 bits sont quasi-inutilisées



- Avec 6 octets : 2^{46} adresses globales possibles
- Adresse Ethernet ≠ Adresse IP
- Il y a plus d'adresses Ethernet que d'adresses IPv4
- Adresses figées sur silicium (l'IEEE octroie les numéros aux constructeurs)
- Autrefois : l'utilisateur fixait lui-même les adresses (source d'erreurs !)

2. Sous-couche MAC

Format des adresses Ethernet

- Pourquoi @MAC ≠ @IP **?**
- Plusieurs explications
  - Distinguer les adresses physiques des adresses logiques
  - @MAC liée à une machine sur un réseau. Si la station se déplace (nomadisme ou mobilité) : risque de conflit d'adresse – Ce n'est plus vrai aujourd'hui (chaque @MAC est choisie de manière unique au moment de la fabrication de la carte Ethernet)
  - Séparer le business du niveau MAC de celui du niveau Réseau (éviter le monopole de technologie)

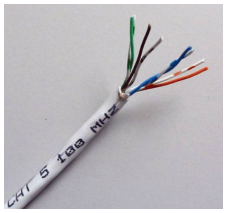
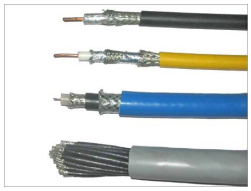
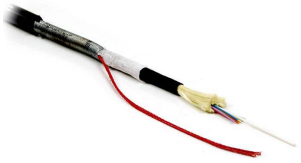
3. Couche physique

Fonctions de la couche physique

- Emission et réception de bit
- Codage et décodage de bit
- Génération de préambule
- Détection de collision
- Génération d'horloges pour la synchronisation
- Test de fonctionnement de la ligne de transmission

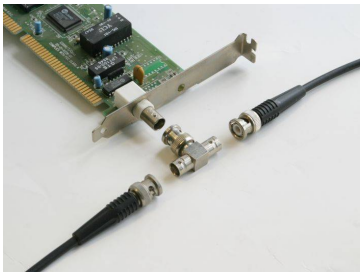
3. Couche physique

Supports et connecteurs

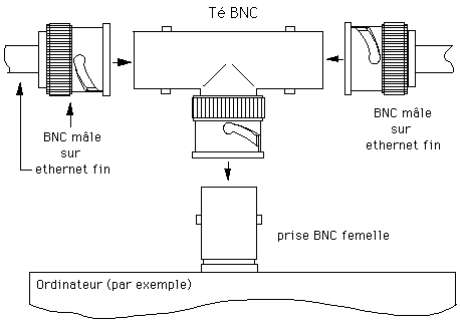





3. Couche physique

Raccordement – Thin Ethernet (Coax)



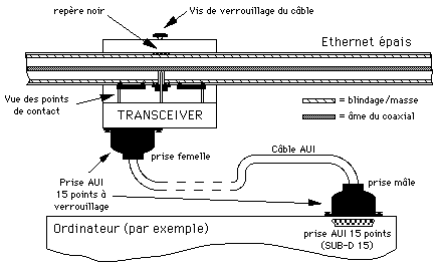
Thin Ethernet



- Facile à installer
- Coût réduit
- Sensible aux bruits
- Atténuations des signaux
- Nombre réduit de stations

3. Couche physique

Raccordement – Thick Ethernet (Coax)



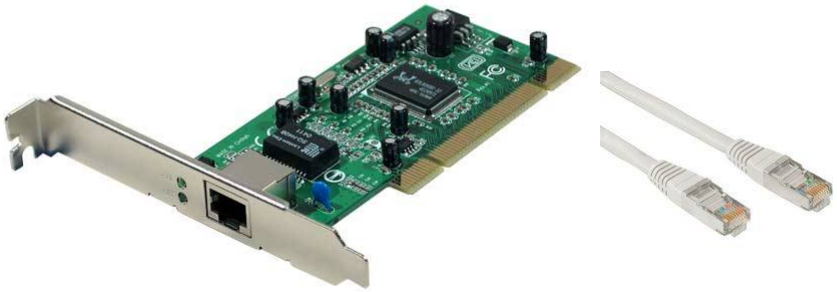
Principe général

Transeiver

- Plus résistant aux manipulations
- Plus de protection contre les parasites
- Plus cher
- Plus encombrant

3. Couche physique

Raccordement – RJ45



Ethernet RJ45

3. Couche physique

Raccordement – Fibre optique (Fast et Giga Ethernet)

3. Couche physique

Différents standards de niveau physique

10Base2, 10BaseT, 10GBaseLX…

{Débit} {Signalisation} Câblage — **Longueur** (m)

- {Débit}
  - 1 Mb/s
  - 10 Mb/s
  - 100 Mb/s
  - 1Gb/s
  - 10 Gb/s
  - 40 Gb/s
  - 100 Gb/s
- {Signalisation}
  - Base
  - Broadband
- Câblage
  - 2 : Thin coax
  - 5 : Thick coax
  - T : Twisted pair
  - F : Fiber
  - S : Short wave (fiber)
  - L : Long wave (fiber)
  - T2 : 2 Twisted pair
  - T4 : 4 Twisted pair
  - LX, FX, SX : fiber optics
  - CX : shielded balanced copper
- Longueur (m)
  - 25, 100
  - 500
  - 1000, 2000
  - 40000

3. Couche physique

Différents standards de niveau physique

Norme IEEE 802.3	Débit (en Mb/s)	Support	Longueur maximum d'un segment
802.3e - 1Base5	1	Paire torsadée	250 m
802.3 -10Base5	10	Câble coaxial (50 Ω)	500 m
802.3a - 10Base2	10	Câble coaxial (50 Ω)	185 m
802.3b - 10Broad36	10	Câble coaxial TV (75 Ω)	180 m
802.3d - FOIRL	10	Fibre optique	1000 m
802.3i - 802.3 10BaseT	10	Paire torsadée (catégorie 3 ou 4)	100 m
802.3j - 10BaseFB et FL	10	Fibre optique	2 000 m
802.3u 100BaseTX	100	Paire torsadée (catégorie 5)	100 m
802.3u 100BaseT4	100	Paire torsadée	100 m
802.3u 100BaseFX	100	Fibre optique	412 m
802.3y 100BaseT2	100	Paire torsadée (catégorie 3 ou 4)	100 m
100BaseVG any-LAN	100	Paire torsadée, Fibre optique	100 m, 2 000 m

Fast Ethernet

Utilise « Demand Priority Protocol » et pas CSMA/CD

3. Couche physique

Standards de niveau physique

Norme IEEE 802.3	Débit (en Mb/s)	Support	Longueur maximum d'un segment
802.3z 1000Base-SX	1000	Fibre optique	500 m
802.3z 1000Base-LX	1000	Fibre optique	5000 m
802.3z 1000Base-CX	1000	Paire torsadée	25 m
IEEE802.3ab :1000BaseT	1000	Câble coaxial, Paire torsadée	100 m
802.3ae 10GbaseCX4	10 000	Fibre optique	15 m
802.3ae 10GbaseT	10 000	Fibre optique	100 m
802.3ae 10GbaseSR	10 000	Fibre optique	100 m
802.3ae 10GbaseLX4	10 000	Fibre optique	10 000 m (MAN)
802.3ae 10GbaseLR	10 000	Fibre optique	40 000 m (MAN)
P802.3ba 40GBase	40 000	Fibre optique	des Km (MAN)
P802.3ba 100GBase	100 000	Fibre optique	des Km (MAN)

Giga Ethernet

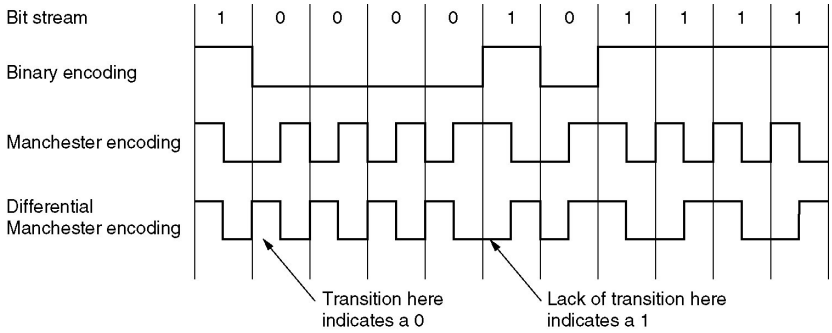
??? Ethernet

Utilisation du full duplex sur des liaisons point-point : chaque station reliée à un hub/switch émet sur un canal et reçoit sur un autre : donc les collisions sont éliminées/réduites.

3. Couche physique

Codage physique

- A l'origine : codage Manchester



3. Couche physique

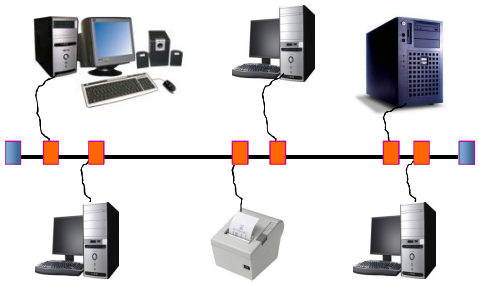
Codage physique

- Versions récentes : codage NRZ et autres
- Utilisation du code 4B/5B (➔ Perte de 20% de débit)

Code	Valeur en Héxa	Code	Valeur en Héxa	Code	Symbole de contrôle
11110	0	10010	8	00000	quiet
01001	1	10011	9	11111	idle
10100	2	10110	A	00100	halt
10101	3	10111	B	11000	J
01010	4	11010	C	10001	K
01011	5	11011	D	01101	T
01110	6	11100	E	00111	R
01111	7	11101	F	11001	S
Les combinaisons binaires restantes sont invalides					

4. Architectures de réseau Ethernet

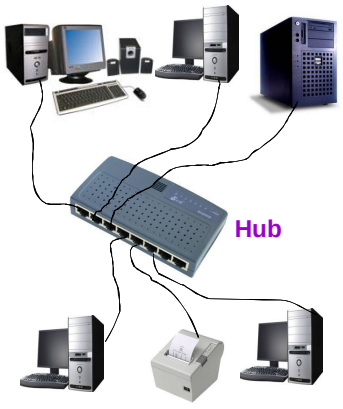
Architecture en Bus



- Inconvénients
  - **Manipulation accidentelle des bouchons et points de raccordement**
  - **Coupure du câble**

4. Architectures de réseau Ethernet

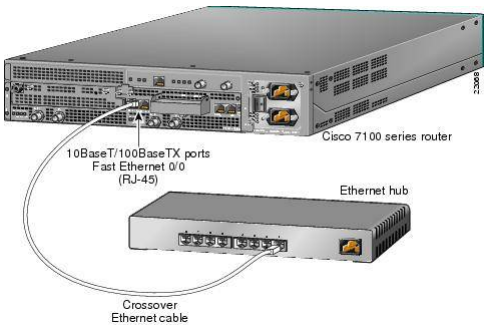
Architectures en Etoile

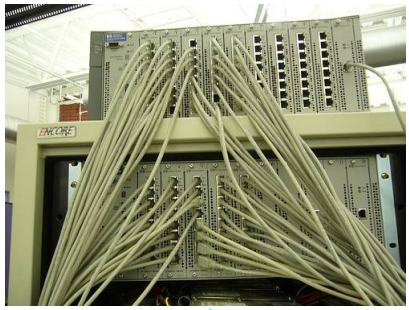


- Avantages : **Palier les inconvénients du bus (coupures du bus et incidents au niveau des bouchons**

4. Architectures de réseau Ethernet

Hub Ethernet



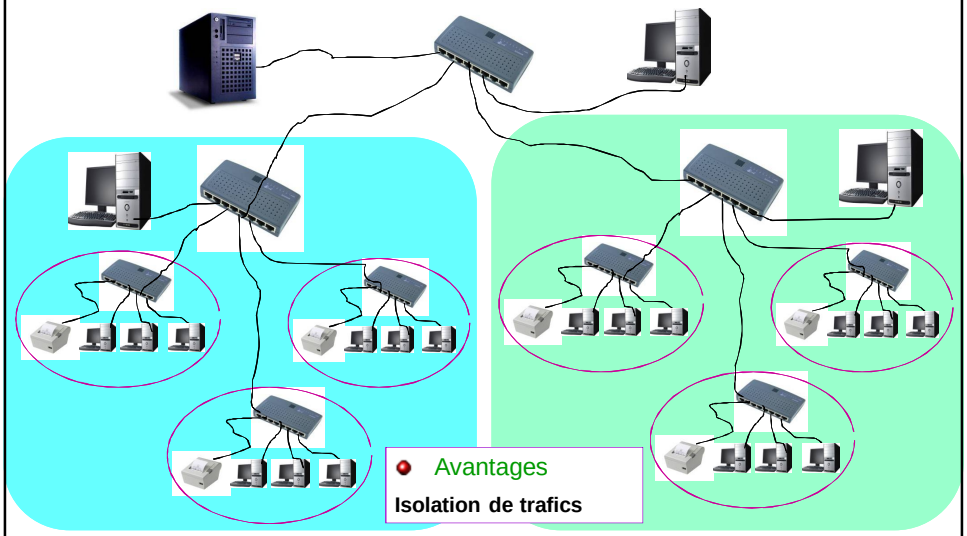


Plus de câbles

- Le hub agit au niveau physique uniquement
- Il sert de répéteur (régénération) de signaux
- Le hub évite l'utilisation de bouchons de lignes visibles

4. Architectures de réseau Ethernet

Architecture en arbre

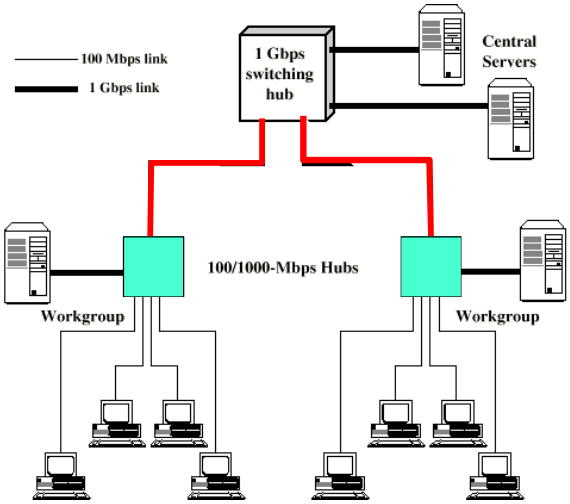


- Avantages

Isolation de trafics

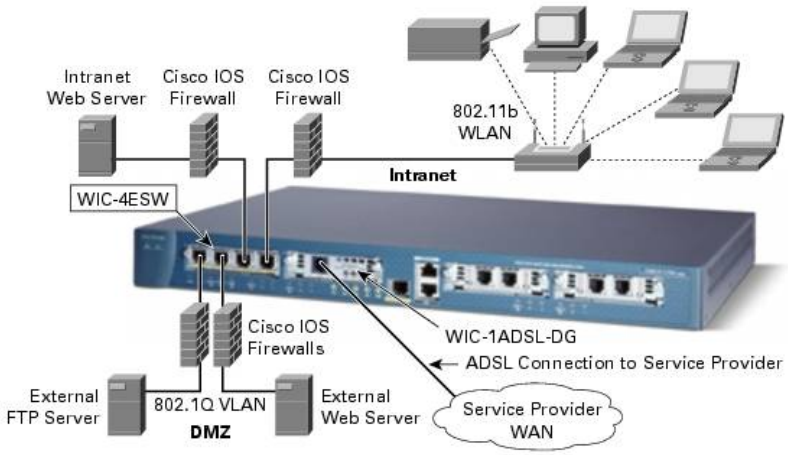
4. Architectures de réseau Ethernet

Architecture en arbre – débits hétérogènes



4. Architectures de réseau Ethernet

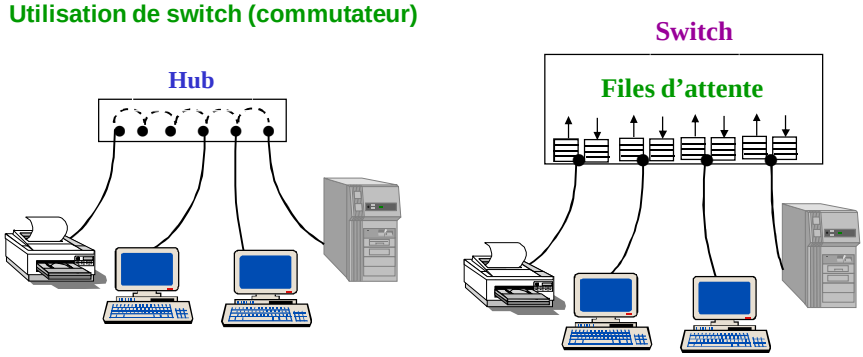
Architecture en arbre



4. Architectures de réseau Ethernet

Switch Ethernet

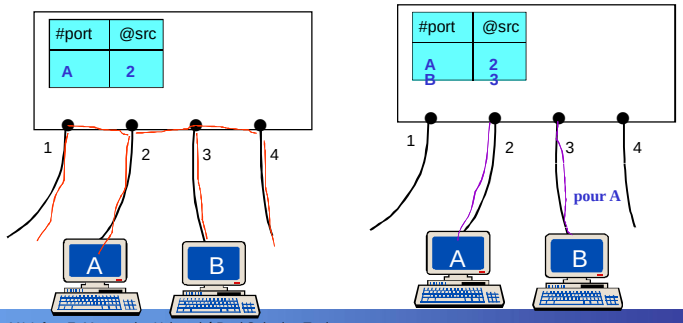
- **Ethernet est un médium partagé**
  - Une seule station peut transmettre même avec plusieurs hubs
  - Délai d'attente important (surtout en cas de trafic élevé)
- **Utilisation de switch (commutateur)**



4. Architectures de réseau Ethernet

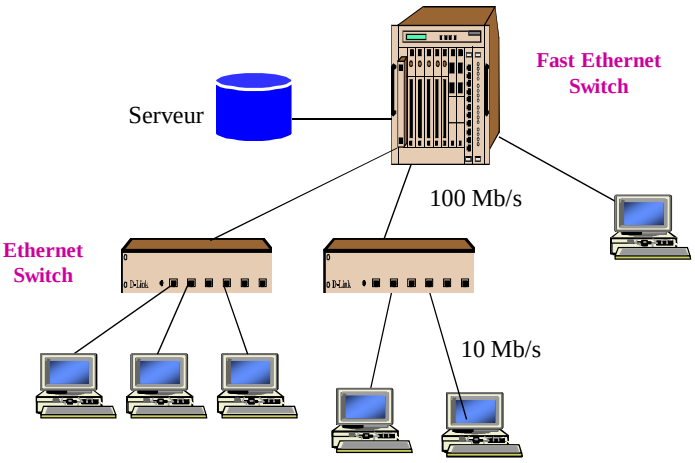
Switch Ethernet

- Objectif : palier les insuffisances des hubs
- Le switch apprend les stations de destination en mémorisant les ports des adresses sources dans une table
- Le switch ne fait pas de rediffusion systématique vers tous les ports mais seulement vers les ports de destination adéquats
- ➔ augmentation des capacités de transmission de trames sans collision



4. Architectures de réseau Ethernet

Combinaison de switchs Ethernet



5. Analyse de performance d'Ethernet

Formule d'inter-indépendance des paramètres Ethernet

Bits, sec, b/s

$$L\min \geq 2 * T\max * Débit$$

m, m/s

$$T\max = \frac{LongRes}{(2/3)\times(3\times10^8)} = \frac{LongRes}{(2*10^8)}$$

$$L\min \geq \frac{LongRes * Débit}{10^8} \qquad Débit \leq \frac{10^8 \times L\min}{LongRes} \qquad LongRes \leq \frac{10^8 \times L\min}{Débit}$$

- 100 Mb/s et 1 Km ➔ Lmin = 1000 bits
- 1 Gb/s et Lmin = 100 octets ➔ Longueur ≤ 80 m
- Lmin = 100 octets et Longueur = 500 m ➔ Débit ≤ 160 Mb/s

5. Analyse de performance d'Ethernet

Formule d'inter-indépendance des paramètres Ethernet

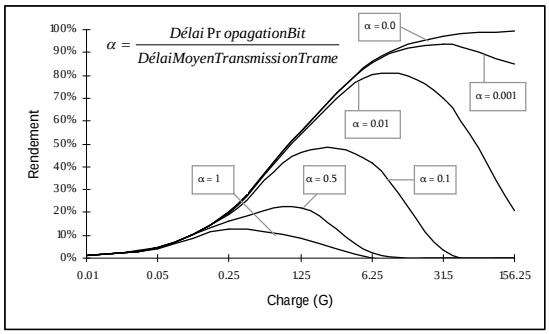
$$1/Débit \leq T\max = \frac{LongRes}{(2*10^8)} \Rightarrow LongRes \geq \frac{2 \times Débit}{10^8}$$

- 100 Mb/s ➔ LongRes ≥ 2 m
- 1 Gb/s ➔ LongRes ≥ 20 m

- Les standards Ethernet imposent une distance minimum entre stations

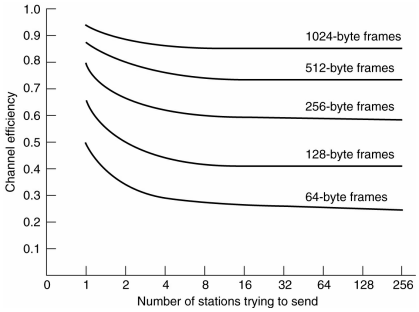
5. Analyse de performance d'Ethernet

Impacts de la longueur du réseau



5. Analyse de performance d'Ethernet

Impacts de la taille de trame



5. Analyse de performance d'Ethernet

Efficacité de CSMA/CD

- Efficacité de CSMA/D = pourcentage du débit physique que les stations peuvent atteindre
- Elle dépend de la longueur du réseau, du débit physique et de la taille des trames.

- Elle est de l'ordre de : $$\frac{1}{1+5\times\frac{TempsDePropationBit}{TempsMoyenDeTransmissionDeTrame}}$$

- Exemple : Longueur = 2500 m, Débit = 10 Mb/s et Taille moyenne de trame = 620 bits conduisent à une efficacité de 50%

6. Conclusion

Leçons apprises

- Ethernet fonctionne bien si la charge globale est faible (moins de 30% du débit théorique du réseau)
- Presque tous les réseaux actuels ont :
  - Moins de 200 machines (même si les standards prévoient 1024)
  - La longueur maxi dépasse rarement 2 km.
- Limites de Ethernet
  - Rajouter des machines revient à augmenter la probabilité de collision (donc moins il y a de machines mieux c'est)
  - Il est inefficace pour les échanges où la longueur des données utiles est petites (il n'est pas adapté aux applications industrielles et embarquées)
  - Le débit max est inversement proportionnel à la longueur max
- Clés de succès d'Ethernet par rapport à ses concurrents : Prix, disponibilité des cartes, facilité d'installation et configuration, simplicité, robustesse
- Il a bénéficié d'un lobbying énorme

Chapitre 4

Réseau FDDI

(*Fiber Distributed Data Interface*)

Etude de réseau à jeton

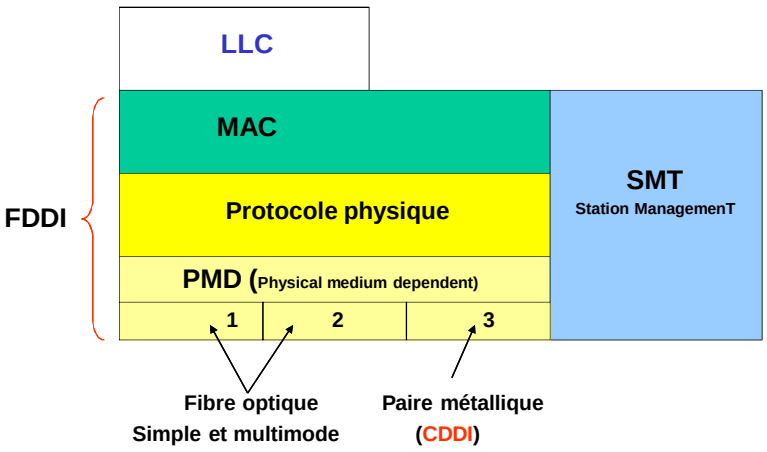
1. Introduction à FDDI

FDDI en bref

- FDDI : premier réseau sur fibre optique
- Fibre optique ➔ sécurité accrue au niveau physique
- Réseau MAN ou LAN
- Maximum of 500 stations en boucle redondante ou 1000 sur boucle simple
- Etendue maxi = 100 km sur boucle redondante ou 200 km sur boucle simple
- Premier réseau à offrir 100 Mb/s
- Réseau à jeton ➔ temps d'attente avant accès au canal borné
- Existe aussi sur paire métallique (CDDI)

1. Introduction à FDDI

Architecture du standard ANSI X3T9.5



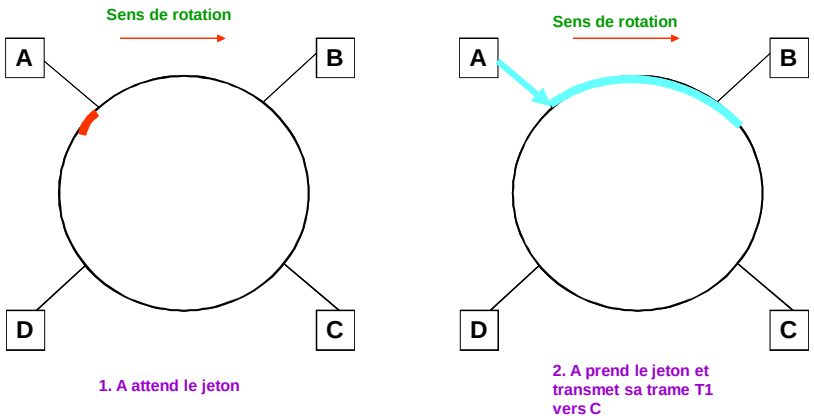
2. Sous-couche MAC

Principe d'utilisation du jeton sur FDDI

- Un jeton tourne sur la boucle
- La station qui voit passer le jeton et qui a des données à transmettre retire le jeton
- Elle transmet sa ou ses trames et libère le jeton
- A un instant donné, on peut avoir plusieurs trames de données en circulation sur la boucle
- Le jeton peut être soit en circulation soit bloqué dans une station
- La station qui se reconnaît comme destinataire d'une trame la recopie et positionne le bit Ack à 1
- La trame fait un tour complet et elle est retirée par sa source.

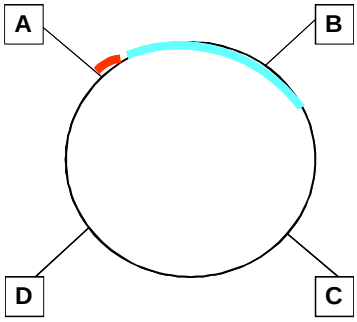
2. Sous-couche MAC

Exemple d'utilisation du jeton sur FDDI

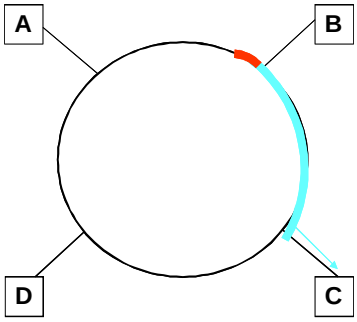


2. Sous-couche MAC

Exemple d'utilisation du jeton sur FDDI



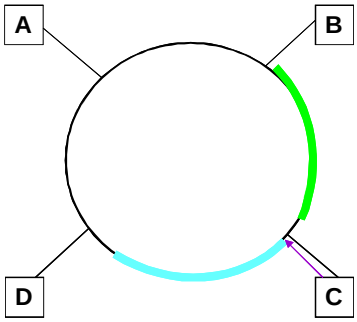
3. A libère le jeton.
Sa trame est encore
sur la boucle



4. La trame de A arrive à C
qui la recopie

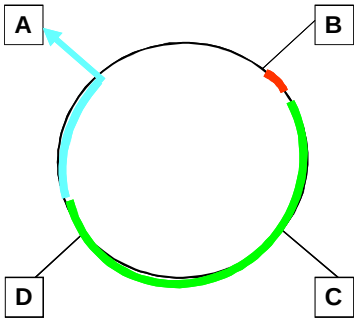
2. Sous-couche MAC

Exemple d'utilisation du jeton sur FDDI



5. C finit de recopier la trame et
positionne le bit d'Ack.

B intercepte le jeton et envoie
une trame T2 vers D



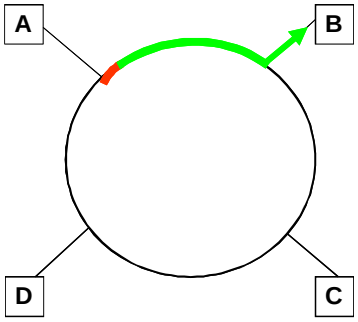
6. B libère le jeton.

D recopie la trame T2 de B

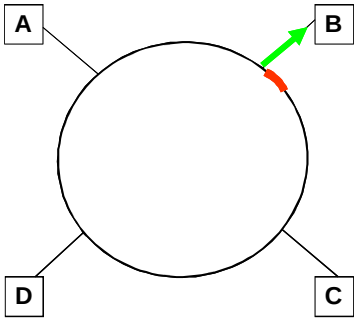
A absorbe sa trame T1

2. Sous-couche MAC

Exemple d'utilisation du jeton sur FDDI



7. A laisse passer la trame T2.
Il laisse passer aussi le jeton.
B absorbe sa trame T2.



8. B a absorbé sa trame et laisse passe le jeton.

2. Sous-couche MAC

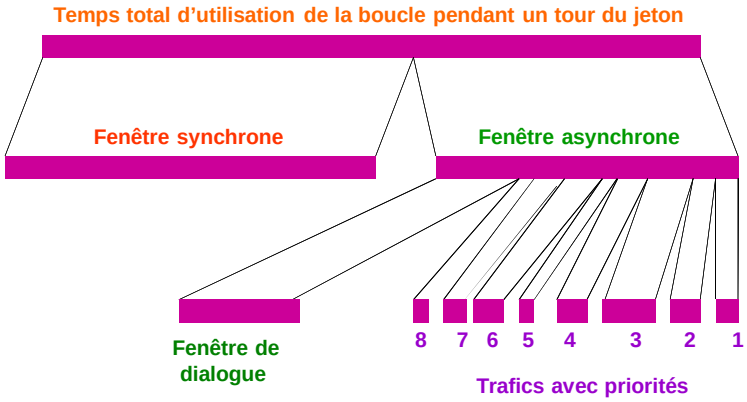
Principes de base de l'accès FDDI

- Accès par jeton temporisé
- Garantie de délai d'accès aux applications multimédia et temps réel
- Optimisation des temps de réponse pour les trafics aléatoires selon priorité

- Distinction de trafics
  - Périodique (ou synchrone ou isochrone)
    Ex. La voix téléphonique, la vidéo
  - Apériodique (ou asynchrone ou anisochrone) avec ou sans priorités
    Ex. transfert de fichier, messagerie…
  - Flux de dialogue pair à pair (optionnel)

2. Sous-couche MAC

Décomposition du temps d'accès à la boucle FDDI



Le temps séparant deux passages successifs du jeton dans toutes les stations est inférieur à 2*TTRT

2. Sous-couche MAC

Trafic synchrone

- **A l'initialisation du réseau sont fixés :**
  - **TTRT (target token rotation time)**
  - **SA_i (synchronous allocation)** /* pour chaque station i */
- **Garantie d'accès : Chaque station dispose (à chaque tour du jeton) d'un quantité SAi pour transmettre ses données synchrones**

$$\sum_{i=1}^{n} SA_i \leq TTRT - \tau$$

τ : temps nécessaire au jeton pour faire un tour complet de la boucle

2. Sous-couche MAC

Trafic asynchrone (non restreint)

- Toutes les stations connaissent la valeur du TTRT
- Toutes les stations mesurent la durée réelle de rotation du jeton

  Utilisation du compteur TRT (Token Rotation Time)
- Si le jeton arrive en avance (i.e. TRT < TTRT) la station peut utiliser le temps THT (Token Holding Time) pour transmettre des données apériodiques. THT = TTRT – TRT
- Si le jeton arrive en retard (i.e. TRT > TTRT), la station ne peut pas transmettre de données apériodiques
- Si le temps de rotation du jeton dépasse 2*TTRT, la boucle est réinitialisée.

- Le mode restreint (ou dialogue) permet à deux stations de s'échanger des données apériodiques pendant un certain temps sans que les autres stations ne puissent émettre de données apériodiques

2. Sous-couche MAC

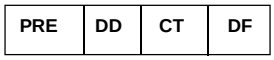
Algorithme complet de transmission avec FDDI

/* Phase d'initialisation */
LC$_i$ = 0 ; Attendre_Jeton ; TRT$_i$ = TTRT ; Déclencher TRT$_i$
Passer le jeton /* Dans le premier tour du jeton, il n'y a pas d'émission de trames de données */
/* Phase de fonctionnement normal : utilisation du jeton pour transmettre des données */
Tant que vrai Répéter
{ Si TRT$_i$ atteint la fin de temporisation Alors LC$_i$ = LC$_i$ +1
Si LC$_i$ > 1 Alors Réinitialiser la boucle
Sinon TRT$_i$ = TTRT ; Déclencher TRT$_i$
Finsi ; Finsi
||
Si Arrivée du jeton
Si LC$_i$ = 0 alors
THT$_i$ = TRT$_i$; TRT$_i$ = TTRT ; Déclencher TRT$_i$
Transmettre les trames périodiques, s'il y en a, jusqu'à concurrence du SA$_i$
Déclencher THT$_i$
Tant que THT$_i$ > 0 {Transmettre des apériodiques s'il y en a} ; Passer le jeton
Sinon
LC$_i$ = 0 ; /* TRT n'est pas réinitialisé dans ce cas, afin d'accumuler le retard. */
Transmettre les trames périodiques jusqu'à concurrence du SA$_i$
Passer le jeton
Finsi ; Finsi ; }

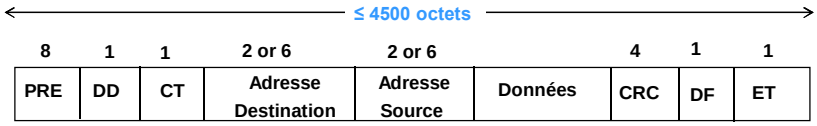
2. Sous-couche MAC

Format de trame FDDI

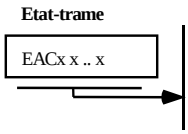
PRE : Préambule
DD : délimiteur de début (code JK)
CT : contrôle trame
DF : Délimiteur de fin (code IT)
ET : état de trame



Format du jeton



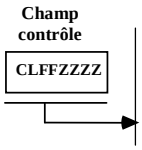
Format de trame de données



E : indique s'il y a eu erreur de transmission ou non
A : indique si l'adresse de destination a été reconnue ou non
C : indique si la trame a été recopiée par son destinataire ou non
x..x : extension des bits d'état

2. Sous-couche MAC

Format de trame FDDI



C : indique si la trame est synchrone ou asynchrone
L : indique si les adresses sont sur 2 ou 6 octets
FF : indique si c'est une trame LLC ou une trame de contrôle MAC
ZZZZ : bits de contrôle

CLFFZZZZ	Signification
10000000	Jeton normal
11000000	Jeton restreint
1L000011	Demande de jeton
1L000010	Feu d'alarme
0L01rPPP	Trame asynchrone avec la priorité PPP
1L01 rrrr	Trame synchrone (rrrr : réservé pour extension future)

2. Sous-couche MAC

Procédure d'initialisation de la boucle FDDI

- Emission en continu d'une trame de *demande d'acquisition du jeton*
- Si une seule station fait la demande d'acquisition du jeton, elle obtient le jeton dès que sa demande lui revient
- Si plusieurs stations demandent l'acquisition du jeton, en même temps, une seule station obtient le jeton, en respectant les règles suivantes :
  - Toute station qui ne demande pas à acquérir le jeton répète la demande sur la boucle
  - Si une station a demandé ou veut demander l'acquisition du jeton : elle laisse passer la demande reçue, si elle est plus prioritaire que la sienne ou bien elle absorbe la demande, si elle est moins prioritaire que la sienne
  - Les règles de priorité sont fixées des demandes sont :
    - La demande ayant le TTRT le plus petit est prioritaire
    - En cas d'égalité des valeurs du TTRT, c'est la station qui a l'adresse la plus courte qui est prioritaire
    - En cas d'égalité des valeurs du TTRT et des longueurs des adresses, c'est la station qui a l'adresse la plus basse qui est prioritaire
- La station qui s'impose crée un jeton et le fait circuler sur la boucle

2. Sous-couche MAC

Procédures de surveillance de la boucle FDDI

- Contrôle de la boucle
  - Le jeton peut se perdre suite à une panne de la station qui l'a retiré ou suite à des erreurs de transmission subies par le jeton lors de sa transmission.
  - Contrôle décentralisé de la boucle : toute station réinitialise la boucle si :
    - Elle détecte que le temps de rotation du jeton dépasse 2*TTRT
    - Elle détecte que sa trame ne lui revient pas au bout d'un délai égal à celui qu'il faut pour faire un tour complet de la boucle
- Détection de coupure de boucle
  - Toute station détecte que la boucle est coupée si rien ne lui parvient au bout d'un délai supérieur à celui pour faire un tour complet de la boucle
  - La station transmet en continu une trame feu d'alarme
  - La station arrête de transmettre la trame feu d'alarme quand sa trame feu alarme lui revient. Elle lance ensuite la procédure de réinitialisation de la boucle.

2. Sous-couche MAC

Interface MAC-LLC

MA-Data.request (*adrs_dest(1), unité_données(1), classe_service(1),*
.....
adrs_dest(n), unité_données(n), classe_service(n))

MA-DATA.confirmation *(nombre_unités_données, état_transmission, classe_service_fourni)*

MA-DATA.indication *(adrs_dest, adrs_source, unité_de_données, état_réception)*

MA-TOKEN.request *(classe_jeton_à_capturer)*

3. Couche physique

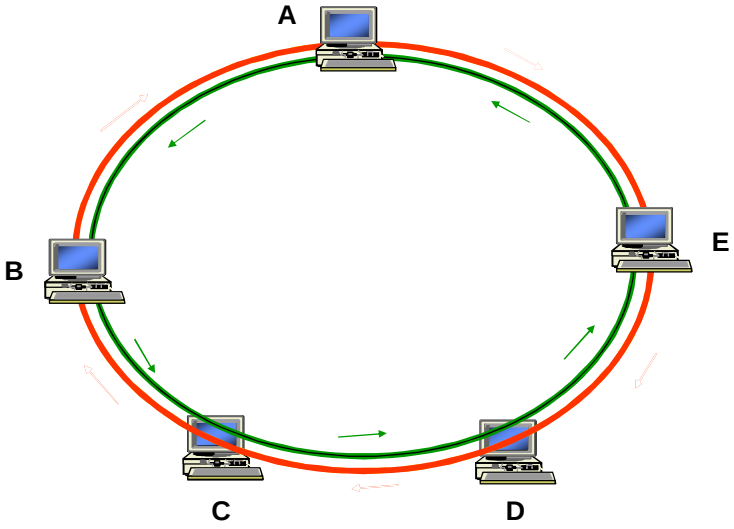
Codage 4B/5B

- **Objectif : détection d'erreurs au niveau physique et utilisation de codage physique simple**
  - 4B/5B avec NRZI (le 4B/5B contient assez de transitions pour palier les insuffisances du NRZI et éviter l'utilisation de codes différentiels qui exigent un rythme de modulation deux fois celui du NRZI)
- **Les trames sont acquittées au niveau physique**
- **Modulation à 125 Mb/s pour avoir 100 Mb/s au niveau MAC**

Code	Valeur en Héxa	Code	Valeur en Héxa	Code	Symbole de contrôle
11110	0	10010	8	00000	quiet
01001	1	10011	9	11111	idle
10100	2	10110	A	00100	halt
10101	3	10111	B	11000	J
01010	4	11010	C	10001	K
01011	5	11011	D	01101	T
01110	6	11100	E	00111	R
01111	7	11101	F	11001	S
Les combinaisons binaires restantes sont invalides					

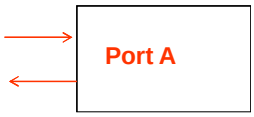
3. Couche physique

Boucle redondante



3. Couche physique

Raccordement au support

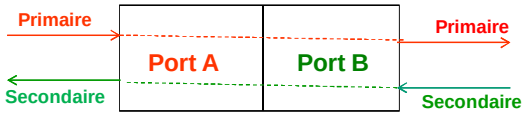


Carte SAS (Single Attachement Station)

Carte DAS (Dual Attachement station)

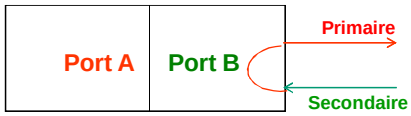
3. Couche physique

Principe de contournement



Fonctionnement normal

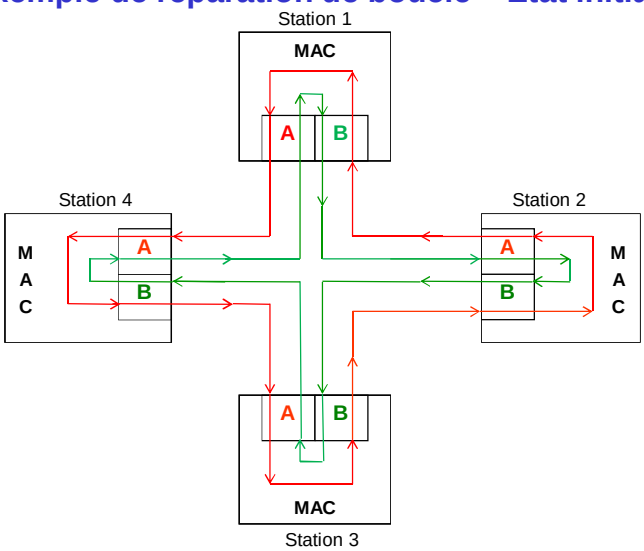
Contournement à gauche



Contournement à droite

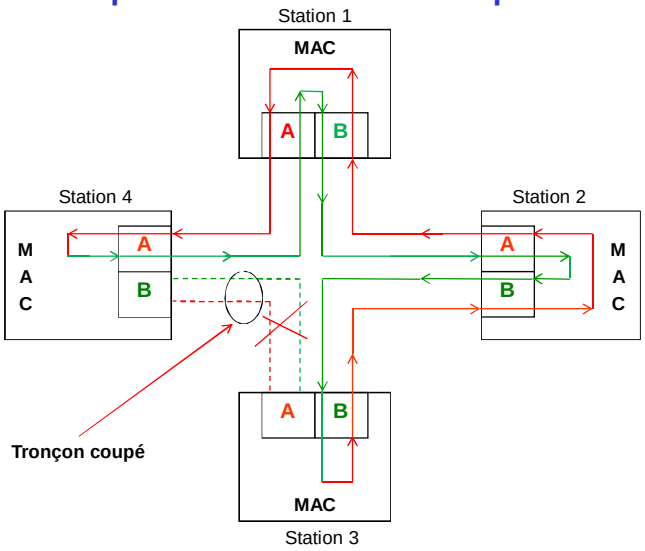
3. Couche physique

Exemple de réparation de boucle – Etat initial



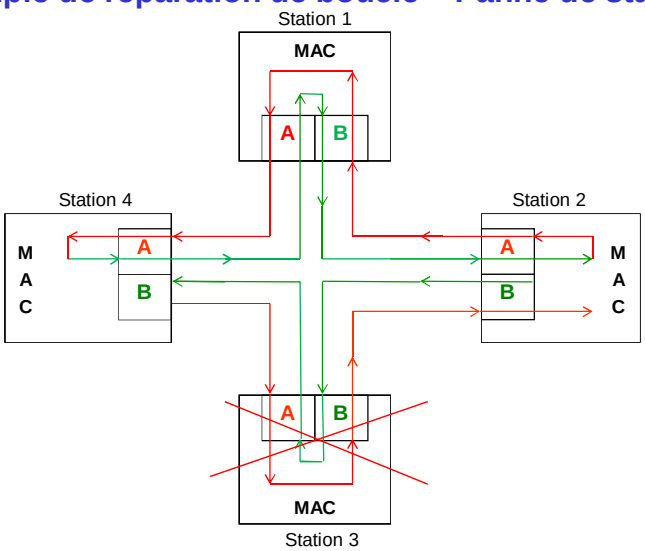
3. Couche physique

Exemple de réparation de boucle – Coupure de tronçon



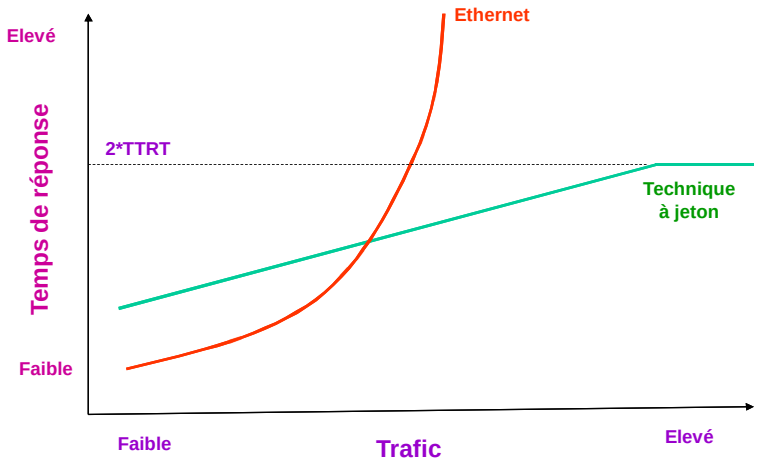
3. Couche physique

Exemple de réparation de boucle – Panne de station



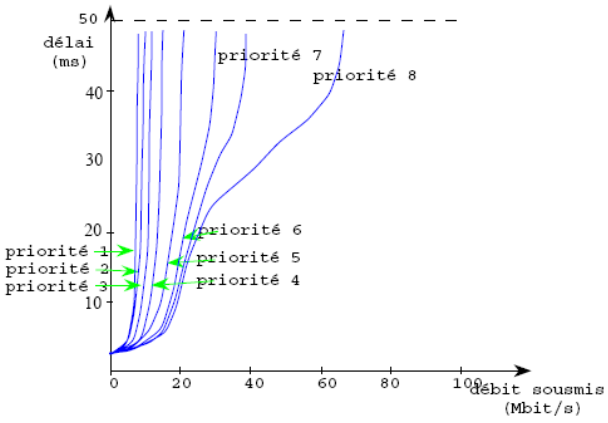
4. Performance de FDDI

Temps d'attente pour une station : FDDI vs Ethernet



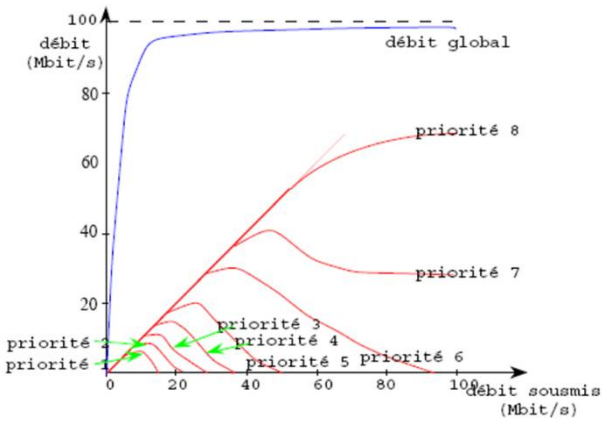
4. Performance de FDDI

Délai d'attente pour les flux apériodiques



4. Performance de FDDI

Débit des flux asynchrones selon les niveaux de priorité



5. Pourquoi FDDI a-t-il échoué ?

Raisons de l'échec

- 100 Mb/s fin des années 1980 : pas d'applications qui ont besoin de ce débit
- Pas de vente massive des cartes FDDI
- Pas d'intégration massive des fonctionnalités dans le silicium
- Pas d'enthousiasme et support massif des grands constructeurs
- Une carte Ethernet : quelques dizaines voire une centaine d'euros
- Une carte FDDI : plusieurs centaines (parfois plus de 1000 euros)

5. Pourquoi FDDI a-t-il échoué ?

Exemples de cartes FDDI

5. Pourquoi FDDI a-t-il échoué ?

Exemples de cartes Ethernet

1G Ethernet NIC PCI

Chapitre 5

Réseau ATM

(*Asynchronous Transfer Mode*)

1. ATM et RNIS

Milieu des 1980 : vers une société de l'information

Education

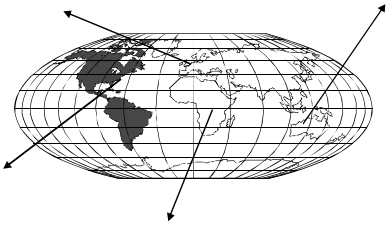
Information

Communication

Banque

Santé

Contrôle



Achats

Circulation

Services domestiques (jeux, loisirs…)

TV

Police

SAMU

Pompiers

1. ATM et RNIS

Besoin de RNIS (Réseau numérique à intégration de services)

ISDN (Integrated Services Digital Network)

- **Disposer d'une technologie**
  - Adaptée aux applications actuelles et futures
  - Permettre de la vidéo et audio de haute qualité
  - Interconnexion à des débits allant de quelques Kb/s à des Mb/s ou Gb/s
  - Utilisable au niveau de l'accès et au niveau cœur
    - → Unification des réseaux
  - Garantissant la QoS (différencier les services selon leurs besoins)
  - Fiable, robustesse
  - Prédictible (temps de réponse borné)
  - Facile d'utilisation pour la prise en compte des équipements déjà existants
  - Adaptée à tous les supports de transmission
  - Permettant le business des réseaux et services

1. ATM et RNIS

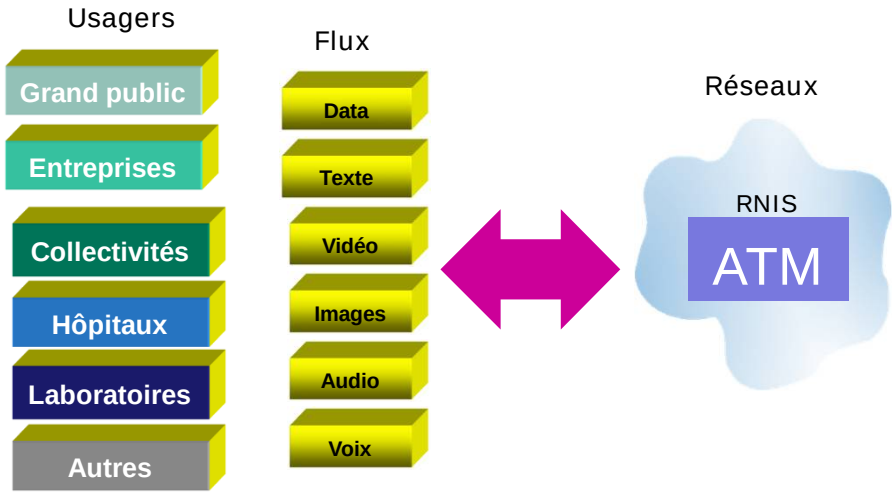
Exemples de débits selon les flux

Type d'information		Débit	Remarques
Données		Débits très divers	Données avec des débits continus ou en rafales
Texte		Plusieurs kb/s	Transmission de texte de grand volume
Son	Téléphonie	64 kb/s 11 kb/s	Ligne téléphonique normale Voix sur IP (VoIP)
	Qualité CD	1,4 Mb/s	
Image	Télécopie	64 kb/s	Télécopie du groupe 4
	Vidéophonie	64-128 kb/s	Vidéo téléphonie (qualité réduite)
	TV std	120 Mb/s 1,5 Mb/s	TV standard non compressée TV standard compressée (MPEG-1)
	TV HD	1-3 Gb/s 10-30 Mb/s	HDTV non compressée HDTV compressée (MPEG-2)
	Traitement graphique	Très variable	Dépend des modèles 2D ou 3D, de la qualité des images, de l'animation…

1. ATM et RNIS

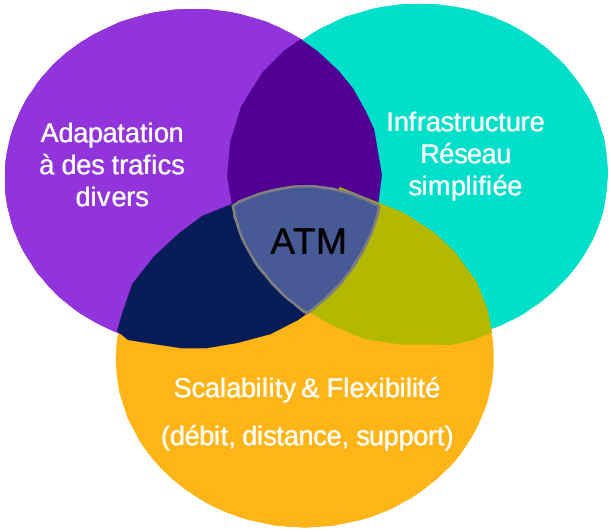
Besoin de RNIS (Réseau numérique à intégration de services)

ISDN (Integrated Services Digital Network)



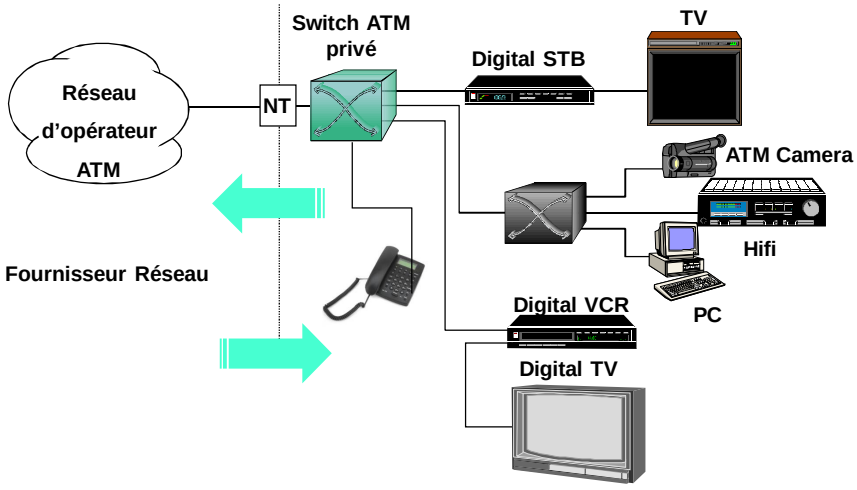
1. ATM et RNIS

Avantages de ATM



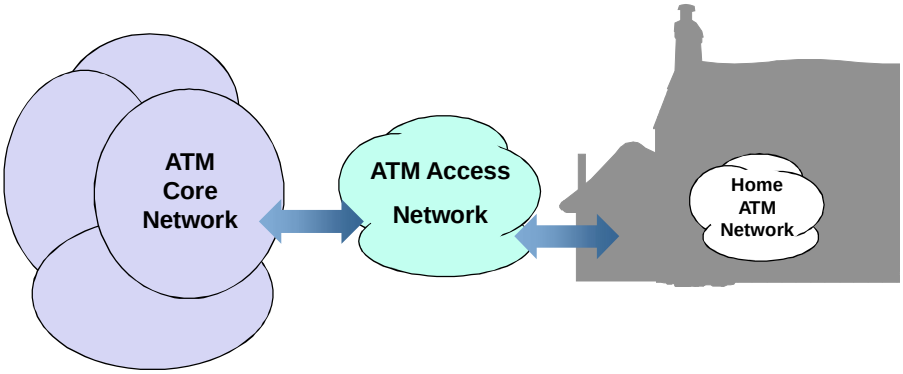
1. ATM et RNIS

Tous les équipements sur le même réseau



1. ATM et RNIS

Objectif initial : de l'ATM partout

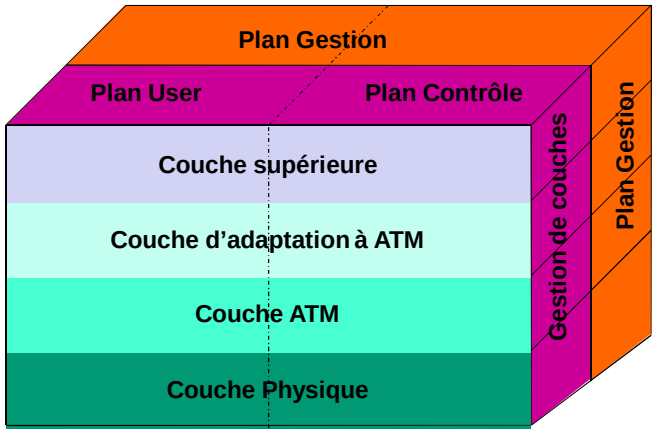


- Aujourd'hui : ATM se trouve au cœur des réseaux
- MPLS (MultiProtocol Label Switching) remplacerait ATM

1. ATM et RNIS

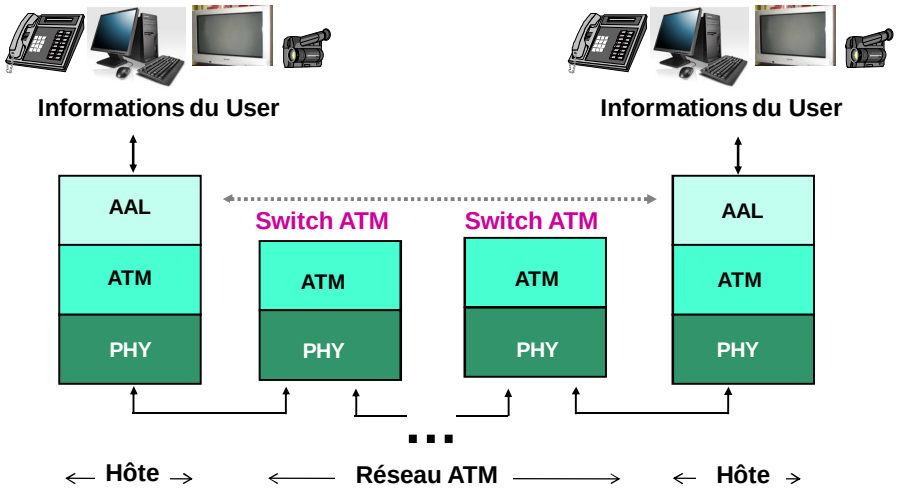
Architecture ATM

- **Plan User :** transfert des infos de l'usager
- **Plan Contrôle :** contrôle de connexions et appels
- **Plan Gestion :** gestion de l'ensemble du système
- **Gestion de couches** : gestion couche par couche



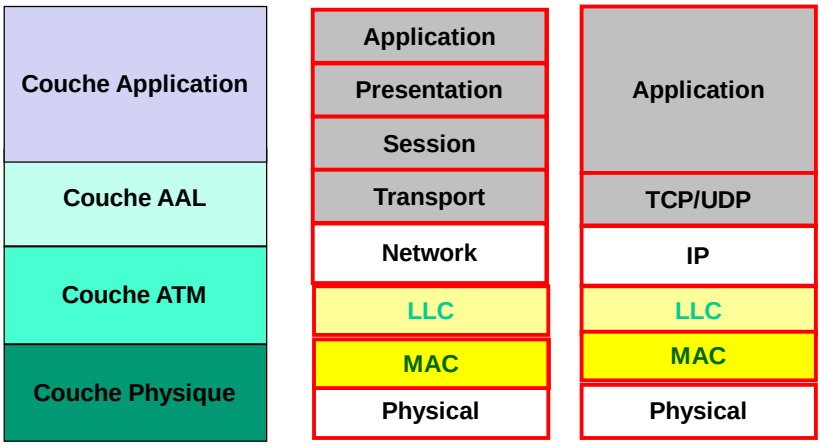
1. ATM et RNIS

ATM – Plan User



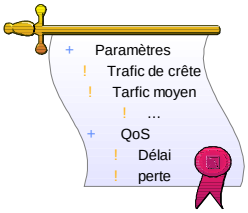
1. ATM et RNIS

ATM vs Modèles OSI et TCP/IP : le premier rêve !

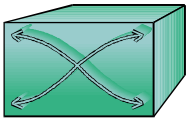


1. ATM et RNIS

3 mots clés pour comprendre ATM



- **Contrat** : Service orienté connexion



- **Commutation** : réseau assurant la commutation

- **Cellule** : paquet de petite taille FIXE

1. ATM et RNIS

ATM en bref

- **ATM = Une solution complète : offre des services couvrant toutes les couches de transport de données**
- **Standard développé au niveau européen et soutenu/promu par le CCITT (ITU actuellement)**
- **ATM forum créé en 1991 pour promouvoir ATM**
- **ATM prend ses racines dans les réseaux d'opérateurs**
  - ATM est orienté connexion
  - ATM est un système de commutation de cellules de taille fixe

2. Couche AAL

Catégories de service ATM

- **Natures de flux**
  - Son, voix, vidéo, images animées
    - Contraintes de débit, de délai de traversée et de gigue
    - Un certain taux de perte acceptable
  - Texte, data, binaire, images fixes
    - Pas de contraintes de débit et délai (meilleur effort)
    - Taux de perte nul
- **Deux catégories de services**
  - Communication temps réel
    - Constant bit rate (CBR)
    - Real-time variable bit rate (VBR)
  - Communication non temps réel
    - Non-real time variable bit rate (nrt-VBR)
    - Available bit rate (ABR)
    - Unspecified bit rate (UBR)
    - Guaranteed frame rate (GFR)

2. Couche AAL

Catégories de service ATM

- **CBR**
  - Données générées à un rythme fixe
  - Messages de taille fixe
  - Données à délivrer en respectant les timings
  - Eg. Vidéo non compressée, audio non compressé
- **RT-VBR**
  - Données générées de manière irrégulière, avec rafale
  - Message de taille variable
  - Données à délivrer en respectant des délais
  - Eg. Vidéo et audio compressés, messages d'alarme

2. Couche AAL

Catégories de service ATM

- **nRT-VBR**
  - Données générées à un rythme irrégulier
  - Messages de taille variable
  - Pas de timings à respecter, mais un temps de réponse optimisé
  - Eg. Systèmes transactionnels (banque, télé-achat, compagnies aériennes)
- **UBR**
  - Données générées à un rythme irrégulier
  - Messages de taille variable
  - Taux de perte et délais tolérables
  - Pas de spécification de trafic (débit moyen non connu)
  - Eg. ftp, mail

2. Couche AAL

Catégories de service ATM

- **ABR**
  - Données générées à un rythme irrégulier
  - Messages de taille variable
  - Pas de timings à respecter
  - Débit max et moyen connus
  - Obtenir le débit qui se rapproche du débit moyen (quand cela est possible)
  - Eg. Web browsing, Interconnexion de LANs par ATM
- **GFR**
  - Equivalent de UBR
  - Le taux de perte porte sur les messages et pas seulement sur les cellules (pour les paquets IP perdre une cellule d'un paquet revient à jeter toutes les autres cellules du paquet)
  - Eg. Utilisation d'ATM en tant que IP backbone

2. Couche AAL

Catégories de service ATM

Service	QoS exigée			Débit du trafic	Timing Émetteur/ récept	Protocole
	Délai	Gigue	Perte			
CBR	Borné	Faible	Faible	Constant	Requis	AAL1
Rt-VBR	Borné	Faible	Moyenne	Variable	Requis	AAL2
Nrt-VR	À optimiser	Best effort	Moyenne	Variable	Non requis	AAL3/4
ABR	Best effort	Best effort	Moyenne	inconnu	Non requis	AAL5 – 3/4
UBR	Best effort	Best effort	Elevée	Inconnu++	Non requis	AAL5 – 3/4
GFR	Best effort	Best effort	Elevée	Elevée	Non requis	AAL5

2. Couche AAL

Spécification de contrat ATM

- ATM orienté connexion
- Connexion ➔ Contrat (SLA : service level agreement)
- Contrat ATM
  - Paramètres de trafic
    - PCR (peak cell rate) : débit de crête
    - SCR (sustainable cell rate) : débit moyen
    - MCR (minimum cell rate) : débit minimum
    - MFS (maximum frame size)
    - MBS (maximum burst size) : taille maxi de rafale
  - Paramètres de Qualité de service
    - CTD (max cell transfer delay)
    - CDV (cell delay variation) : gigue
    - CLR (cell loss rate)

Les paramètres à spécifier dépendent du type de service

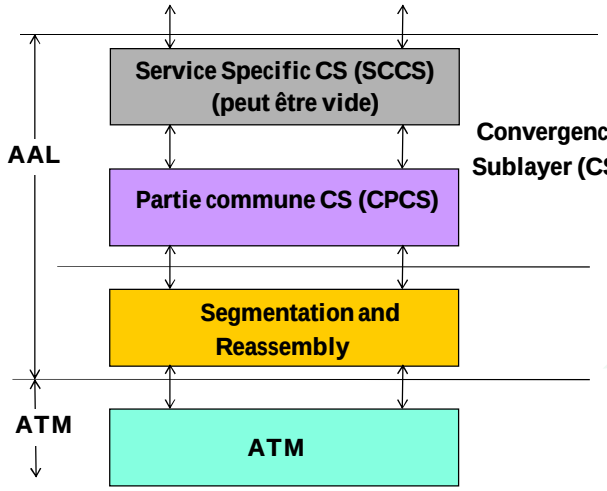
2. Couche AAL

Paramètres de trafic et QoS selon les services ATM

	Service ATM					
Attribut	CBR	rt-VBR	nrt-VBR	UBR	ABR	GFR
Paramètres de trafic						
PCR	Spécifié			Spécifié	Spécifié	Spécifié
SCR, MBS	Non spécifié	Spécifié		Non spécifié		
MCR	Non spécifié				Spécifié	Non spécifié
MCR, MBS, MFS, CDVT	Non spécifié					Spécifié
Paramètres de QoS						
CDV	Spécifié		Non spécifié			
CTD	Spécifié		Non spécifié			
CLR	Spécifié			Non spécifié		

2. Couche AAL

AAL = CS + SAR

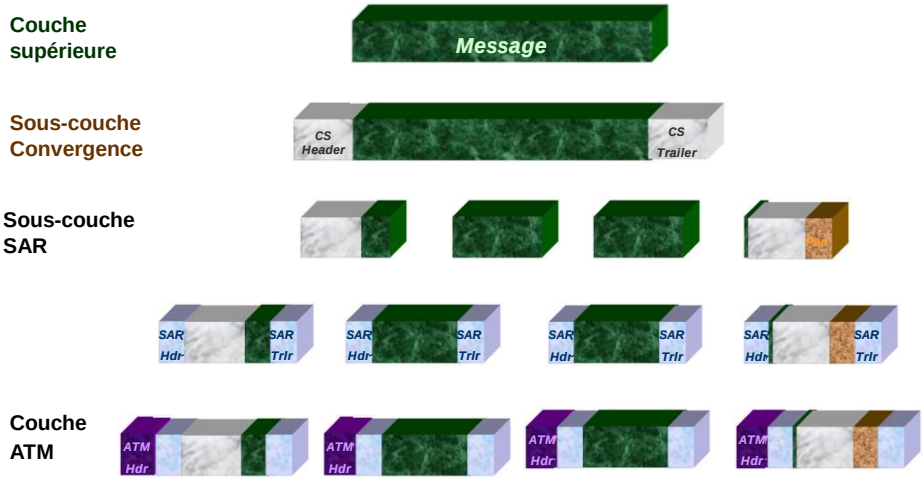


- Interface avec la couche supérieure
- Gestion de cellules perdues ou en retard
- Détection et gestion d'erreurs

- Fragmentation et réassemblage de messages
- Génération des champs de contrôle SAR

2. Couche AAL

Fragmentation et encapsulation par AAL



2. Couche AAL

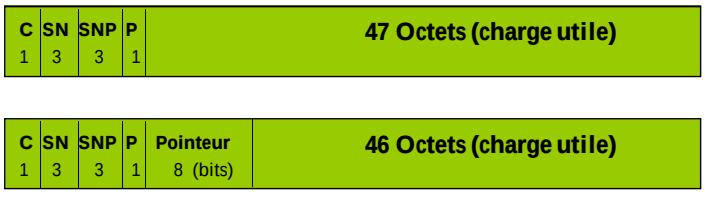
Protocole AAL1 (CBR)

- Prise en compte des besoins de contraintes strictes de QoS
- Conçue pour la transmission d'audio ou de vidéo non compressée
- Livraison de cellules au destinataire à un rythme fixe
- Absorption de la variation des délais de transfert
- En entrée : un flot de bits, sans frontières de message (flux continu)
- Pas de mécanisme de retransmission à cause des délais qu'il engendre
- Monitoring (observation) des performances (taux de perte, débordement de buffer, taux d'erreur, délais …)
- Pas de protocole de niveau CS.

2. Couche AAL

Protocole AAL1 (CBR)

- Format de cellule pour AAL1



Bit C (=0) : pour caler l'horloge du récepteur
SN (sequence number) : pour détecter les cellules manquantes ou mal insérées
SNP (SN protection) : CRC sur le SN
P : bit de parité de l'entête
Pointeur (optionnel) : indique la position du message suivant (rarement utilisé)

2. Couche AAL

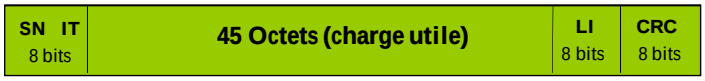
Protocole AAL2 (RT-VBR)

- Prise en compte des besoins de contraintes strictes de QoS
- Conçue pour la transmission d'audio ou de vidéo compressée et messages urgents (critiques)
- Livraison de cellules au destinataire en respectant les délais
- En entrée : des messages
- Pas de mécanisme de retransmission à cause des délais qu'il engendre
- Monitoring (observation) des performances (taux de perte, débordement de buffer, taux d'erreur, délais …)
- Pas de protocole de niveau CS.

2. Couche AAL

Protocole AAL2 (RT-VBR)

- Format de cellule pour AAL2



SN (sequence number) : pour détecter les cellules manquantes ou mal insérées
IT (Information Type) : indique si la cellule transporte le début, le milieu ou la fin de message.
LI (Length Indicator) : pour supprimer les infos de bourrage

2. Couche AAL

Protocole AAL3/4

- Combinaison de AAL3 et AAL4
- Conçue pour supporter du trafic en mode flot ou message avec ou sans connexion mais sans contrainte de QoS
- Permet le multiplexage de circuit (quand plusieurs flux sont envoyés d'une machine à une autre)
- Les messages manipulés ont une taille de 65535 octets. Ils sont complétés puis découpés en cellules

2. Couche AAL

Protocole AAL3/4

- Format de message pour AAL3/4

CPI	Btag	Taille Buffer	Charge Utile	Bourrage	NotUsed	Etag	Longueur
1 octet	1 octet	2 octets	< 65536 octets	0-3 octets	1 octet	1 octet	2 octets

CPI (Common part indicator) : indique le type de message et unité de compte (en octets ou autre)
Btag et Etag : délimiteurs de début et fin de message
Taille Buffer : indique la taille du message à envoyer (permet au récepteur de réserver la mémoire pour accueillir le message)
Longueur : taille des infos utiles du message

- Format de cellule pour AAL3/4

ST	SN	MID	44 Octets (charge utile)	LI	CRC
2	4	10 bits		6 bits	10 bits

ST : indique si la cellule se trouve au début, au milieu ou à la fin du message
SN : sequence number
MID (Message Id) : sert en cas de multiplexage
LI (Length Information) : infos utiles contenues dans la cellule

2. Couche AAL

Protocole AAL5

- Appelée aussi SEAL (Simple Efficient Adaptation Layer)
- Conçue pour le support de trafic aléatoire sans contraintes de QoS
- Utilisé pour le support de trafic IP
- Les cellules contiennent jusqu'à 48 octets de charge utile (le protocole SAR ne rajoute aucun champ de contrôle)

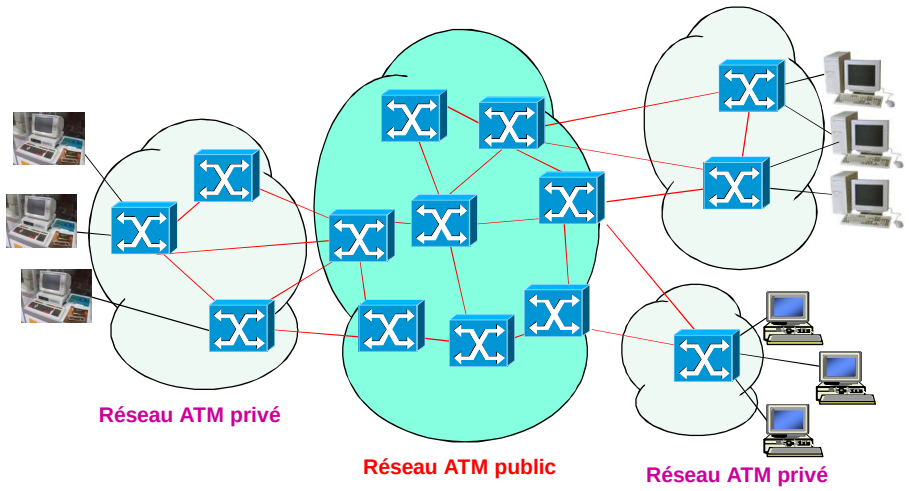
- Format de message pour AAL5

Charge Utile < 65536 octets	UU 1 octet	Réservé 1 octet	Longueur 2 octets	CRC 4 octets

UU (User to User) : marquage utilisé par les couches supérieures

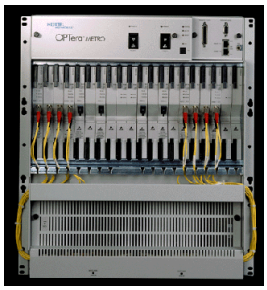
3. Couche ATM

Structure générale de réseaux ATM



3. Couche ATM

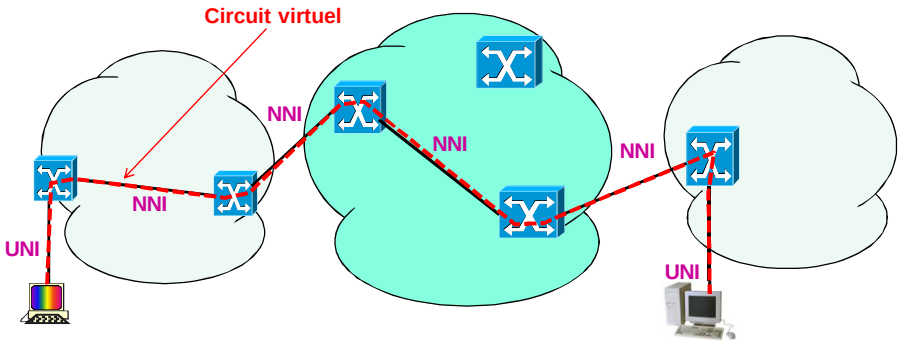
Exemples de switch ATM




3. Couche ATM

Structure générale de réseaux ATM

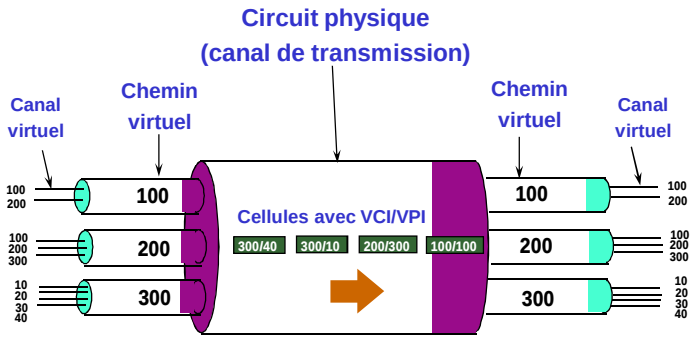
- **Deux interfaces**
  - UNI (User to Network Interface)
  - NNI (Network to Network Interface)



ATM ➔ Commutation de cellule sur des circuits virtuels

3. Couche ATM

Circuit physique, canal virtuel, chemin virtuel



3. Couche ATM

Canal virtuel, chemin virtuel, circuit physique

- **Canal virtuel (VC : virtual channel)**
  - Concept utilisé pour identifier (partiellement) une connexion pour envoyer les données d'un flux(User to Network Interface)
  - VCI (Virtual Channel Identifier) : Un Id est associé à chaque CV valable pour chaque switch. Le VCI change le long d'un circuit virtuel
- **Chemin virtuel (VP : virtual path)**
  - Concept utilisé pour regrouper des CV afin d'en faciliter la gestion
  - VPI (Virtual Path Identifier) : Un Id est associé à chaque VP valable pour chaque switch. Le VPI change le long d'un circuit virtuel
- **Circuit physique** : conduit de transmission : ligne de transmission

3. Couche ATM

Circuit virtuel

- **CV permanent**

  Les tables des switchs sont configurées de manière statique

- **CV temporaire**

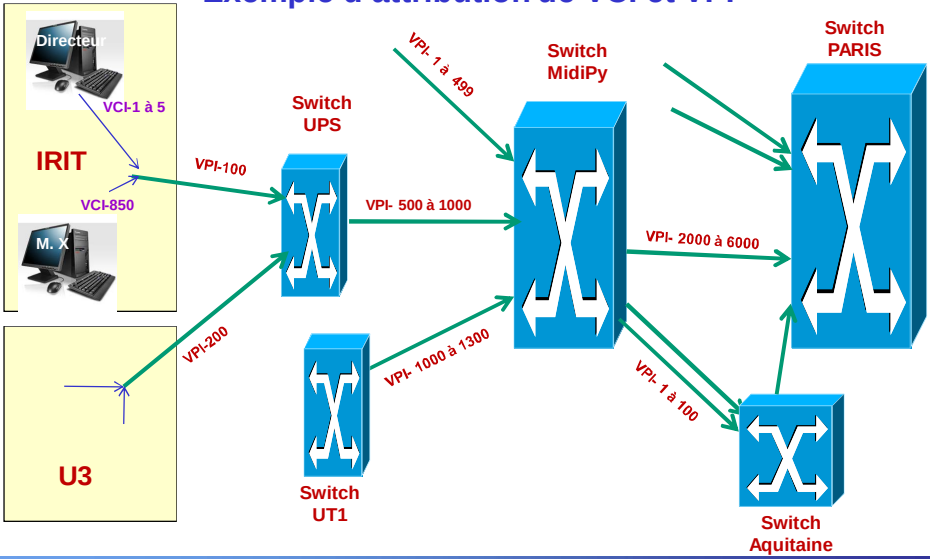
  Les tables des switchs sont configurées de manière dynamique lors de l'appel d'établissement de connexion

- **Des algorithmes de routage statiques/dynamiques sont utilisés. Les standards ATM ne spécifient pas d'algorithmes de routage.**

- **Choix des VCI et VPI : non spécifiés par le standard ATM**

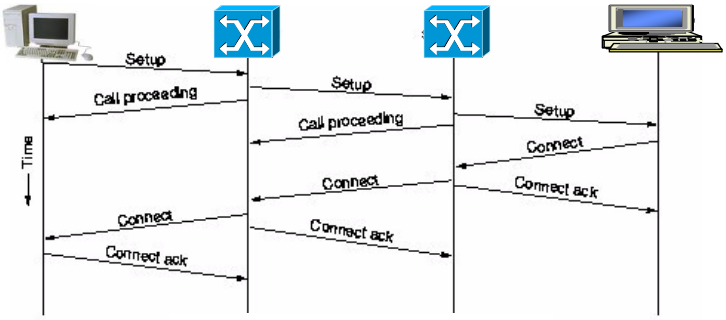
3. Couche ATM

Exemple d'attribution de VCI et VPI

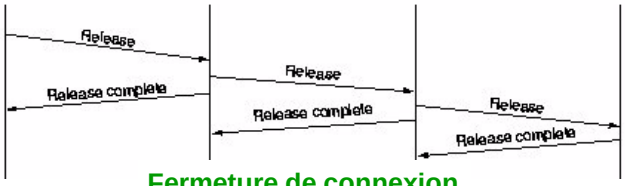


3. Couche ATM

Etablissement et fermeture de circuit virtuel



Etablissement de connexion



Fermeture de connexion

3. Couche ATM

Messages d'établissement/fermeture de circuit virtuel

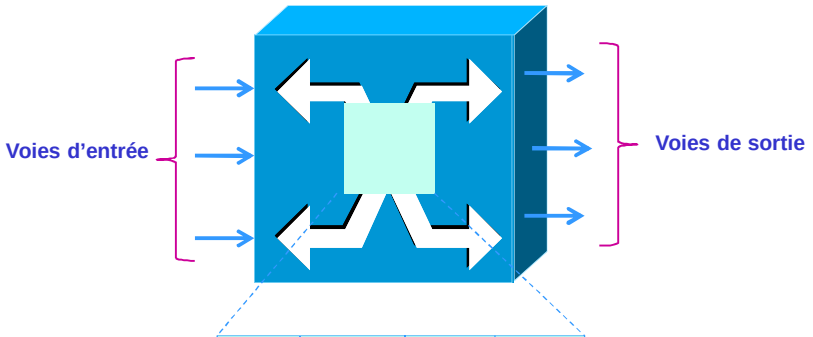
- **SETUP** : Demande d'établissement de circuit virtuel (i.e. connexion)
- **CALL PROCEEDING** : Demande de connexion en cours
- **CONNECT** : Acceptation de connexion
- **CONNECT ACK** : Confirmation de connexion
- **RELEASE** : Demande de fermeture de connexion
- **RELEASE COMPLETE** : Connexion fermée

Autres messages liés aux circuits virtuels

- **NOTIFY, STATUS, STATUS ENQUIRY, ALERT**

3. Couche ATM

Table de commutation



Une entrée dans la table par CV traversant le switch

Voie d'entrée	VPI/VCI entrant	Voie de sortie	VPI/VCI sortant

3. Couche ATM

Exemples de circuits virtuels

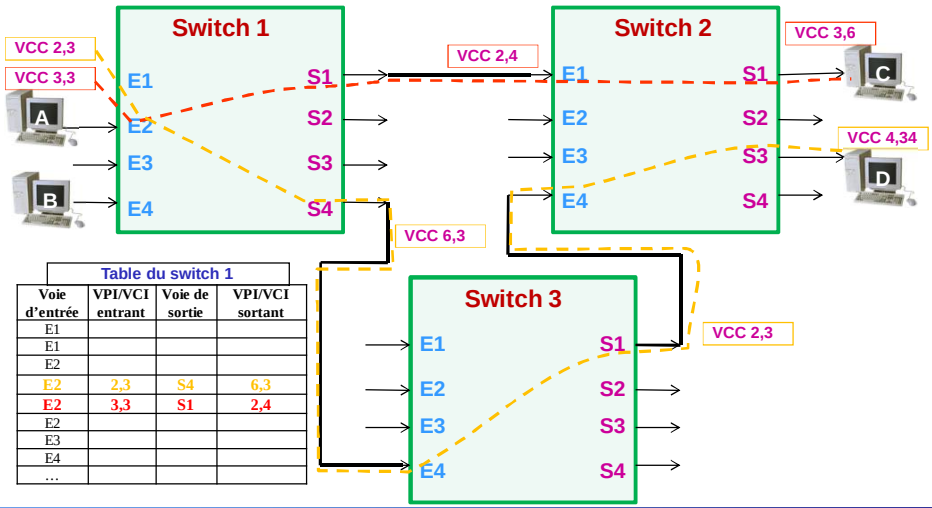


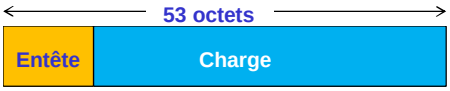
Table du switch 1

Voie d'entrée	VPI/VCI entrant	Voie de sortie	VPI/VCI sortant
E1			
E1			
E2			
E2	2,3	S4	6,3
E2	3,3	S1	2,4
E2			
E3			
E4			
…			

3. Couche ATM

Cellule ATM

- **Cellule de taille fixe**
  - Entête (5 octets)
  - Charge (48 octets)
    - → Données normales
    - → Données de signalisation
    - → Données de gestion



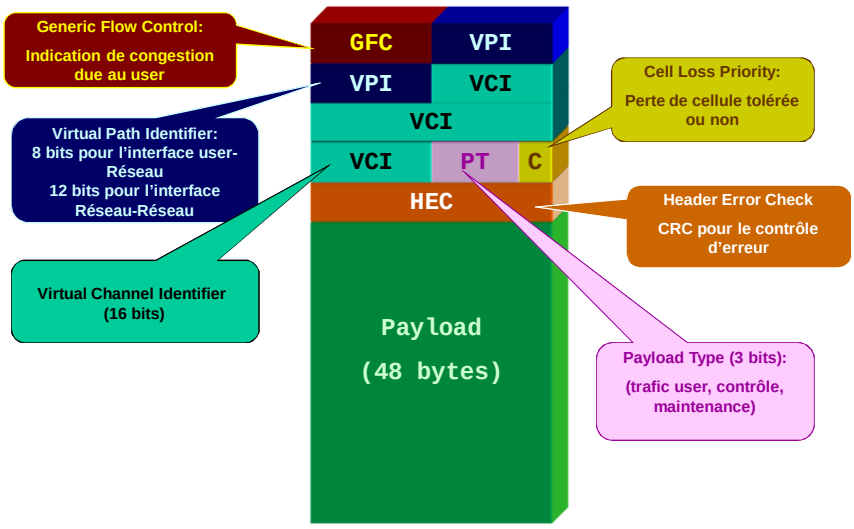
3. Couche ATM

Cellule ATM

- **Pourquoi une taille fixe ?**
  - Des cellules de taille constante permettent une meilleure utilisation des buffers
  - La commutation des cellules de taille fixe peut être optimisée : commutation câblée utilisant des registres
  - Les applications ciblées (voix, audio, vidéo) adaptées au découpage de flux continus en cellules de taille fixe
- **Quelle taille choisir ?**
  - Point de départ : mettre une portion de voix par cellule et par trame
  - US : préféraient 64 octets
  - Europe : préféraient 32 octets
  - Compromis : 48 octets (32 + 64 / 2)
  - 48 octets correspondent à 6 ms de voix téléphonique (la perte d'une cellule passe inaperçue chez le récepteur – 1 phonème dure environ 32 ms)

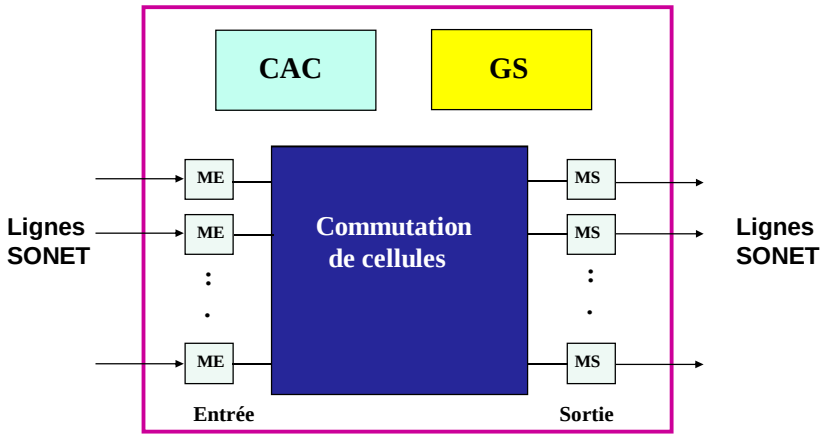
3. Couche ATM

Format de cellule ATM



3. Couche ATM

Architecture générique de switch ATM



ME = Module d'entrée MS = Module de sortie

CAC = Contrôle d'admission de connexion SM = Gestion de switch

3. Couche ATM

Fonctions réalisées par les switchs ATM

- **Commutation de cellules** des ports d'entrée vers les ports de sortie ; c'est la fonction principale
- **Etablissement et contrôle des VP et VC**
  - Utilisation d'un protocole de signalisation pour véhiculer les infos spécifiant le contrat (paramètres de trafic et paramètres de QoS)
  - Application d'un contrôle d'admission de nouvelle connexion
- **Gestion de réseau**
  - Gestion de fautes
  - Gestion de performances
  - Gestion de configurations

3. Couche ATM

Fonctions réalisées par les switchs ATM

- **Module d'entrée : pour chaque cellule entrante**
  - Extraction de cellules à partir de la trame SONET/SDH
  - Contrôle du HEC des cellules
  - Détermination du port et VP/VC de sortie (utiliser la table de commutation)
  - Pour les switchs de bordure : contrôle de trafic (seau percé)
  - Élaboration d'infos de gestion de réseau (taux d'utilisation…)
- **Module de commutation**
  - Aiguillage des cellules vers les ports de sortie
  - Rejet de cellule si débordement et/ou CLP=1
- **Modules de sortie : pour chaque cellule sortante**
  - Mise à jour du VPI/VPI (sortant)
  - Génération de HEC
  - Placement octet/octet de la cellule dans la trame SONET/SDH à partir
  - Elaboration d'informations d gestion de réseau

3. Couche ATM

Fonctions réalisées par les switchs ATM

- **Contrôle d'admission**
  - Sur la base des ressources disponibles (place vide dans les trames en sortie), de la destination du flux, des paramètres de flux et de QoS, le CAC décide d'accepter ou de refuser une demande de connexion
  - Négociation et renégociation avec les utilisateurs
  - Gestion et allocation des VP et VC en fonction des demandes et libérations de connexion

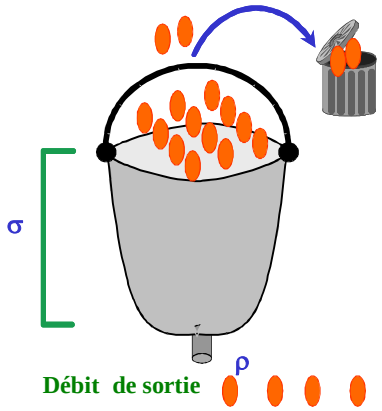
3. Couche ATM

Fonctions réalisées par les switchs ATM

- **Contrôle de trafic utilisateur**
  - **L'utilisateur peut volontairement ou non dépasser le débit de crête négocié lors de l'établissement de connexion**
    ➔ Impact sur la QoS offerte aux autres usagers
  - **Contrôle du trafic entrant sur chaque connexion**
  - **A chaque connexion est associé un seau percé (qui ne doit pas déborder)**
  - Seau percé (leacky bucket) défini par :
    → Débit moyen d'écoulement du seau (ρ)
    → Taille maximale du seau (σ)

3. Couche ATM

Fonctions réalisées par les switchs ATM – Seau percé



σ : taille maxi (burst Size)

ρ : débit moyen

3. Couche ATM

Mise en œuvre algorithmique du seau percé

```
TTA = ta(1)+I /* TTA initialisé à l'instant de l'arrivée de la première cellule */

Répéter indéfiniment
     Arrivée de la cellule k (k>1)
     Si TTA < ta(k)
               alors TTA = ta(k) + I
     Sinon     Si TTA > ta(k) + L
                         Alors cellule non conforme
               Sinon TTA = TTA + I
               Finsi
     Finsi
FinRépéter

TTA : Temps théorique d'arrivée (à l'arrivée de la première cellule TTA = ta(1) + I)
ta(k) : temps d'arrivée de la kème cellule
I : Incrément
L : Limite
```

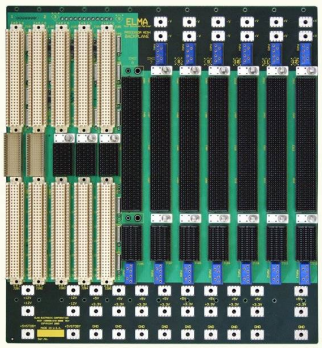
3. Couche ATM

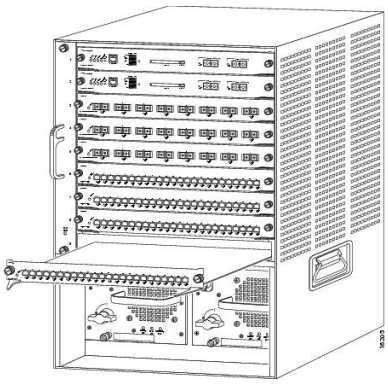
Architectures matérielles des switchs ATM

- **Propriétés attendues d'un switch ATM**
  - Très haut débit
  - Très faible délai de commutation ➔ **Réalisation câblée**
  - Très faible taux de perte de cellules
  - Capacité de diffusion
  - Faible coût d'implantation
  - …
- **Architectures matérielles de switch ATM**
  - **Architectures de fond de panier (utilisées quand il y a peu de lignes d'E/S)**
  - **Architectures à mémoire partagée (rares)**
  - **Architectures à multiplexeurs : *crossbar*, *Banyan*…**

3. Couche ATM

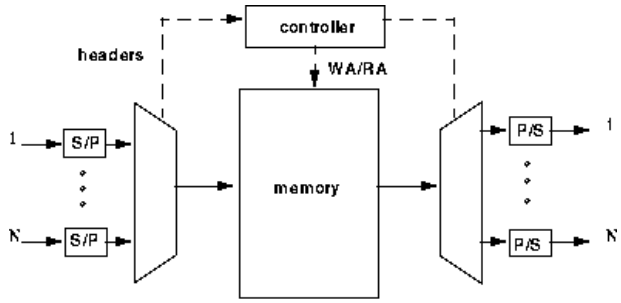
Switch ATM – Fond de panier





3. Couche ATM

Switch ATM – A mémoire partagée

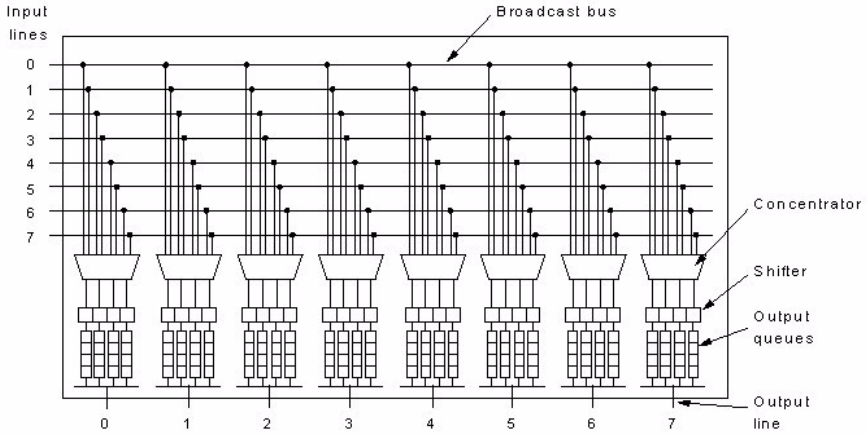


RA = read address
WA = write address
S/P = serial to parallel
P/S = parallel to serial

3. Couche ATM

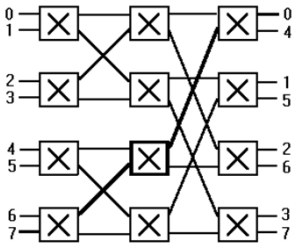
Multiplexeurs *crossbar* (totalement interconnectés)

- Les lignes d'entrée sont reliées à toutes les lignes de sortie.
- Le filtre correspondant au VPI/VCI de la cellule à commuter est passant (il laisse passer la cellule vers la voie de sortie)



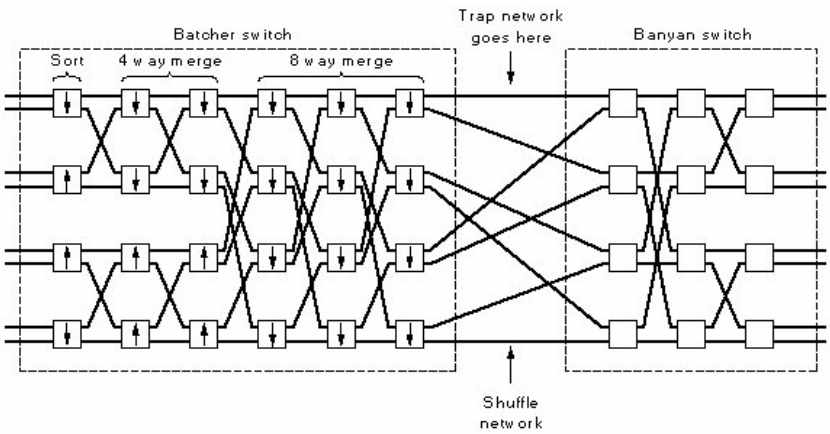
3. Couche ATM

Architecture Banyan



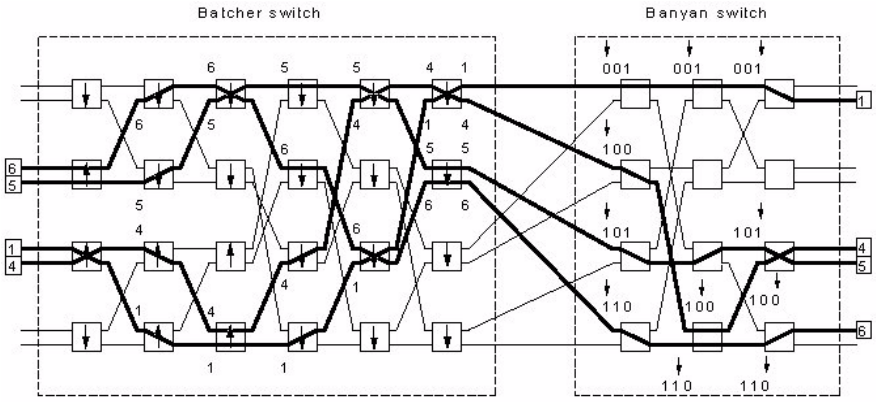
3. Couche ATM

Architecture Batcher-Banyan



3. Couche ATM

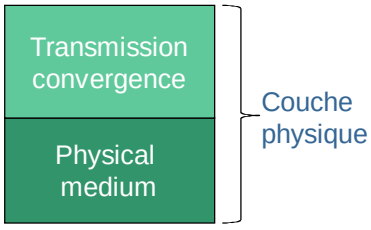
Architecture Batcher-Banyan – Exemple



4. Couche physique

Structure et fonctions de la couche physique

- **TCS (Transmission Convergence Sublayer)**
  - Reconnaissance de bit
  - Reconnaissance de frontière de cellule
  - Génération de trame
- **PM (Physical medium Sublayer)**
  - Emision et réception de bit en fonction du médium
  - Adaption au support optique, électrique...



4. Couche physique

Standards de transmission pour ATM

- **Transmission sur fibre optique**
  - 2 standards très proches
  - SONET (Synchronous Optical NETwork) /* Bell research */
    - débit de transmission de base: STS-1 (51,84 Mb/s)
  - SDH (Synchronous Digital Hierarchy)
    - Europe + autres
    - Débit de transmission de base: STM-1 (155,52 Mb/s)
    - SDH est en voie d'extinction sur le marché

4. Couche physique

Débits de transmission de SONET et SDH

STS/ OC	Débit	STM	Débit
STS/OC-1	51.84 Mb/s		
STS/OC-3	155.52 Mb/s	STM-1	155.52 Mb/s
STS/OC-12	622.08 Mb/s	STM-4	622.08 Mb/s
STS/OC-24	1.244 Gb/s		
STS/OC-48	2.488 Gb/s	STM-16	2.488 Gb/s
STS/OC-192	10 Gb/s	STM-64	10 Gb/s
STS/OC-256	13.271 Gb/s	STM-128	20 Gb/s
STS/OC-768	40 Gb/s	STM-256	40 Gb/s
STS/OC-3072	160 Gb/s	STM-1024	160 Gb/s

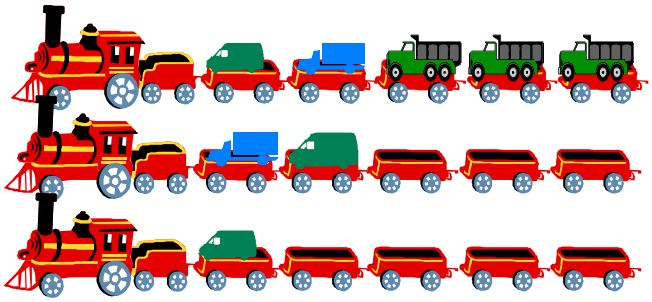
SONET
OC : Optical Carrier
STS : Synchronous Transport Signal

SDH
STM : Synchronous Transport Module

4. Couche physique

Transmission optique

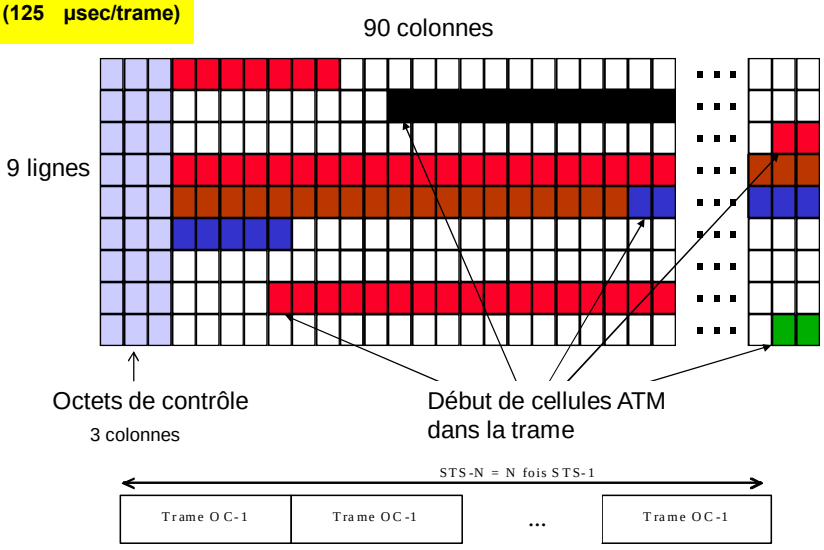
- Trame optique envoyée toutes les 125 µs (même vide)
- 125 µs : fréquence d'échantillonnage de la voix téléphonique



4. Couche physique

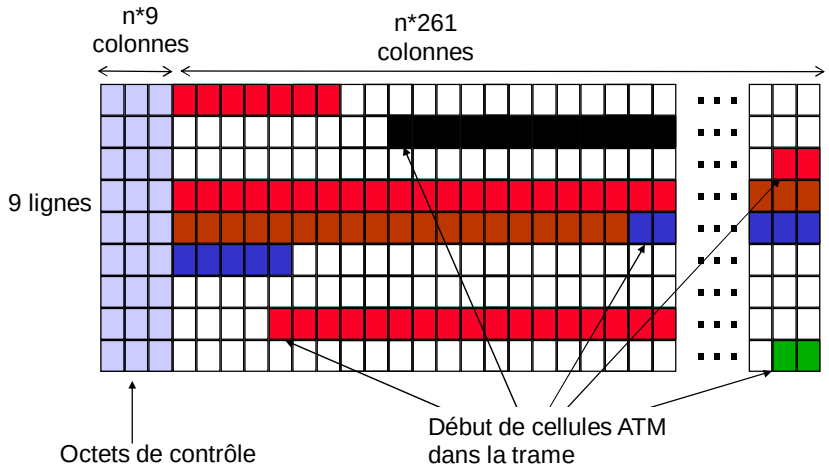
8000 trames/sec (125 µsec/trame)

Format de trame SONET - OC-1



4. Couche physique

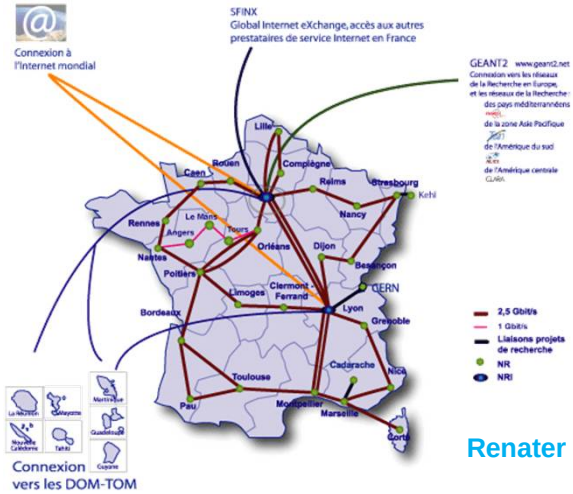
Format de trame SDH – STM-n



4. Couche physique

Exemple d'utilisation – Renater

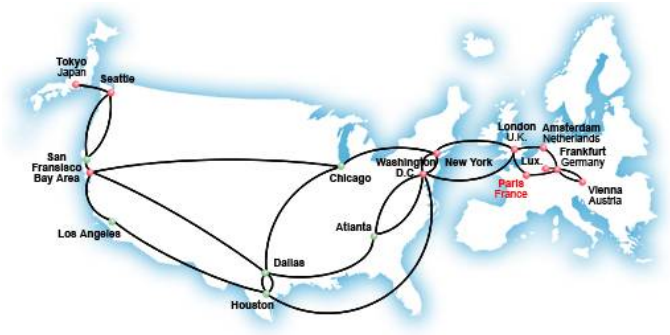
- En 2006 : Renater-4 a abandonné ATM mais gardé que SONET



Renater 5 (janvier 2009)

4. Couche physique

Exemple d'utilisation – Backbone mondial



- backbone Tout-IP sur Sonet/SDH
- une capacité plus de **250 Gbps**,
- la boucle européenne étant de 22 Gbps,
- le lien transatlantique est de 40 Gbps

5. Conclusion

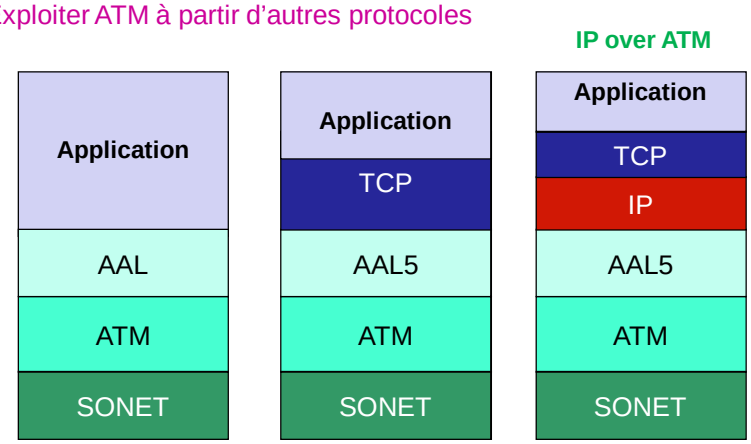
- ATM a apporté des avancées significatives dans le domaine des réseaux à QoS
- ATM a été le premier réseau à offrir QoS de bout en bout à grande échelle

- ATM : abandonné petit à petit
  - Jugé trop complexe
  - Trop cher
  - Pression de la communauté IP (IP gratuit vs. ATM payant)
  - Pression stratégique

5. Conclusion

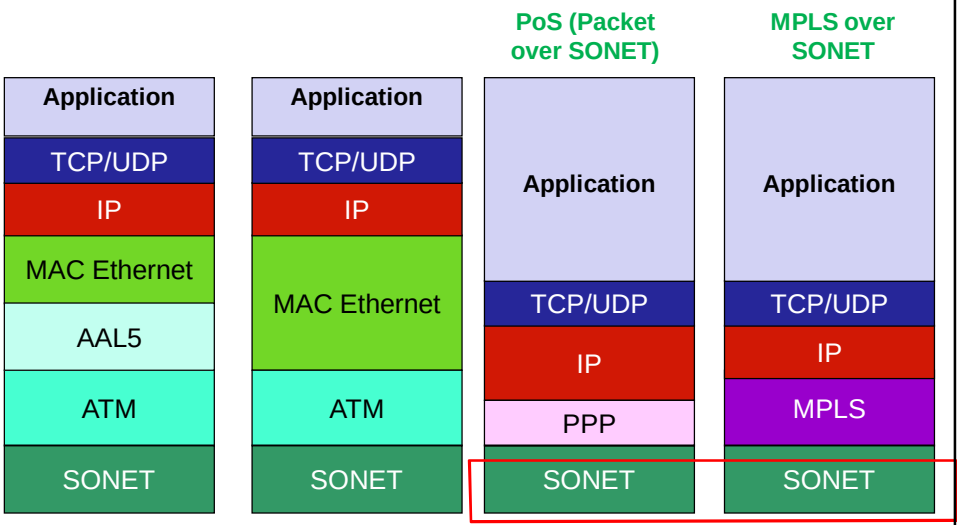
Diverses solutions d'exploitation des infrastructures ATM

- ATM comme réseau cœur (jusqu'à présent)
- Exploiter ATM à partir d'autres protocoles



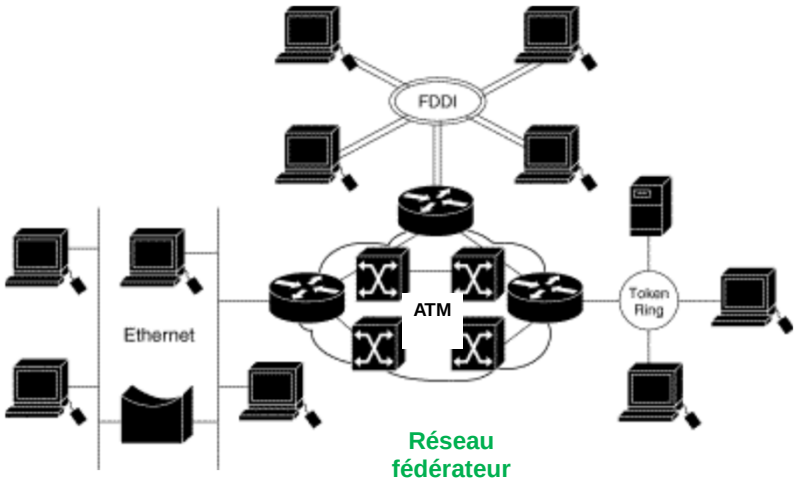
5. ATM et les autres protocoles et réseaux

Diverses solutions d'exploitation des infrastructures ATM



5. ATM et les autres protocoles et réseaux

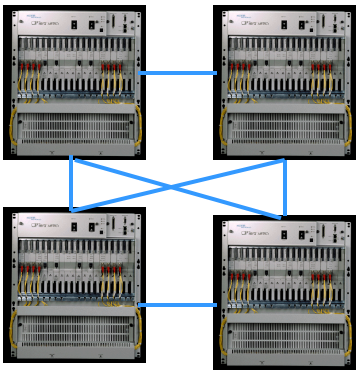
Diverses solutions d'exploitation des infrastructures ATM



Réseau fédérateur

6. Conclusion

Asynchronous Transfer Mode



Automated Teller Machine

Chapitre 6

Réseaux sans fil

Caractéristiques et principaux standards

7. Standards et technologies de réseaux mobiles (Res Mob)

(Bluetooth, ZigBee, Wifi, WiMAX, WiRAN)

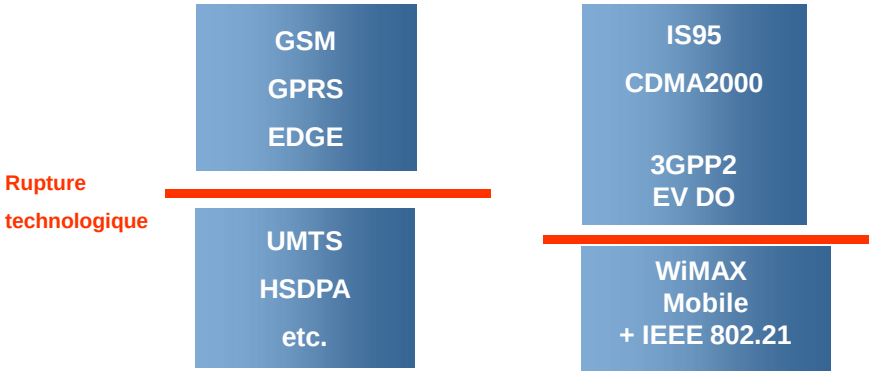
7. Standards et technologies de Res Mob

Classes de réseaux sans fils – selon l'étendue

- **WBAN: wireless body area network**
- **WPAN: wireless personal area network**
- **WLAN: wireless local area network**
- **WRAN: wireless regional area network**
- **WWAN: wireless wide area network**

7. Standards et technologies de Res Mob

Réseaux de télécom (WWAN)



GSM : Global System for Mobile communications
EDGE : Enhanced Data Rates for GSM Evolution
HSDPA : High Speed Downlink Packet Access
EV DO Evolution-Data Optimized

GPRS: General Packet Radio Service
UMTS : Universal Mobile Telecommunications System
3GPP2 : *3rd Generation Partnership Project 2*

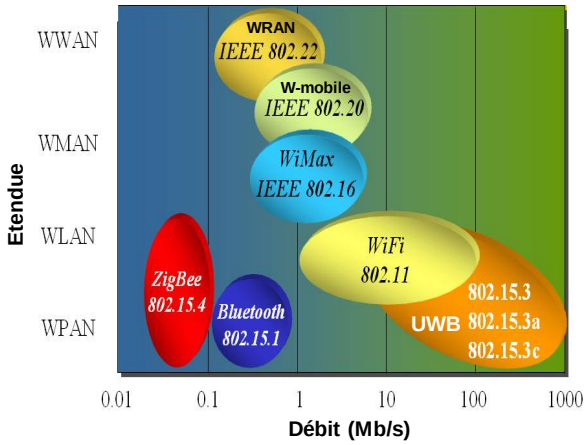
7. Standards et technologies de Res Mob

Standards de Réseaux IT

- **WPAN** : IEEE 802.15 et WiMedia
  - IEEE 802.15.1 - Bluetooth
  - IEEE 802.15.3 – UWB (Ultra WideBand)
  - IEEE 802.15.4 – ZigBee
- **WLAN** : IEEE 802.11 et WiFi
  - IEEE 802.11b, a, g
  - IEEE 802.11s, i, f
  - IEEE 802.11e (qualité de service)
  - IEEE 802.11n (190 Mb/s + intégration de 11e, 11f et 11i)
- **WMAN** : IEEE 802.16 et WiMax
  - IEEE 802.16-2004
  - IEEE 802.16e/IEEE 802.20 (Wi-Mobile)
- **WRAN** : IEEE 802.22 et WiRAN
  - Utilisation de la bande TV 54-698 MHz

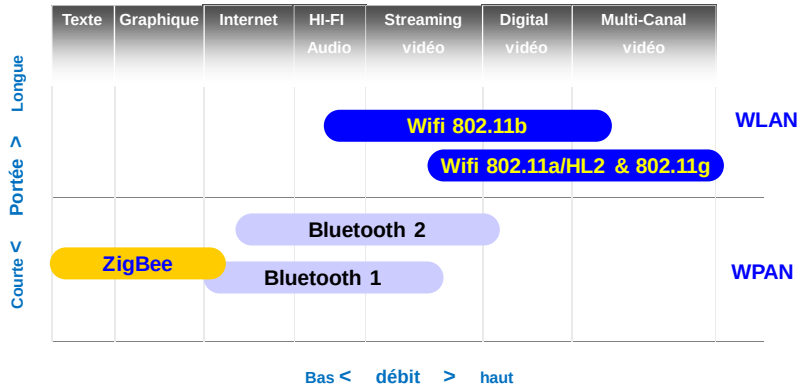
7. Standards et technologies de Res Mob

Portées et débits des principales technologies sans fils



7. Standards et technologies de Res Mob

Comparaison des principales technologies sans fils



7. Standards et technologies de Res Mob

Comparaison des principales technologies sans fils

Market Name	ZigBee™	---	Wi-Fi™	Bluetooth™
Standard	802.15.4	GSM/GPRS CDMA/1xRTT	802.11b	802.15.1
Application Focus	Monitoring & Control	Wide Area Voice & Data	Web, Email, Video	Cable Replacement
System Resources	4KB - 32KB	16MB+	1MB+	250KB+
Battery Life (days)	100 - 1,000+	1-7	.5 - 5	1 - 7
Network Size	Unlimited (2^{64})	1	32	7
Bandwidth (KB/s)	20 - 250	64 - 128+	11,000+	720
Transmission Range (meters)	1 - 100+	1,000+	1 - 100	1 - 10+
Success Metrics	Reliability, Power, Cost	Reach, Quality	Speed, Flexibility	Cost, Convenience

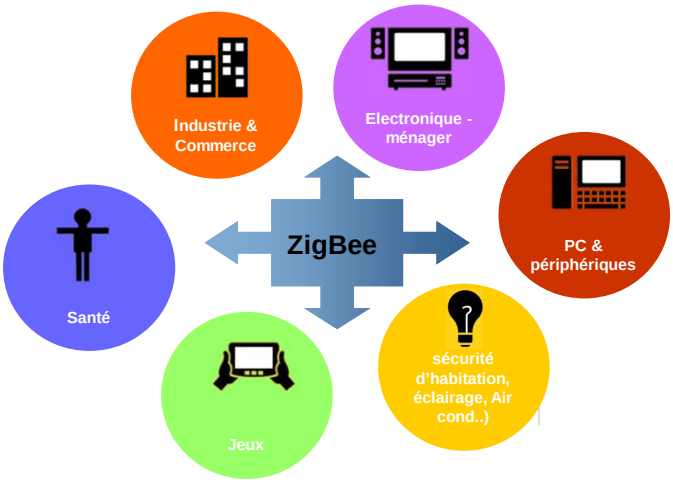
7. Standards et technologies de Res Mob

Réseaux ZigBee – WiMedia (std IEEE 802.15.4)

- Nom = contraction de "zig-zagging patterns of bees between flowers"
- Technologie pour réseaux de capteurs
- Basé sur le Std IEEE 802.15.4 (CSMA/CA)
- Créé par ZigBee Alliance
- Caractéristiques :
  - Faible débit (20 à 250 Kb/s)
  - Faible distance
  - Faible consommation
  - Petits paquets de données

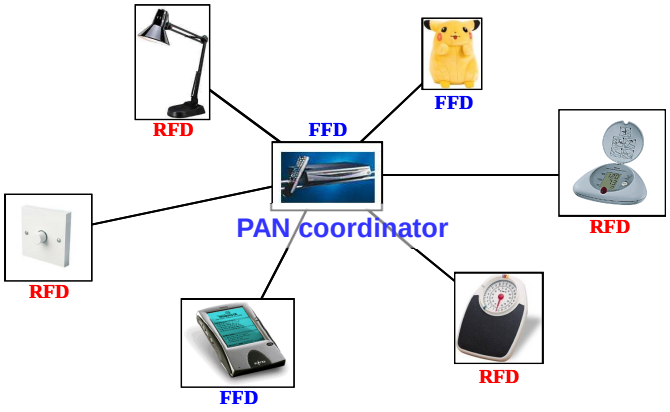
7. Standards et technologies de Res Mob

Réseaux ZigBee - Domaines d'applications



7. Standards et technologies de Res Mob

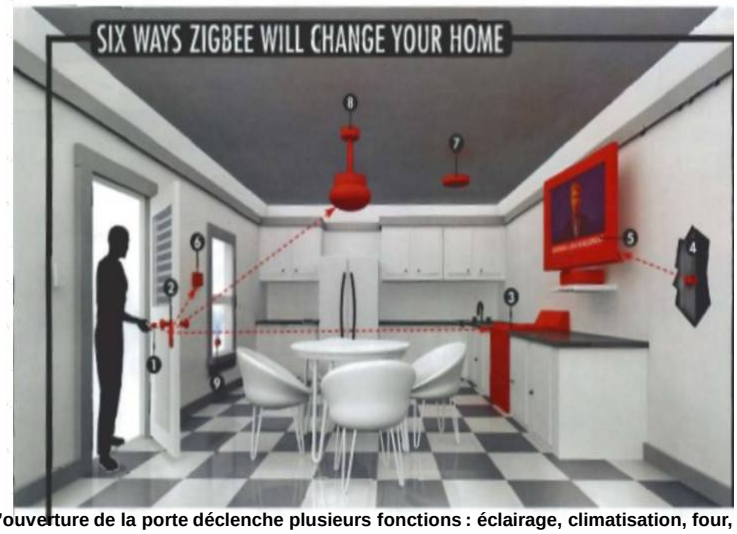
Réseaux ZigBee - Exemple de réseau



Full Function Device (FFD)
Reduced Function Device (RFD)

7. Standards et technologies de Res Mob

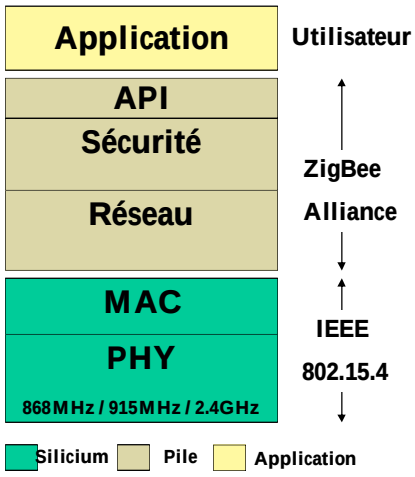
Réseaux ZigBee - Exemple de réseau



L'ouverture de la porte déclenche plusieurs fonctions : éclairage, climatisation, four, TV, musique

7. Standards et technologies de Res Mob

Réseaux ZigBee – Architecture



7. Standards et technologies de Res Mob

Réseaux Bluetooth (Std IEEE 802.15.1)

- Bluetooth fonctionne dans la bande (sans licence) centrée sur 2.45GHz avec des canaux RF : 2420+k MHZ, k=0..78.
- Distance maxi entre nœuds : 10 m
- Débit : 720 kb/s
- Coût très bas (chip à ~$5).
- Très faible consommation : 100 mW à 100 m et 1 mW à 1 m
- Flux ciblés : data, audio, graphiques, vidéo (!)
- Appareils ciblés : personnels (PC et périphériques, caméra, appareil photo…).


Clavier et souris Bluetooth


Oreillette Bluetooth


Adaptateur USB Bluetooth


Jouet Bluetooth

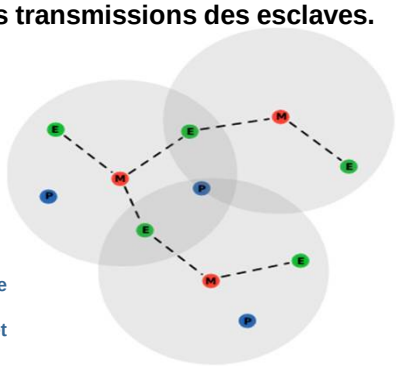

Lunettes Bluetooth


Montre Bluetooth

7. Standards et technologies de Res Mob

Réseaux Bluetooth – Principe général

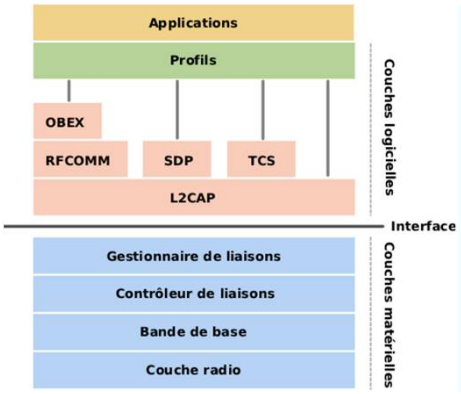
- **Jusqu'à 8 appareils peuvent former un piconet.**
- **Au maximum 10 piconets dans la même zone de couverture.**
- **Chaque piconet est composé d'un maître et d'esclaves.**
- **Le maître orchestre les transmissions des esclaves.**



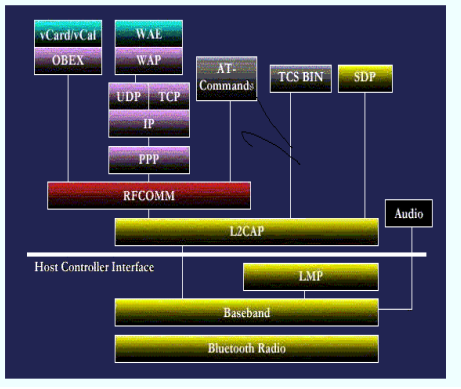
E : esclave
M : Maître
P : Piconet

7. Standards et technologies de Res Mob

Réseaux Bluetooth – Pile de protocole



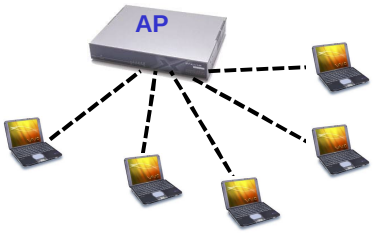
Architecture générale



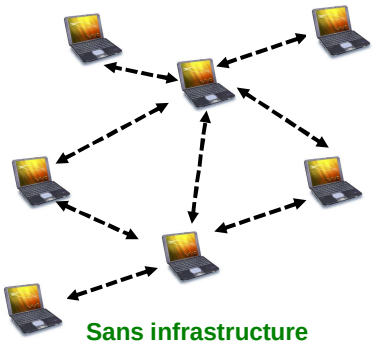
Architecture spécialisée

7. Standards et technologies de Res Mob

Réseaux Wifi (WIreless FIdelity)



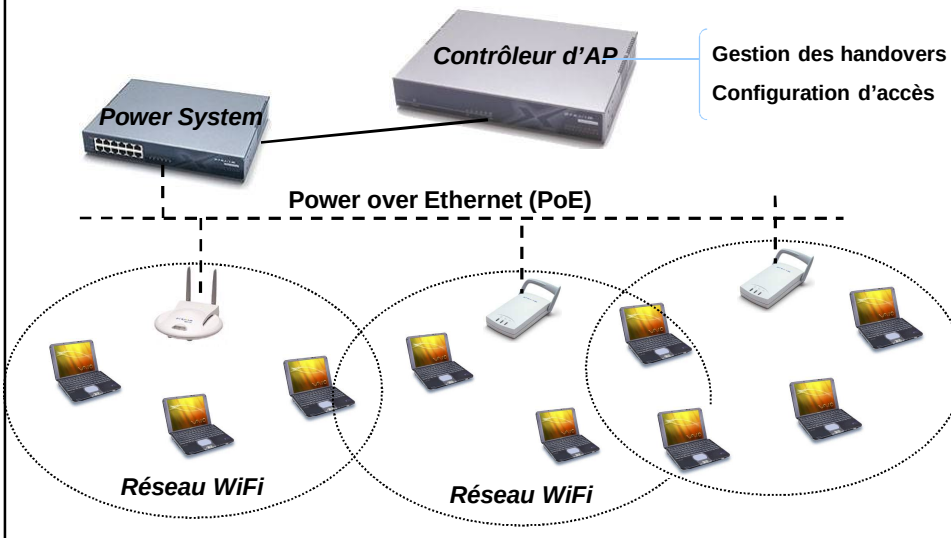
Avec infrastructure



Sans infrastructure
= réseau ad hoc
= MANET (Mobile Area Network)

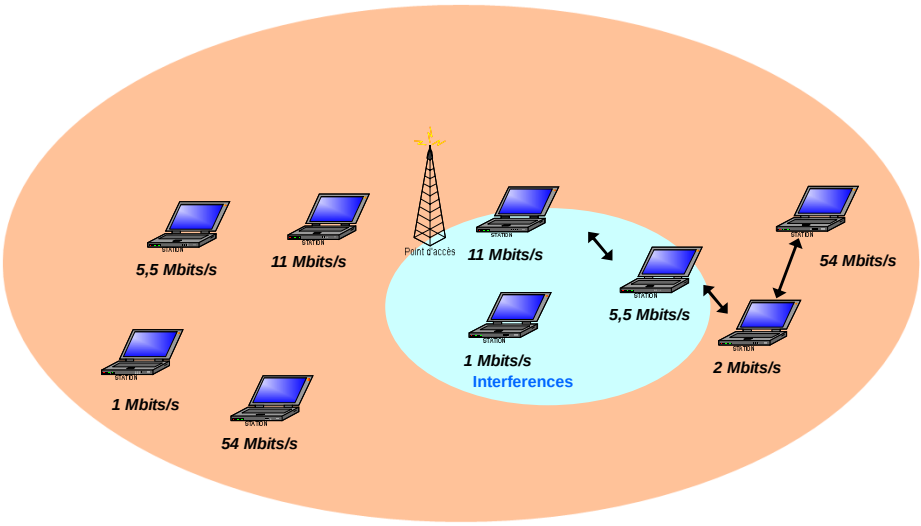
7. Standards et technologies de Res Mob

Réseaux Wifi



7. Standards et technologies de Res Mob

Réseaux Wifi – Attention aux débits

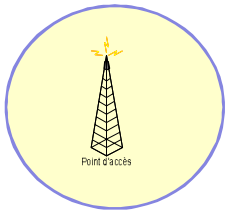


7. Standards et technologies de Res Mob

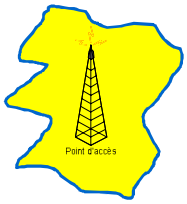
Réseaux Wifi – Limites

- **Environnement**
  - Murs, meubles, objets divers
- **Distance entre équipements**
- **Interférences**
  - Autres réseaux voisins
  - Fours microondes
  - Autres équipements

➔**Technologies MIMO**



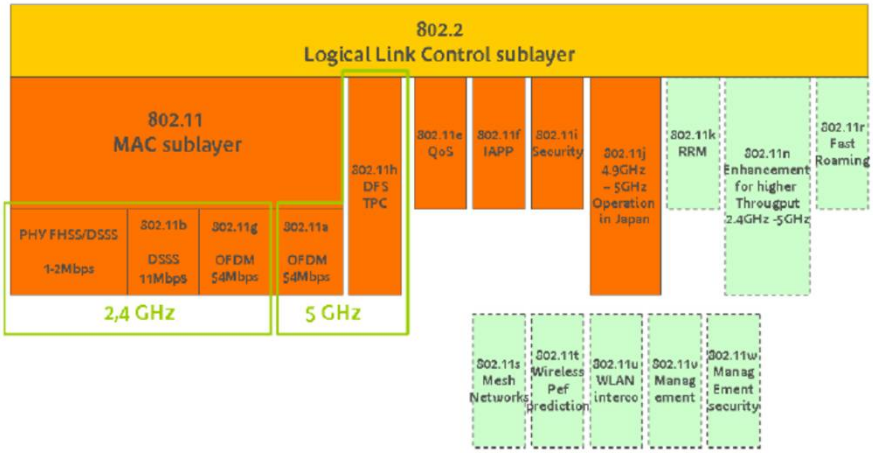
Portée idéale



Portée réelle

7. Standards et technologies de Res Mob

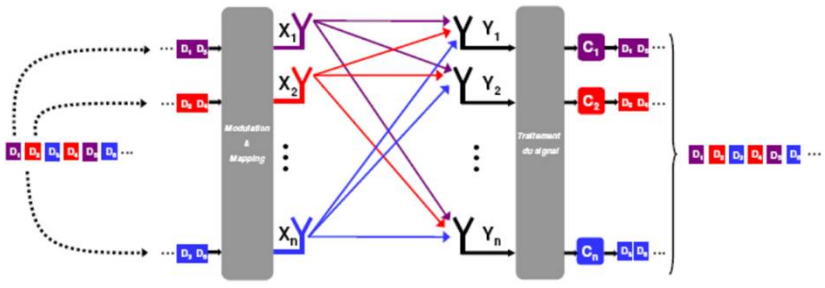
Réseaux Wifi – Beaucoup de standards



7. Standards et technologies de Res Mob

Réseaux Wifi – Technologies MIMO

(Multiple Input Multiple Output)

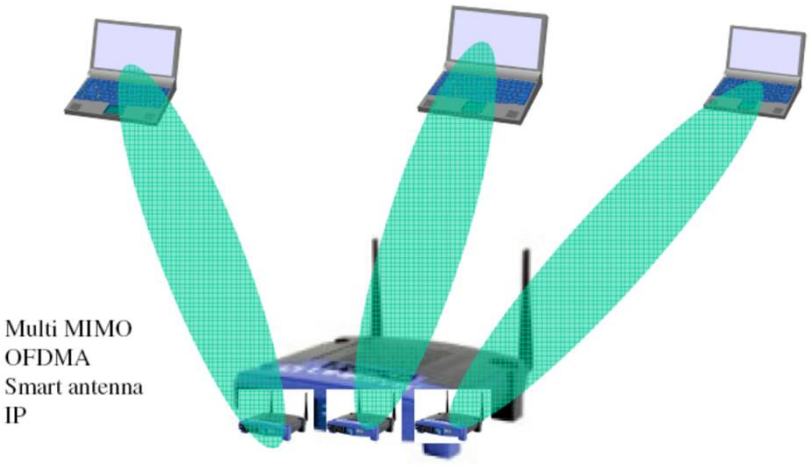


Pour : vitesse de transmission = f(Nombre d'antennes)

Contre : difficulté de mise en œuvre, peu de diversité

7. Standards et technologies de Res Mob

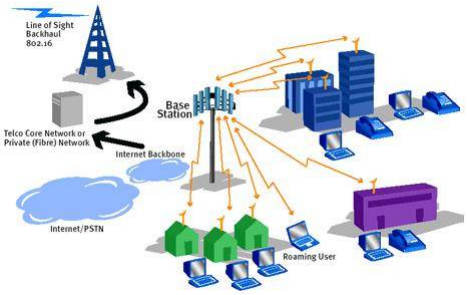
Réseaux Wifi – Technologies MIMO



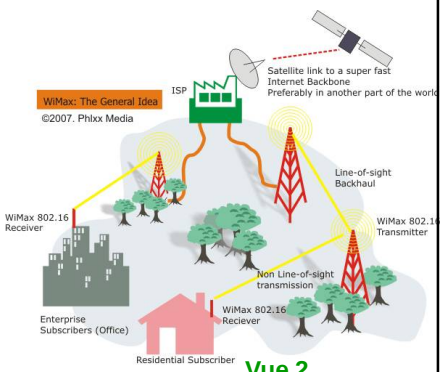
7. Standards et technologies de Res Mob

Réseaux WiMAX (Std IEEE 802.16)

WiMAX = Worldwide interoperability for Microwave Access



Vue 1



Vue 2

- **Réseau métropolitain (ou d'agglomération)**
- **50 km à 70 Mb/s (en théorie) -- 10 km à 20-30 Mb/s (en pratique)**

7. Standards et technologies de Res Mob

WiMAX – Exemple d'antennes

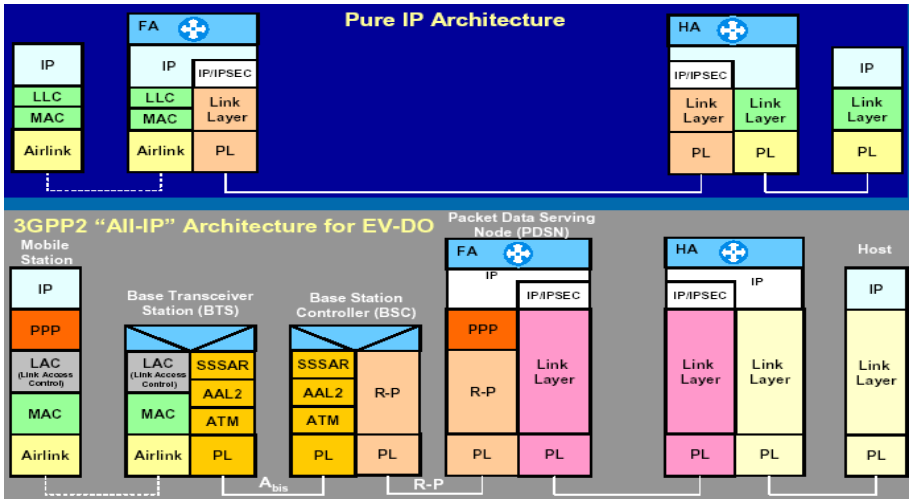
7. Standards et technologies de Res Mob

WiMAX mobile (std IEEE 802.16e)

- **Nouvelle spécification pour Universal WiMAX**
  - Fréquence < 3.5 GHz
  - Au moins 1 Mbit/s par utilisateur
  - Vitesse jusqu'à 130 km/h
  - Grande cellule (1 km approximativement)
  - Ambiant
  - Garantie de QoS
  - Sécurité EAP-TLS

7. Standards et technologies de Res Mob

WiMAX mobile (std IEEE 802.16e)



7. Standards et technologies de Res Mob

Réseaux WiMAX mobile (norme IEEE 802.16m)

- Std à approuver en 2009
- Transmission en SOFDMA
- Basé sur les réseaux cognitifs
- 1 Gb/s (downlink)
- 100 Mb/s (uplink)

7. Standards et technologies de Res Mob

Réseaux WiRAN – Wireless Regional Area Network (Std IEEE 802.22)

- **Bande de fréquence : 54 – 862 MHz**
  - France : SECAM sur la bande 47 – 798 MHz
- **Cognitive radio**
  - Terminaux sans licence mais ne perturbant pas les communications avec licence
- **Canaux de 6, 7 ou 8 MHz**
  - Vitesse de transmission : 18 Mbit/s / canal de 6 MHz
  - Voie descendante 1,5 Mbit/s à 4 Mbit/s
  - Voie montante : 384 kbit/s ?
- **Puissance : 1 W descendant, 100 mW montant**
- **Technique de transmission :** OFDM
- **Support de la qualité de service au niveau MAC**
- **Coût très faible**

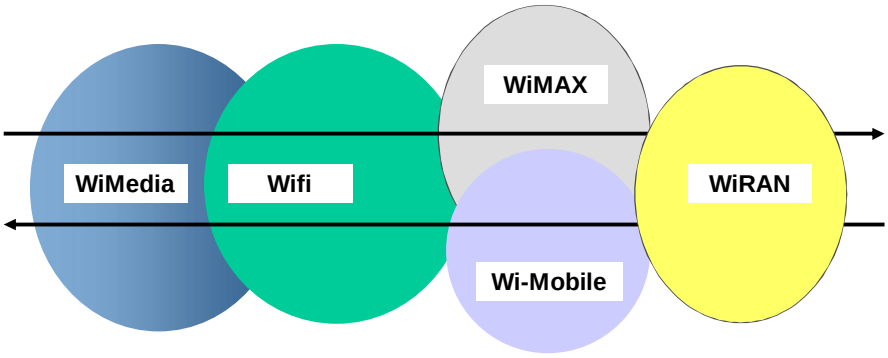
7. Standards et technologies de Res Mob

Réseaux WiRAN (Std IEEE 802.22)

- **Le terminal n'a pas besoin d'être déclaré (aux USA)**
- **Les caractéristiques radio sont contrôlées par l'émetteur**
- **GPS/Galileo pour déterminer les fréquences à utiliser**
- **Couverture jusqu'à une cinquantaine de kilomètres**
- **600 terminaux à 1 Mbit/s pour un canal de 6MHz avec la technologie d'allocation cognitive**
- **300 MHz de bande passante**
  - 30 000 utilisateurs multimédia par point d'accès
  - 1 000 000 de paroles téléphoniques

7. Standards et technologies de Res Mob

Handover entre les différents standards

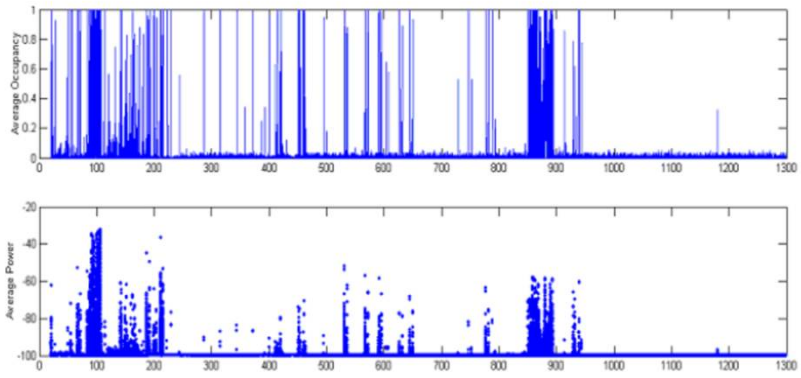


Principale difficulté : maintenir la QoS pendant les handovers

7. Standards et technologies de Res Mob

Réseaux cognitifs

- Spectre de fréquences dans les réseaux actuels



7. Standards et technologies de Res Mob

Réseaux cognitifs

- **Aujourd'hui : spectre de fréquences semble quasi complet, car les réseaux actuels sont peu adaptatifs**
- **Futur : plus de fréquences seront disponibles + équipements intelligents ➔ spectre quasi inoccupé**
- **Radio cognitive**
  - **Scrutation permanente de l'air à la recherche de fréquences libres**
  - **Analyse du spectre pour déterminer les meilleures fréquences à utiliser**
  - **Transmettre sur les fréquences libres**
  - **Décision distribuée de choix de bandes de fréquences entre partenaires dans une session**
  - **Changer de fréquences en cas de détection de collisions fréquentes sur la bande actuelle**
  - **Utilisation de *smart* antennes (adaptation de l'orientation, du choix de fréquences…)**

Chapitre 7

Réseaux cellulaires

1. Besoins des utilisateurs et évolution des réseaux cellulaires

Besoins des utilisateurs

- Types de flux diversifiés : voix, images, sons, textes, data
- Types d'applications
  - Du très général (eg. messagerie) au spécifique (travail personnel et spécialisé)
  - Du grand public au spécialiste (commercial, médecin urgentiste…)
- Qualité de service
  - Débit, temps de réponse
  - Disponibilité (« *anywhere, anytime connected* »)
  - Sécurité
- Terminaux : intégration (tout en un)

1. Besoins des utilisateurs et évolution des réseaux cellulaires

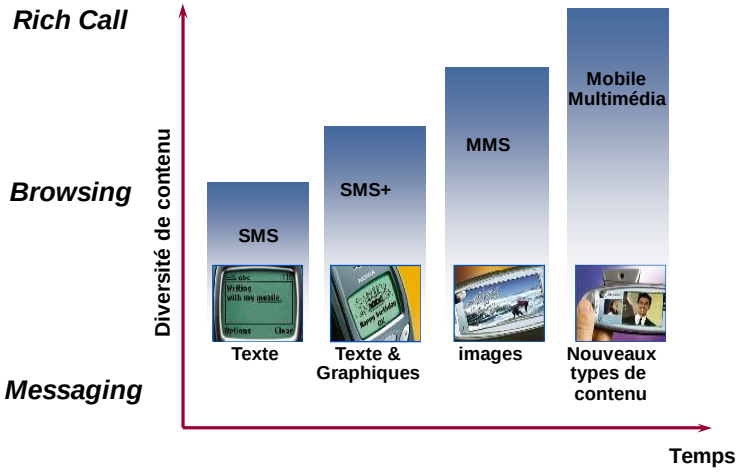
Mobile = tout en un

1. Besoins des utilisateurs et évolution des réseaux cellulaires

Mobile = accès à tout

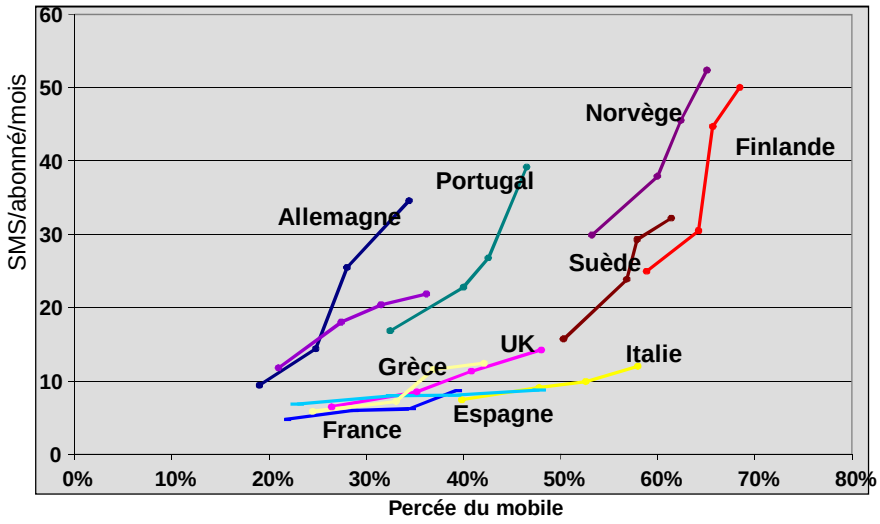
1. Besoins des utilisateurs et évolution des réseaux cellulaires

Evolution de la messagerie



1. Besoins des utilisateurs et évolution des réseaux cellulaires

Croissance des SMS en Europe (2006-2007)



1. Besoins des utilisateurs et évolution des réseaux cellulaires

Grand public – Vagues des réseaux sans fils

- **Vague 1 : téléphonie mobile**
  - Encore en cours
  - Business le plus important
- **Vague 2 : Accès sans fil à Internet**
  - Accès Internet via les WLAN (Wifi) personnels, d'entreprises ou d'organisations
  - Prolifération des hot spots
  - 2.5 G et 3G en compétition pour l'accès à Internet via le mobile
- **Vague 3 : Réseaux ad hoc (actuellement)**
  - Interconnexion de mobiles non reliés à des infrastructures
  - Interopérabilité entre réseaux hétérogènes
- **Vague 4 : équipements de plus en plus invisibles !**

1. Besoins des utilisateurs et évolution des réseaux cellulaires

Classes de réseaux sans fils

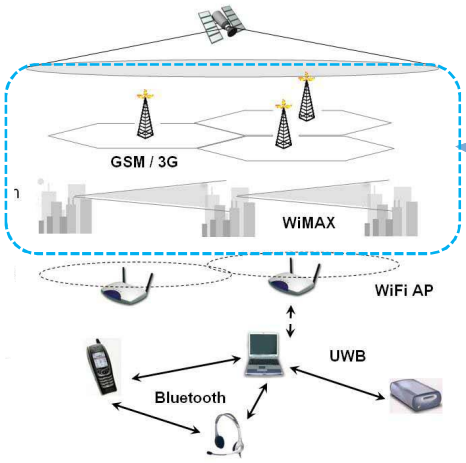
Réseaux de satellite

Wireless Wide Area networks

Wireless Metrop. Area networks

Wireless Local Area networks

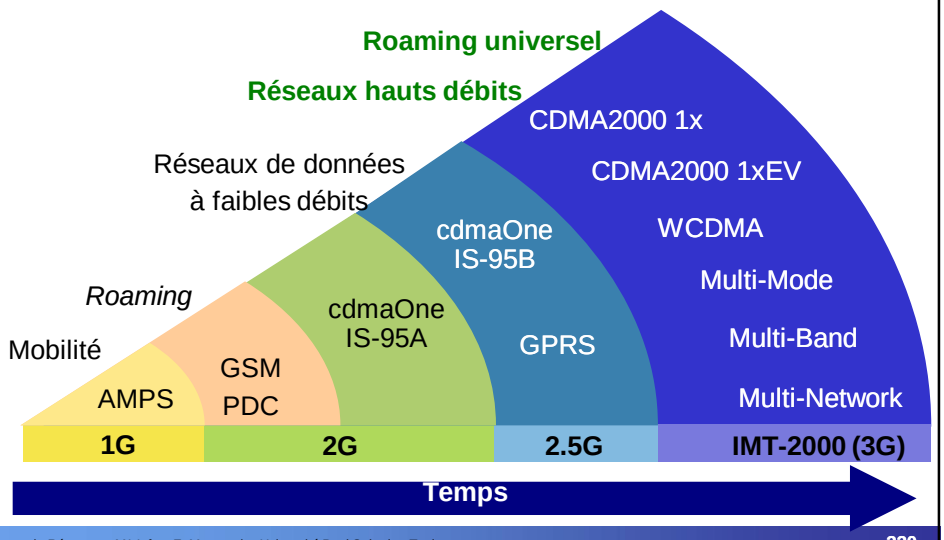
Wireless Personal Area networks



Champ des réseaux cellulaires B3G

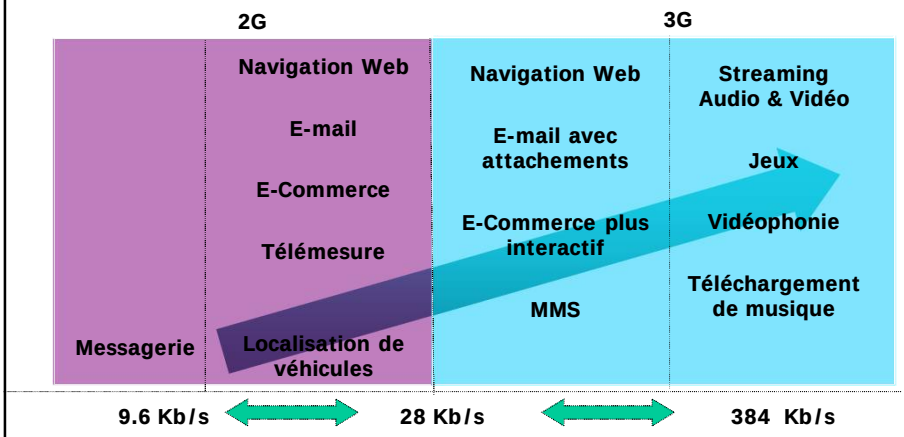
1. Besoins des utilisateurs et évolution des réseaux cellulaires

Positionnement des réseaux cellulaires



1. Besoins des utilisateurs et évolution des réseaux cellulaires

Quelques services phares des réseaux 2G et 3G



1. Besoins des utilisateurs et évolution des réseaux cellulaires

Quelques ordres de grandeurs -

Temps de transfert de 3 min d'un fichier son MP3

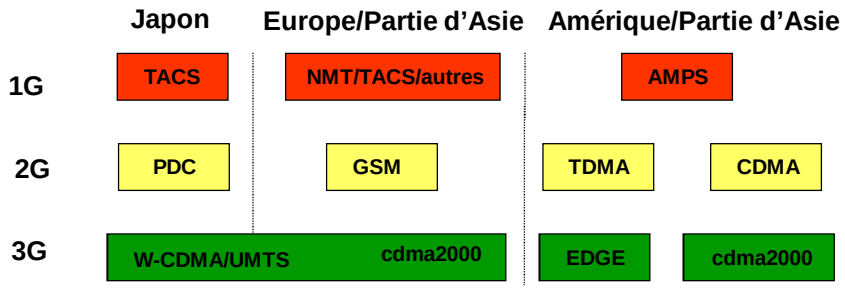
Interface	Débit	Temps de téléchargement en seconde
GSM	9.6 kb/s	2466 (41 minutes)
IS-95A CDMA	14.4 kb/s	1852 (31 minutes)
GPRS	45 kb/s	526 (8.8 minutes)
IS-95B CDMA	64 kb/s	364 (6 minutes)
EDGE	80 kb/s	295 (5 minutes)
CDMA2000 1X	144 kb/s	161 (2.7 minutes) à 1.25 MHz
WCDMA	384 kb/s	61 (1 minute) à 5 MHz
1xEV-DO	2.4 Mb/s	11 (0.2 minutes) à 1.25 MHz

Du GSM à 1xEV-DO : réduction du temps de transfert d'un facteur de 200

1. Besoins des utilisateurs et évolution des réseaux cellulaires

Standards de réseaux cellulaires et leur évolution

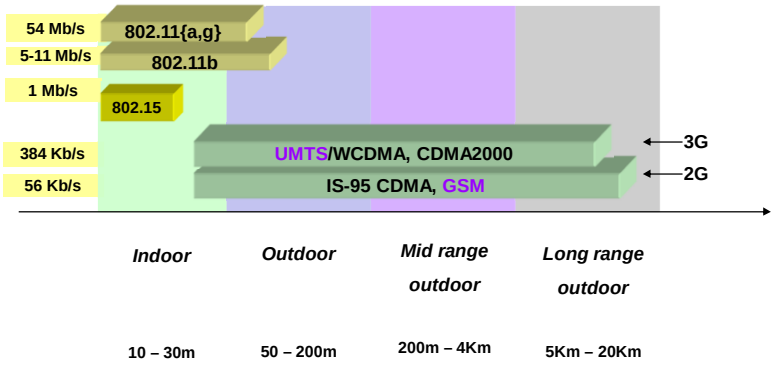
- **Raisons stratégiques ➔ Pas de standard commun pour le moment**



TACS : Total Access Communication System	NMT : Nordic Mobile Telephone
AMPS : Advanced Mobile Phone System	*PDC : Personal Digital Cellular*
EDGE : Enhanced Data Rates for GSM Evolution	*CDMA :Code Division multiple access*
GSM : Global System for Mobile communications	*UMTS* : Universal Mobile Telecommunications System)

1. Besoins des utilisateurs et évolution des réseaux cellulaires

Classes de réseaux sans fils



1. Besoins des utilisateurs et évolution des réseaux cellulaires

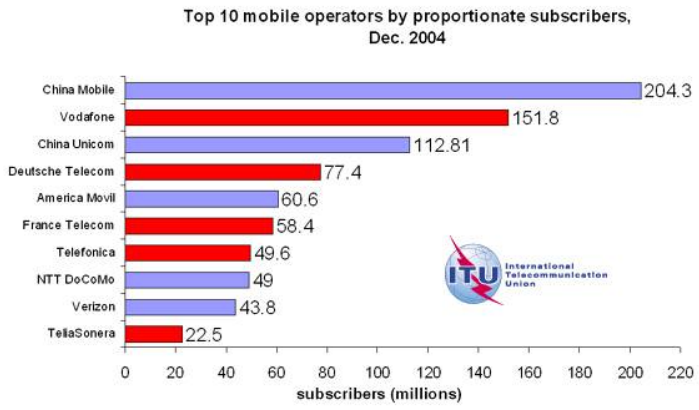
Plates-formes d'applications pour réseaux cellulaires

- **Pour l'accès aux services par le grand public**
  - **WAP** : a eu peu de succès réel mais toujours en activité
  - **SMS** : échange de textes – l'appli la plus populaire
  - **MMS**: échange d'images – s'impose de plus en plus
  - **iMode** : développé au Japon – forme évoluée du WAP – permet l'accès à Internet – tarde à s'exporter réellement

- **Pour le développement d'applications/services par les spécialistes**
  - **J2ME** (Java 2 Micro Edition) : développement d'applications Java pour les technologies mobiles (le mobile devient un ordinateur)
  - **BREW** (*Binary Runtime Environment for Wireless*): Plateforme de Qualcomm pour le développement d'applications pour mobiles

1. Besoins des utilisateurs et évolution des réseaux cellulaires

Opérateurs dominants dans le monde



1. Besoins des utilisateurs et évolution des réseaux cellulaires

Problèmes et défis liés réseaux sans fils

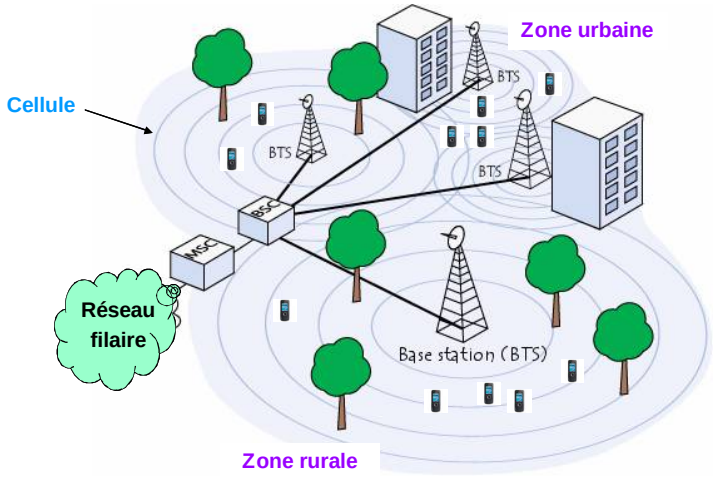
- **Atout : Continuité d'accès aux services pour les utilisateurs mobiles**
- **Problèmes (limites)**
  - Sensibilité aux interférences (fours micro-ondes, moteurs électriques…)
  - Affaiblissement des signaux se propageant dans l'air
  - Difficulté de synchronisation de niveau physique car les signaux se propagent et arrivent sur différents chemins
  - Taux de perte plus élevé que pour les réseaux filaires
  - Débits plus faibles que les réseaux filaires
  - Vulnérabilité des signaux (signaux émis dans l'air captés par tous)
  - Prise en compte de la mobilité des utilisateurs
    - Difficultés de localisation précise des utilisateurs
    - Difficultés de maintien de la QoS
    - Difficultés d'interopérabilité entre technologies (*roaming* universel)
    - Vie privée affectée (on peut tracer les déplacements)
  - Inadéquation des implantations des protocoles conçus pour le monde filaire

2. Principes de base des réseaux cellulaires

Aspects visibles des réseaux cellulaires

2. Principes de base des réseaux cellulaires

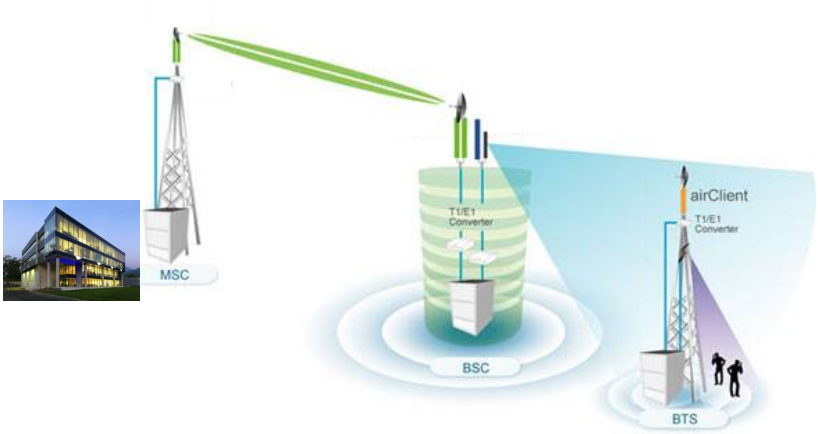
Eléments de base d'un réseau cellulaire – Vue 1



BTS
BSC
MSC

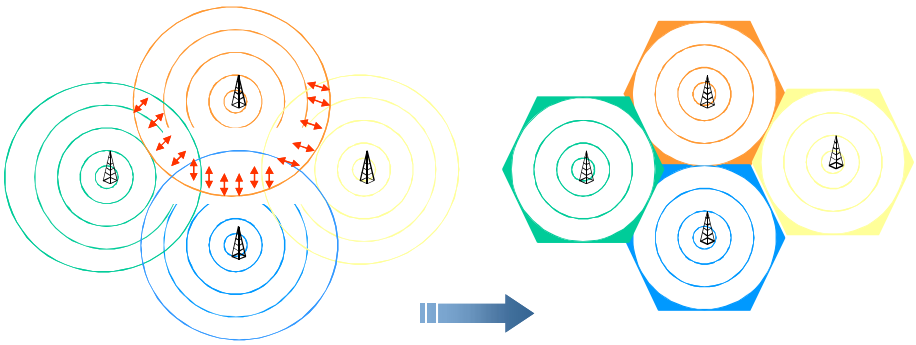
2. Principes de base des réseaux cellulaires

Aspects visibles des réseaux cellulaires – Vue 2



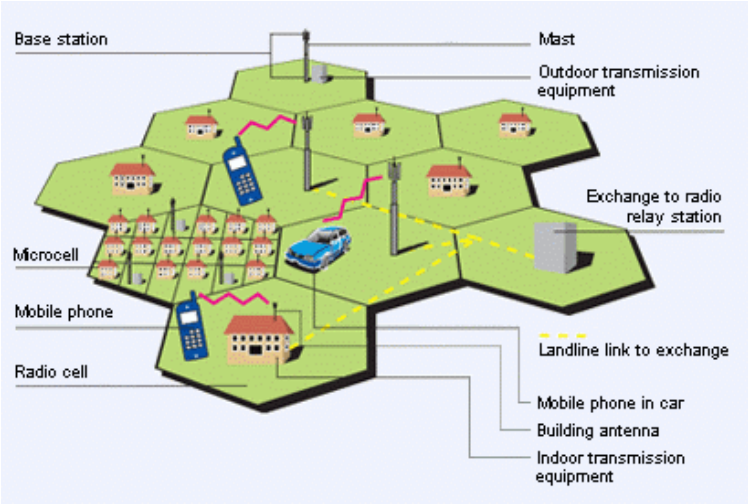
2. Principes de base des réseaux cellulaires

Représentation de cellules (cercle – Hexagone)



2. Principes de base des réseaux cellulaires

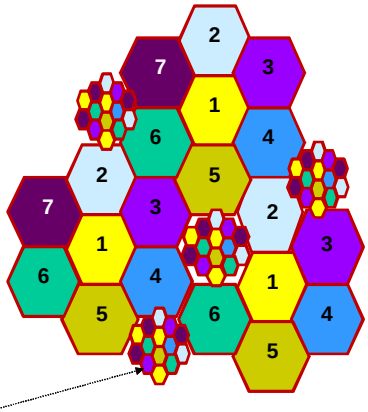
Représentation de cellules en hexagones



2. Principes de base des réseaux cellulaires

Principe de cellule

- Le territoire à couvrir est divisé en cellule
- Réutilisation des fréquences dans des cellules non voisines
- Les sous-ensembles de fréquences sont alloués aux cellules de manière à éviter les interférences entre cellules voisines

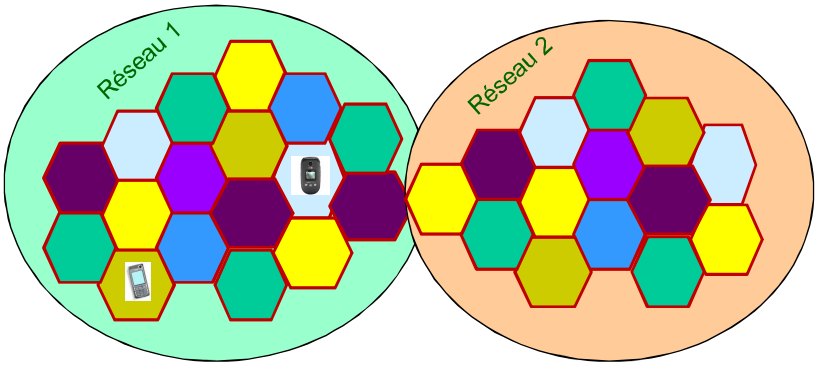


Micro cellules
(zone dense)

2. Principes de base des réseaux cellulaires

Handover ou *Handoff*

- Handoff = poignée de main pour changer de cellule
- Deux types : Handoff horizontal (micro) et vertical (macro)



Micro mobilité

Macro mobilité

2. Principes de base des réseaux cellulaires

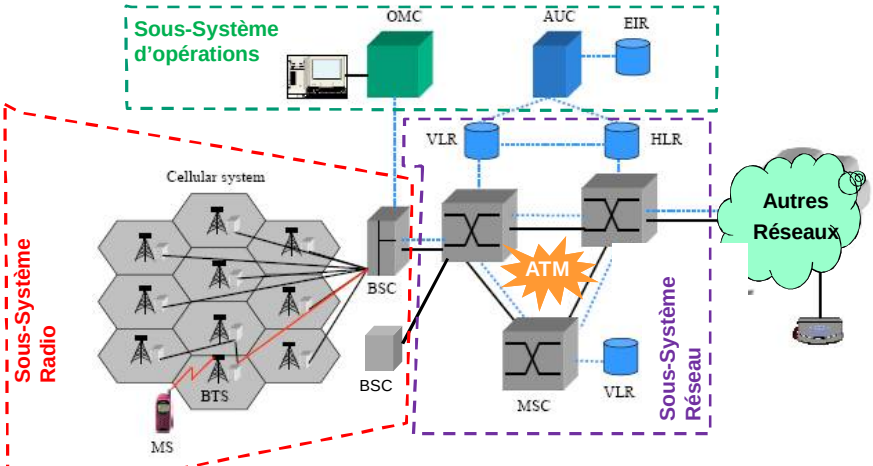
Handover ou *Handoff*

- **Principe**
  - Le mobile mesure la puissance des signaux reçus en provenance des BS qui l'entourent. Il envoie un rapport (périodique) de ses mesures à sa BS.
  - Le handover a lieu quand la puissance reçu d'une autre BS dépasse (pendant un certain temps) celui de sa BS d'enregistrement
- **2 méthodes pour favoriser les handovers par rapport aux appels arrivant**
  - Utilisation de canaux de garde
  - Mise en file d'attente (avec priorité) les demandes de handover

***Roaming* (ou *itinérance*) désigne la capacité des abonnés à accéder à leurs services de téléphonie mobile (voix ou données) depuis des réseaux visités (réseaux de pays étranger).**

3. Réseau GSM

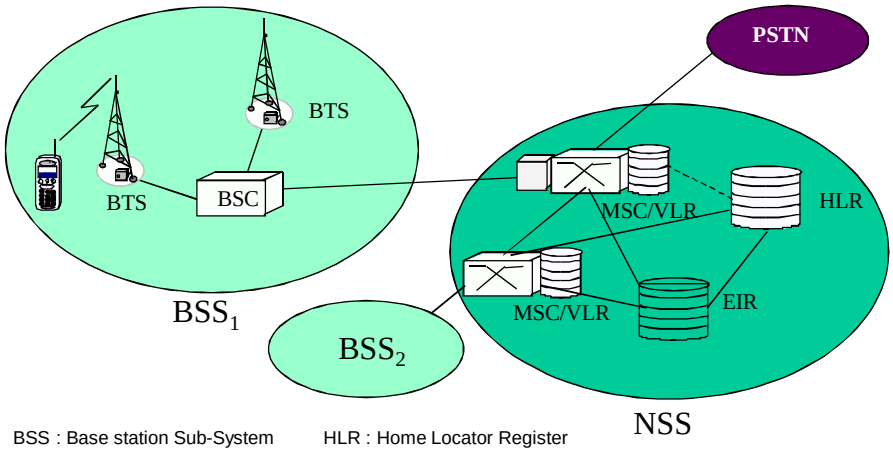
Architecture d'un réseau GSM – Vue 1



BTS : Base Transceiver Station
BSC Base Station Controller
MSC : Mobile Switching Center
GMSC : Gateway MSC HLR Home Location Register
VLR : Visitor Location Register
OMC : Operation and maintenance Center

3. Réseau GSM

Architecture d'un réseau GSM – Vue 2



BSS : Base station Sub-System
NSS : Network Sub-System
HLR : Home Locator Register
EIR : Equipment Identity Register
PSTN : Public Switching Telephone Network

3. Réseau GSM

Architecture d'un réseau GSM – Station mobile (le portable)

- **Fonctions**
  - Accès aux services du réseau
  - Supervision des signaux émis et reçus
  - Affichage de messages
  - Transmission MS/BS : par TDMA-over-FDMA

- **MS = 2 Composants**
  - Equipement possédant son identité internationale **IMEI** (International Mobile Equipement Identity)
  - Carte **SIM** (Subscriber Identity Mobile) contenant :
    - L'identité de l'abonné IMSI (International Mobile Subscriber Identity)
    - La clé Ki (*Individual Subscriber Authencation Key*) servant à l'authentification et au chiffrement de la liaison radio

3. Réseau GSM

Architecture d'un réseau GSM – numéros associés à un mobile et à un abonné

- **IMEI** (*International Mobile Equipement Identity*) identifie l'appareil (permet de bloquer un appareil). Il est composé de 15 chiffres : un code de 8 chiffres donné par l'autorité de certification, un numéro de série codé sur six chiffres et un chiffre de contrôle redondance sur les 14 autres chiffres
- **IMSI** (*International Mobile Subscriber Identity*) : 3 chiffres pour le pays, 2 chiffres pour l'opérateur et 10 chiffres pour l'abonné
- **MSISDN** (*Mobile Station ISDN Number*) : # de téléphone à composer pour appeler le mobile. Ce # n'est pas stocké dans la SIM. La correspondance entre le MSISDN et ISMI n'est connue que par le HLR (sécurité oblige)
- **MSRN** (*Mobile Station Roaming Number*) : numéro utilisé pour router les communications vers un mobile sorti de son réseau (i.e. en cas de *roaming*)

3. Réseau GSM

Architecture d'un réseau GSM – S/système Radio

- **Rôle : distribution du réseau et radiocommunications, gestion de la ressource radio**
- **S/système radio = 1 ou N BTS et 1 ou N BSC**
- **BTS (Base Transceiver Station) ou BS (Base Station)**
  - Communique d'une part avec les MS d'autre part avec la BSC (modulation et démodulation),
  - Transmission du MS vers la BSC sur une liaison MIC (modulation par impulsions codées) en TDMA-over-FDMA
  - Codage de trame et chiffrement
  - Capacité d'environ 72 communications simultanées
  - La puissance émise dépend de la zone à couvrir (puissance réglementée)

3. Réseau GSM

Architecture d'un réseau GSM – S/système Radio

- **BSC (Base Station Controller)**
  - Gestion d'un ensemble de BS
  - C'est l'organe intelligent du S/système radio
  - Allocation des canaux aux MS
  - Codage et décodage de la parole (passer des 64 k/s de la MIC à 13 kb/s par appel)
  - Gestion des handovers entre BS
  - Communication avec le MSC
  - Une BSC gère de 100 à 1000 communications

3. Réseau GSM

Architecture d'un réseau GSM – S/système Réseau

- **Rôle du NSS (Network SubSystem) : commutation et routage**
- **S/système NSS = MSC, VLR, HLR**
- **MSC (Mobile Service Switching)**
  - Gère plusieurs BSC
  - Gère l'interfonctionnement avec d'autres réseaux (filaires ou non) en utilisant une passerelle GMSC (Gateway MSC)
  - Transmission de messages courts
  - Relié au VLR, HLR et EIR
  - Capacité 100 000 abonnés environ

3. Réseau GSM

Architecture d'un réseau GSM – S/système Réseau

- **HLR (Home Location Register)**
  - Il contient les infos nécessaires à la gestion des communications d'abonnés
  - Un HLR peut être associé à une région, un pays, un opérateur…
  - Pour chaque abonné, la base de données du HLR contient :
    - identité internationale de l'abonné (IMSI),
    - son numéro d'abonné MSISDN
    - services souscrits (*roaming*…)
    - position actuelle (VLR/MSC auquel est enregistré actuellement le mobile)
    - paramètres pour l'authentification et chiffrement

3. Réseau GSM

Architecture d'un réseau GSM – S/système Réseau

- **VLR (Visitors Location Register)**
  - Base de données associée au MSC
  - Contient une partie des infos des HLR concernant les abonnés situés dans les BS dépendant du MSC
  - Le VLR enregistre les infos de localisation des mobiles
  - Le VLR détermine les numéros de réacheminement MSRN (*Mobile Station Roaming Number*) pour les communications à destination des mobiles.
  - Les informations enregistrées par un VLR sont effacées lorsque le mobile quitte la zone de ce VLR

3. Réseau GSM

Architecture d'un réseau GSM – S/système d'opérations

- **AUC (AUthentication Center)**
  - Un centre d'authentification AUC (*Authentication Center*) est associé au HLR. Il contient la clé d'authentification Ki unique de l'abonné et génère les valeurs de paramètres utilisés pour l'authentification et le chiffrement.
- **EIR (Equipment Identity Register)**
  - Base de données contenant le numéro international de l'équipement IMEI (*International Mobile Equipement Identity*) permettant ainsi son identification
- **OMC (Operation Maintenance Center)**
  - Gestion d'alarmes, de configurations
  - Gestion de performances, statistiques
  - Autres fonctions de gestion

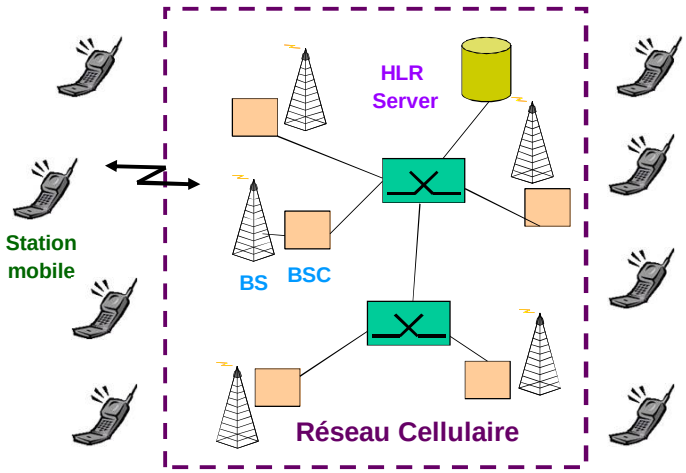
3. Réseau GSM

Phases d'un appel mobile vers mobile

- Supervision de la puissance de signal par le mobile
- Requête de connexion (appel)
- Localisation de l'appelé (*Paging*)
- Appel accepté
- Appel en cours : conversation
- Fin d'appel ou *Handoff*

3. Réseau GSM

Phases d'un appel mobile - Illustration



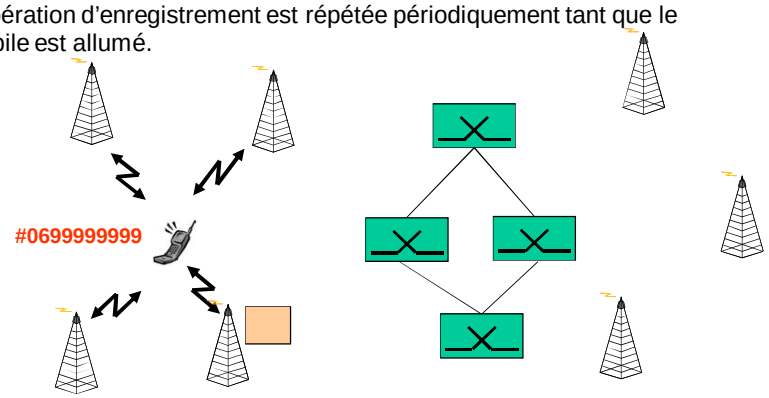
⇨ ⇨ ⇨ ⇨ **On considère le cas simple : une BS par BSC**

3. Réseau GSM

Phases d'un appel mobile – Illustration

Phase enregistrement de mobile

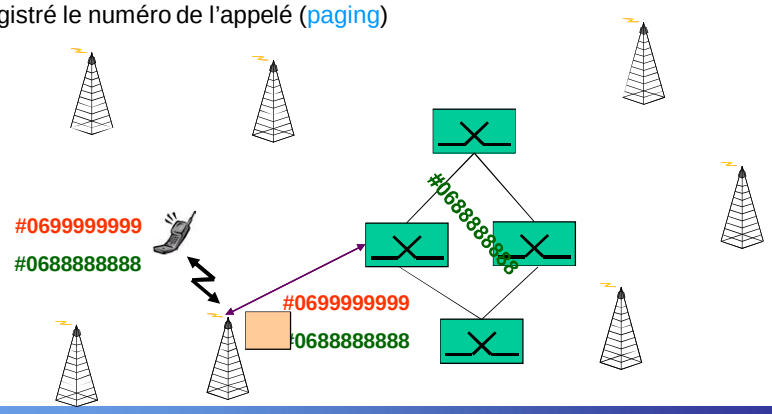
- Une fois allumé, le mobile s'enregistre auprès de la BS y dont le signal est le plus fort. L'enregistrement est effectuée au niveau de la BSC associée à la BS y. Le VLR du MSC est mis à jour.
- L'opération d'enregistrement est répétée périodiquement tant que le mobile est allumé.



3. Réseau GSM

Phases d'un appel mobile – Illustration
Phase Appel d'un numéro

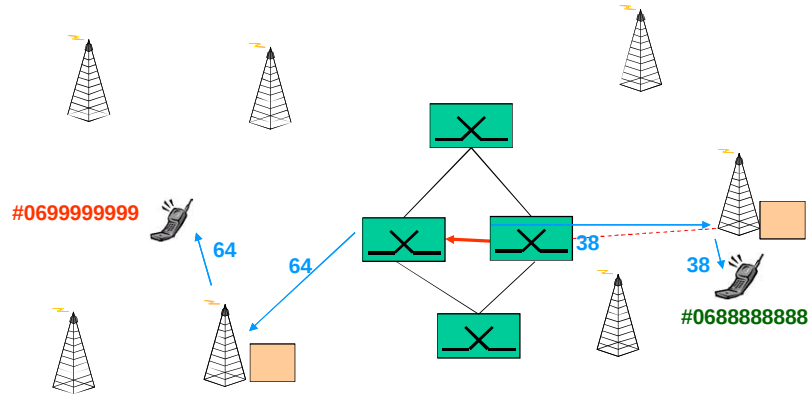
- Le mobile compose le # de l'appelé qui est transmis à sa BS, puis au BSC.
- Le BSC transmet les deux numéros au MSC.
- Le MSC lance une recherche pour savoir auprès de quelle BSC est enregistré le numéro de l'appelé (paging)



3. Réseau GSM

Phases d'un appel mobile – Illustration
Phase Appel d'un numéro

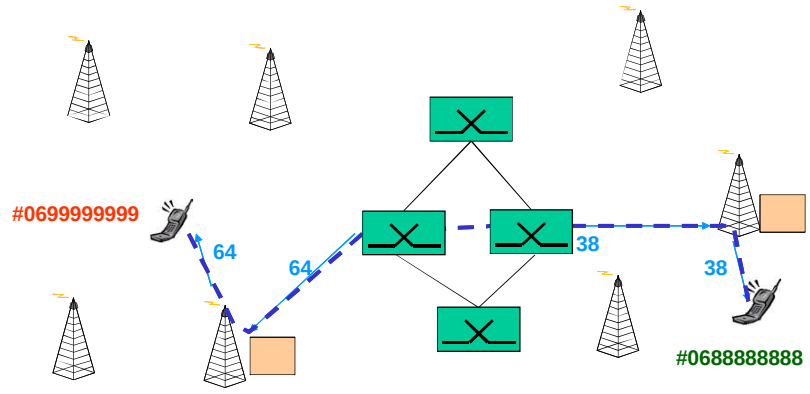
- Le MSC d'enregistrement du numéro de l'appelé répond.
- Les MSC se mettent d'accord sur l'affectation des canaux pour la communication entre appelé et appelant



3. Réseau GSM

Phases d'un appel mobile – Illustration
Phase Conversation

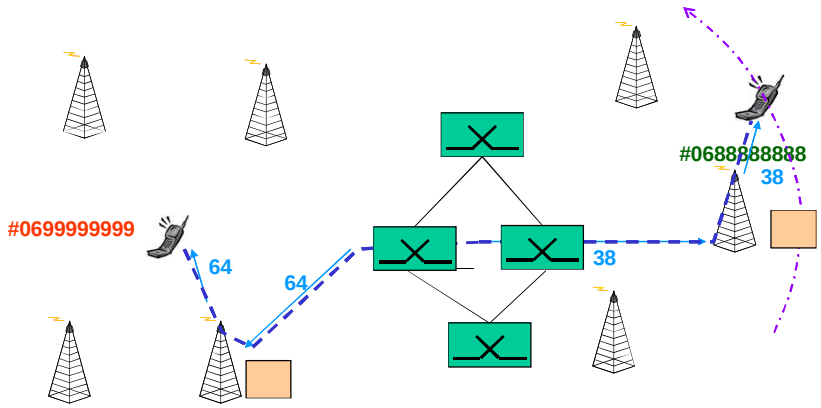
- Les deux correspondent conversent pendant un certain temps



3. Réseau GSM

Phases d'un appel mobile – Illustration
Phase Handover

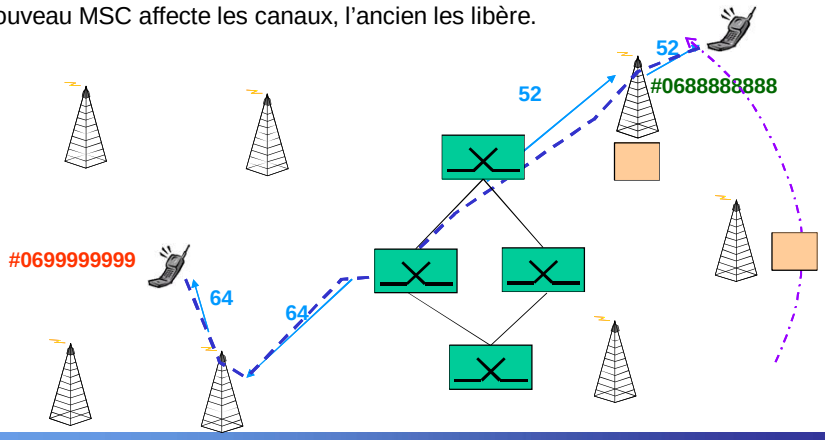
- L'appelé se déplace. Le BSC vers lequel le mobile se déplace est averti.
- Dès que le mobile se trouve dans la zone du nouveau BSC, le *handover* a lieu.



3. Réseau GSM

Phases d'un appel mobile – Illustration
Phase Handover

- Le nouveau BSC prépare le relais. Il communique avec le MSC et lui donne le numéro du mobile qui est en train de pénétrer dans sa zone.
- Le nouveau MSC affecte les canaux, l'ancien les libère.



3. Réseau GSM

Phases d'appel fixe vers un mobile GSM

1. PSTN subscriber keys the MSISDN, (MS telephone number). MSISDN is analyzed in the local exchange in PSTN, which realizes that this is a call to a subscriber in a GSM network. A connection is set up to the GMSC (Gateway MSC).
2. GMSC analyses MSISDN to find out in which HLR the MS is registered, and interrogates the HLR for information about how to route the call to the serving MSC/VLR.
3. HLR translates MSISDN into IMSI, and finds out which MSC/VLR is currently serving the MS. HLR also checks the service, "Call forwarding to C–number". If the service is active the call is rerouted by the GMSC to that number, probably via PSTN.
4. HLR requests a roaming number, MSRN (Mobile Station Roaming Number), from the serving MSC/VLR. MSRN identifies the MSC/VLR.
5. MSC/VLR returns the MSRN via HLR to the GMSC.
6. GMSC reroutes the call to the MSC/VLR, directly or via the PSTN.
7. The MSC/VLR knows in which Location area, LA, the MS is. A Paging message is sent to the BSCs controlling the LA. (The information on which cells belong to which LA is stored in the BSC, but according to the GSM specification it can as well be stored in the MSC).
8. The BSCs distribute the Paging message to the BTSs in the wanted LA. The BTSs transmit the message over the air interface using PCH (Paging channel). To page the MS, IMSI (International Mobile Subscriber Identity) or TMSI (Temporary Mobile Subscriber Identity, valid only in the current MSC/VLR service area) is used.
9. When the MS detects the paging message it sends a request for a signalling channel, SDCCH.
10. BSC provides a SDCCH, using AGCH.
11. SDCCH is used for the call set up procedures, as in the case for "Call from MS", and then a TCH is allocated. SDCCH is released.
The mobile phone rings, and when the subscriber answers the connection is completed.

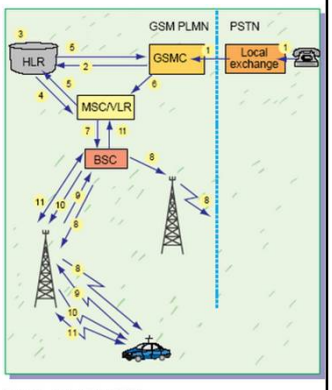
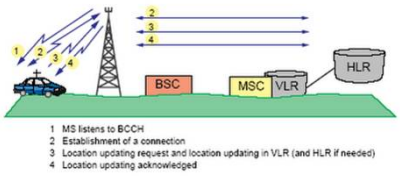


Figure 91 Call to MS from PSTN

3. Réseau GSM

Phases de changement de localisation de mobile



1 MS listens to BCCH
2 Establishment of a connection
3 Location updating request and location updating in VLR (and HLR if needed)
4 Location updating acknowledged

Figure 87 Location updating type normal

1. MS listens to BCCH (Broadcast Control Channel) in the new cell to find out the Location Area Identity, LAI. The new LAI is compared to the old one. If they differ an update of the location needs to take place.
2. MS establishes a connection with the GSM/PLMN via SDCCH (Stand-alone Dedicated Control Channel). Authentication is then performed (with the help of HLR if the MS is unknown in the MSC/VLR).
3. MS sends a Location Updating Request to the system, if the authentication was successful. If the new LA belongs to a new MSC/VLR the HLR will also be updated.
4. Location Updating is acknowledged by the system, and BTS and MS are requested to release the signalling channel.

4. Réseau GPRS

Apports du Réseau GPRS

- Le plus par rapport au GSM : la commutation de paquet.
- Objectifs : échange de données et surtout accès à Internet en bas débit

- En fonction des configurations
  - @ 14.4 kb/s par canal (soit 115.2 kb/s sur 8 canaux simultanés)
  - @ 21.4 kb/s par canal (soit 171.2 kb/s sur 8 canaux simultanés)
- Jusqu'à 8 abonnés par canal (c'est peu !)
- Facturation en fonction de la quantité de données et non du temps de connexion !

GPRS : un petit pas du monde de la téléphonie mobile vers Internet

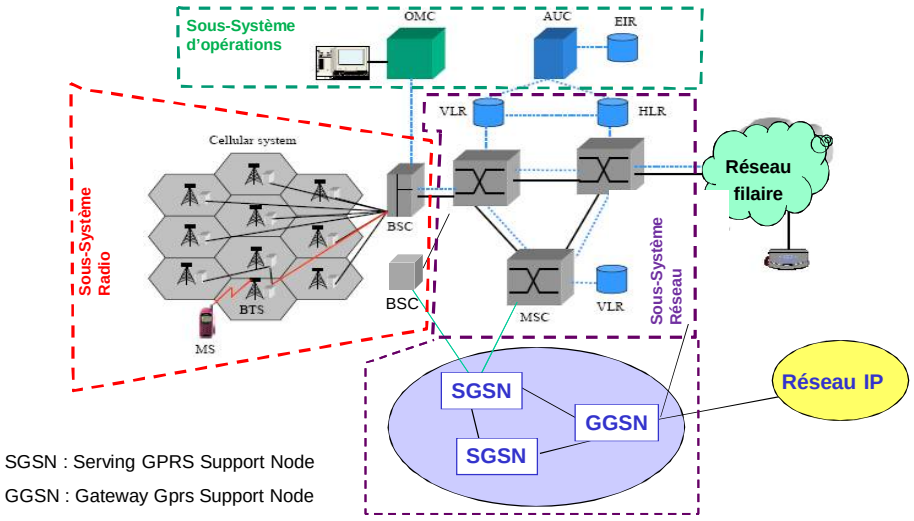
4. Réseau GPRS

Fonctionnalités rajoutées au GSM

- Au niveau du mobile
  - Cohabitation du mode commutation de circuit avec le mode commutation de paquet
  - Fonctionnement en parallèle ou en alternance selon le type de mobile:
    - Mobile de type A : GSM et GPRS en même temps
    - Mobile de type B : GSM ou GPRS (en alternance)
    - Mobile de type C : GSM ou GPRS *a priori*
  - Applications nouvelles pour accéder à Internet
- Au niveau Réseau
  - Implantation de nœuds spéciaux pour gérer le trafic Paquets (SGSN et GGSN)
  - Ajout d'attributs au HLR (liés aux accès Internet)

4. Réseau GPRS

Intégration du GPRS au GSM – Vue 1

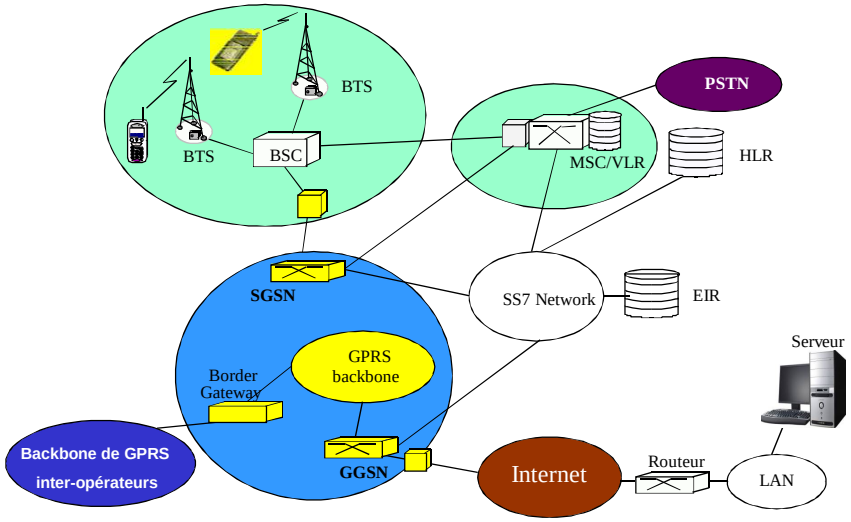


SGSN : Serving GPRS Support Node

GGSN : Gateway Gprs Support Node

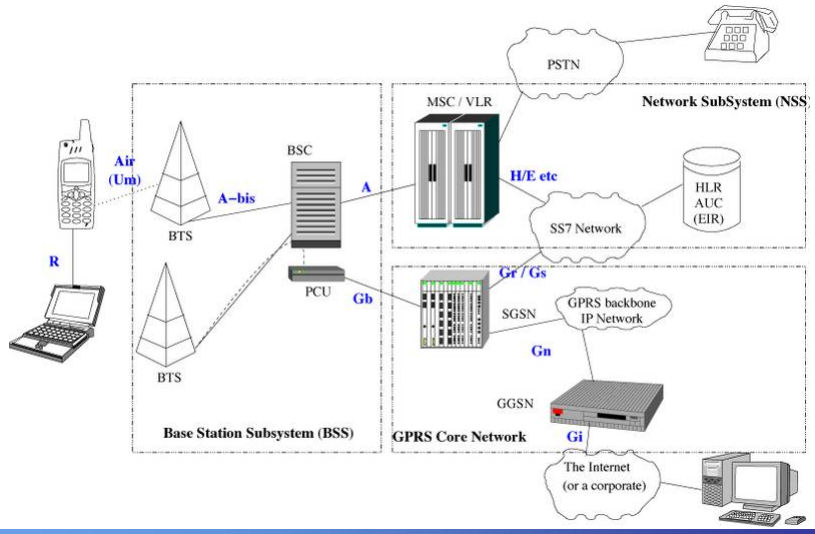
4. Réseau GPRS

Intégration du GPRS au GSM – Vue 2



4. Réseau GPRS

Intégration du GPRS au GSM – Vue 3



4. Réseau GPRS

Rôles des SGSN et GGSN

- **SGSN** (Servicing GPRS Support Node)
  - Gestion des paquets liés à une zone géographique
  - Gestion des utilisateurs GPRS
  - Gestion de la sécurité et contrôle d'accès
  - Équivalent au MSC mais pour les communications en mode paquet
- **GGSN** (Gateway GPRS Support Node)
  - Interopérabilité avec Internet
  - Routage de paquets vers les SGSN en fonction des zones de destination
  - Gestion de sécurité
  - Gestion de la localisation des mobiles
  - Gestion des handovers
  - Facturation…

4. Réseau UMTS

IMT-2000, UMTS, 3G

- **Trois sigles pour la même chose**
  - IMT-2000 (*International Mobile Telecommunication*) terme utilisé par l'ITU-T pour la normalisation
  - UMTS (*Universal Mobile Telecommunications System*) : terme utilisé par les opérateurs les fora 3GPP et 3GPP2
  - 3G (*Third generation*) : terme utilisé par les utilisateurs et grand public

Débits du GSM, GPRS… : trop faibles pour les besoins des applications multimédia mobiles dans Internet ➔ Besoin d'une nouvelle technologie

- **Exigences pour l'IMT-2000 (élaborées par l'ITU-T)**
  - 2 Mb/s pour les abonnés immobiles ou à l'intérieur des bâtiments
  - 384 kb/s pour les piétons et mobiles en zones urbaines
  - 144 kb/s pour les usagers se déplaçant à vitesse élevée (<= 500 km/h)
  - Débits variables pour les zones très vastes (irriguées par satellite)

5. Réseau UMTS

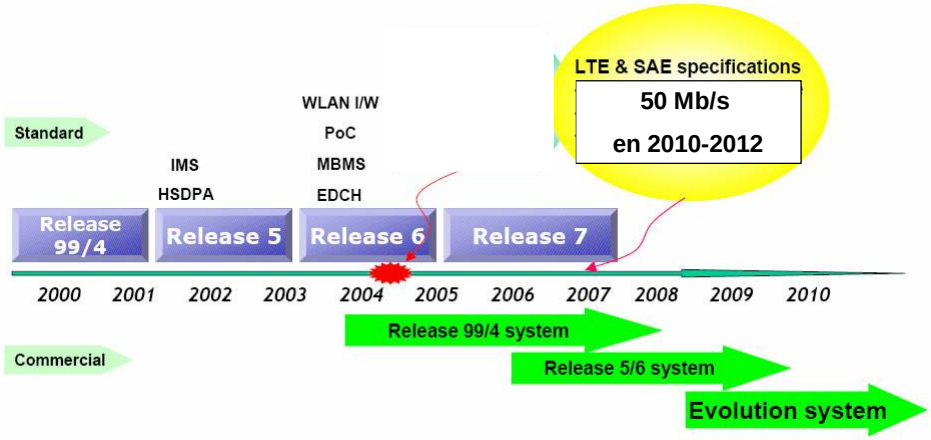
Apports de l'UMTS

- **Les plus de l'UMTS**
  - Offrir une qualité de voix et vidéo similaire aux réseaux fixes : Taux d'erreur entre 10^{-3} et 10^{-6} et délai entre 30 et 300 ms
  - Améliorer la sécurité par rapport au GSM et GPRS
  - Permettre le développement de nouveaux services (nouveaux business)
  - Permettre la couverture de zones isolées (via des connexions satellites ou WiMax)

Spectre de fréquences de l'UMTS : 1885-2025 MHz et 2110-2200 MHz.

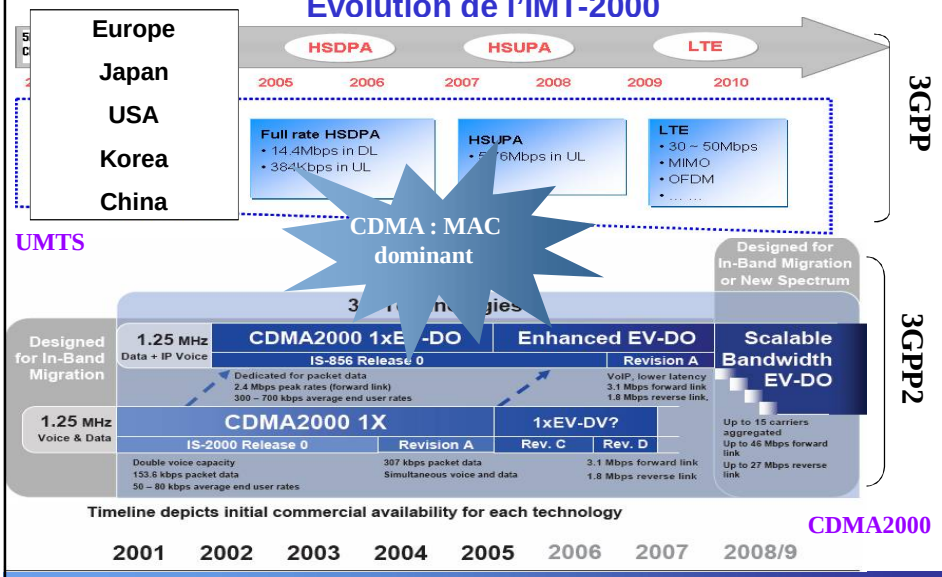
5. Réseau UMTS

Evolution du standard UMTS



5. Réseau UMTS

Evolution de l'IMT-2000



5. Réseau UMTS

Evolution des services de l'UMTS

Release	*Services*
R99 (2000)	MMS, streaming, LCS , MExE, Satellite
R4 (2001)	TrFO, VHE, OSA,
R5 (2002)	VoD, IMS, HSDPA, Wideband AMR, GTT
R6 (2003)	MBMS, IMS phase 2
Rxx (2006 - 2009	HSUPA, LTE

GTT : Global Text Telephony
HSUPA (High Speed Uplink Packet Access)
LCS : location based services
MExE : Mobile Execution Environment
OSA : Open Service Access
CAMEL : Customised Application For Mobile Network Enhanced Logic
VHE : Virtual Home Environment
HSDPA : *High Speed Downlink Packet Access*
IMS : IP Multimedia Subsystem
LTE : Last Term Evolution
MBMS : Multimedia Broadcast Multicast Service
TfFO : Transcoder Free Operation

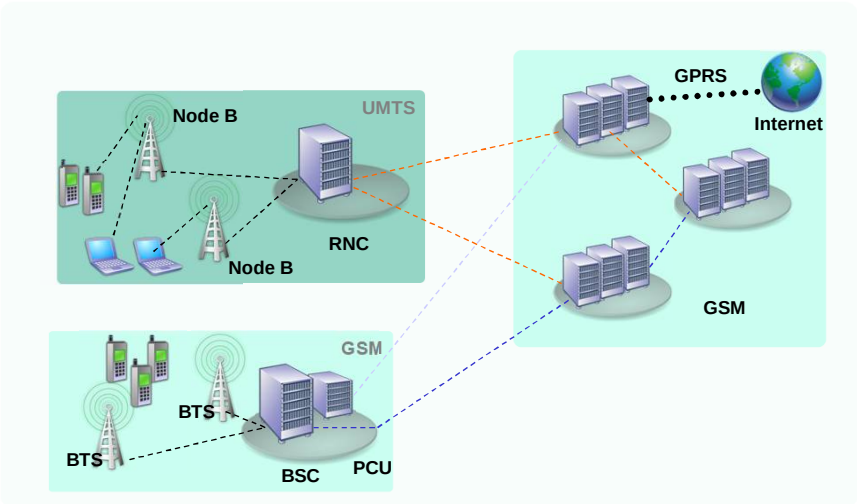
5. Réseau UMTS

Classes de service de l'UMTS

Classe de trafic	Conversationnel	Streaming	Interactif	Background
Caracteri-stiques	Préserver les relations temporelles entre les entités du flux Délai très courts	Préserver les relations temporelles entre les entités du flux Taux d'erreurs faible	Modèle de requête/réponse Taux d'erreurs nul	Aucune contrainte de temps Taux d'erreurs nul
Exemples d'applications	Téléphonie, Vidéo téléphonie, Jeux vidéo	Streaming multimédia	Web browsing, Jeux en réseau	Télécharge-ment, emails

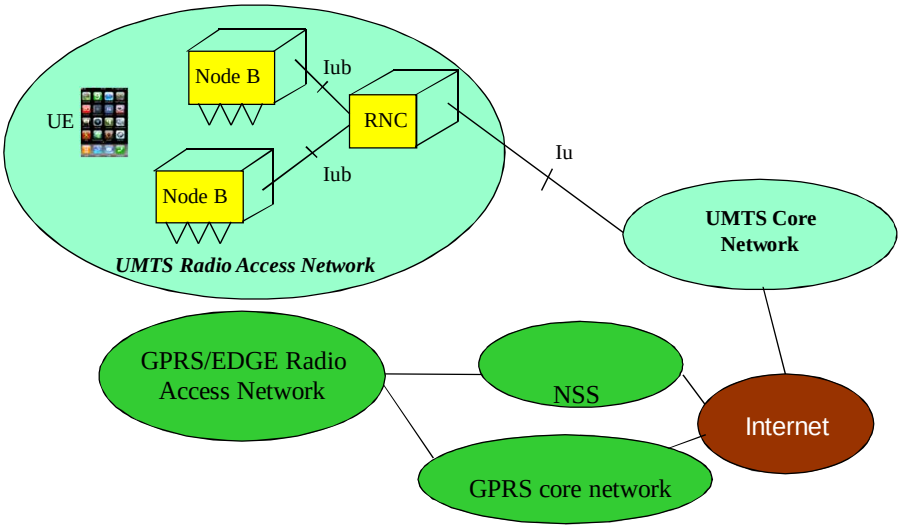
5. Réseau UMTS

Cohabitation 2G, 2.5G et 3G



5. Réseau UMTS

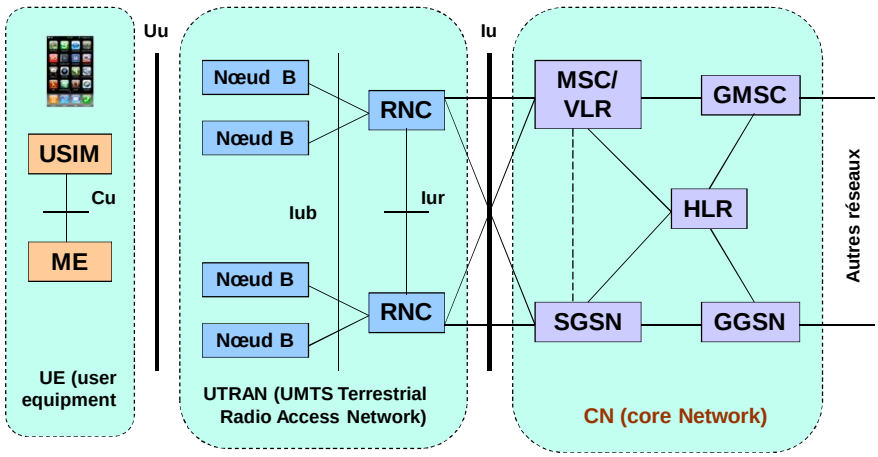
Architecture générale de l'UMTS



5. Réseau UMTS

Architecture général de l'UMTS

- UMTS = 3 parties (UE + UTRAN + CN)



5. Réseau UMTS

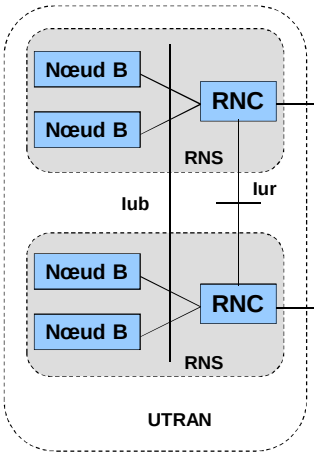
Partie UE (user equipment) de l'UMTS

- UE assure les fonctions suivantes
  - Support d'appel d'urgence sans USIM
  - IMEI (Id de l'équipement)
  - Mise à jour de la position du mobile
  - Gestion de services connectés ou non connectés
  - Algorithmes d'authentification et cryptage
  - Services et applications spécifiques à l'utilisateur

5. Réseau UMTS

Partie UTRAN de l'UMTS

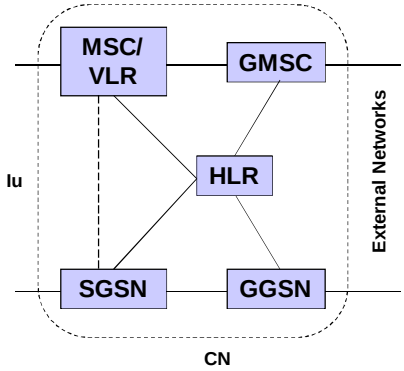
- Rôle : gestion de la ressource radio
- Equivalant du BSS du GSM
- Structure
  - UTRAN = 1 ou plusieurs RNS
  - RNS (Radio Network Subsystem) = 1 ou n Nœud B + 1 RNC
  - RNC : Radio Network Controller
  - Nœud B = Station de base



5. Réseau UMTS

Partie *Core Network* de l'UMTS

- Rôle : gestion des utilisateurs et de l'interopérabilité avec Intenet
- Equivalant du NSS du GSM

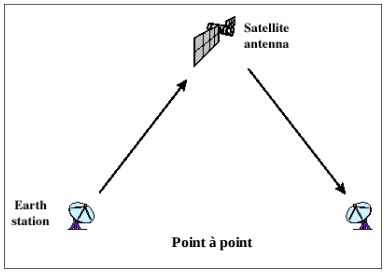


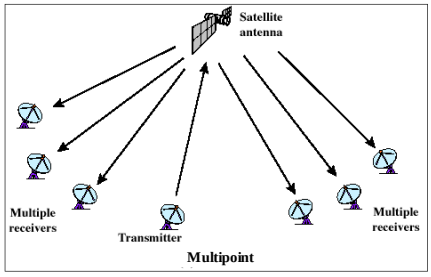
5. Réseaux de satellites

5. Réseaux de satellites

Principe général des liaisons satellitaires

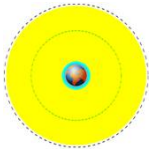
- Domaines d'utilisation : TV, Radio, téléphone longue distance, Navigation, accès Internet, réseau privé d'entreprise
- Stations terrestres munies d'antennes (sources et destinations de données)
- Un satellite avec deux types de liaisons : montantes et descendantes
- Les liaisons descendantes en point à point (téléphone) ou multipoint (TV)
- Transpondeur : conversion de signal montant en signal descendant



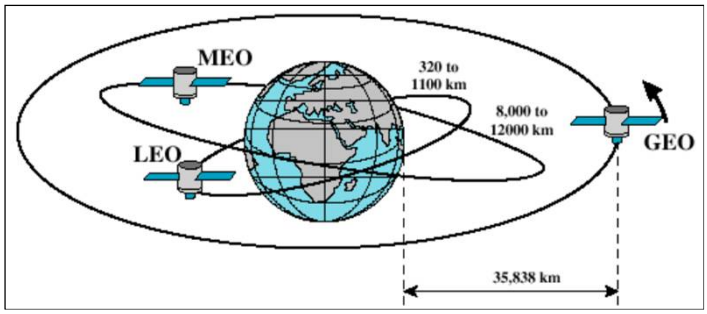


5. Réseaux de satellites

Orbites de satellitaire



- Satellites géostationnaires
- Satellites à orbites moyennes (MEO : *Medium earth orbiting*)
- Satellites à faibles orbites (LEO : *Low earth orbiting*)



5. Réseaux de satellites

Satellites géostationnaires

- Orbite à 35 838 Km
- Tourne au même rythme que la terre au niveau de l'équateur
- Avantages
  - Pas de changement de fréquences (puisque la position est fixe par rapport à la terre)
  - Le suivi du satellite par les stations au sol est simplifié
  - Un satellites peut irriguer ¼ de la terre. Trois satellites séparés de 120° couvrent la plus part des zones inhabitées
- Inconvénients
  - Coûts (satellite et mise en orbite) très élevé
  - En général des liaisons point-à-point
  - Zones polaires mal desservies
  - Délai de propagation élevé (aller-retour de l'ordre de 0.5 s → problème pour la voix)
  - Puissance de transmission très élevée

5. Réseaux de satellites

Satellites MEO

- Orbites plus de 5000 km et moins de 12000 km
- Période de rotation du stellite : environ 6 heures
- Diamètre de couverture : 10000 à 150000 km
- Délai de réponse (aller-retour) < 50 ms
- Durée de visibilité du satellite à partir d'un point fixe : quelques heures
- Avantages/inconvénients : compromis entre GEO et LEO

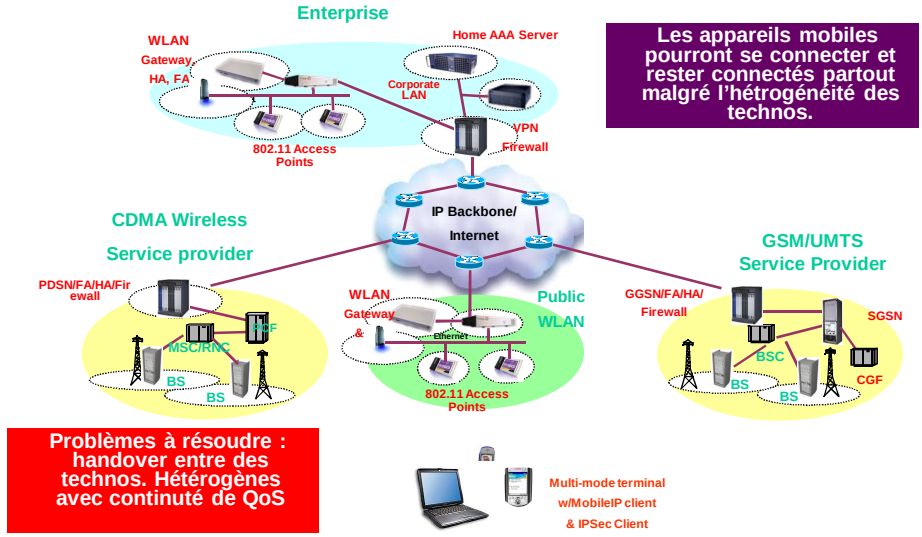
5. Réseaux de satellites

Satellites LEO

- Orbites : plus de 320 km et moins de 2000 Km
- Période de rotation du satellite : 1.5 à 2 heures
- Diamètre de couverture max : 8000 Km
- Avantages
  - Temps de réponse court (inférieur à 20 ms)
  - Signal reçu puissant
- Inconvénients
  - Beaucoup de satellites sont nécessaires pour couvrir des zones importantes 24 sur 24 (un satellite est visible pour un point fixe pendant 20 min)
  - Changements fréquents de fréquences

6. Conclusion

Futur de la mobilité



Les appareils mobiles pourront se connecter et rester connectés partout malgré l'hétrogénéité des technos.

Problèmes à résoudre : handover entre des technos. Hétérogènes avec continuté de QoS

6. Conclusion

Récapitulatif des réseaux sans fils

	DébIT (Mb/s)	Portée (mètres)	Mobilité de l'utilisateur	Fréquence (GHz)
Bluetooth	1 Mb/s	10 mètres	Très faible (dans une salle)	2.4 GHz
UWB	50 Mb/s	<10 mètres	Très faible (dans une sale)	7.5 GHz
Wifi 802.11a	≤ 54 Mb/s	<50 mètres	Faible (dans un bâtiment)	5 GHz
IEEE 802.11b	11 Mb/s	100 mètres	Faible (dans un bâtiment)	2.4 GHz
IEEE 802.11g	≤ 54 Mb/s	100 mètres	Faible (dans un bâtiment)	2.4 GHz
GSM	9.6 Kb/s	10 à 20 km	Moyenne à élevée (conduire en voiture)	900 MHz
3G	≤ 2 Mb/s	5 à 10 km	Élevée (conduire en voiture)	De 1 GHz à 2 GHz
FSO	De 100 Mb/s à 2.5 Gb/s	1 to 2 kilomètres	Aucune (fixe, antennes sur les immeubles)	Terahertz
Satellites	64 Kb/s	Des milliers de Km	Aucune	3 à 30 GHz

6. Conclusion

Principales différences entre 2G et 3G

	W-CDMA	GSM
Carrier spacing	5 MHz	200 kHz
Frequency reuse factor	1	1-18 (tipically 9)
Rate of Power Control	1500 Hz	2 Hz or smaller
QoS	Radio resources management algorithms	Frequencial Network Planning
Frequency Diversity	The 5 MHz bandwidth allows the exploitation of multipath with *Rake* receivers	Frequency Hopping
Packet Data	Traffic-dependent scheduling of packet transmission	In the GPRS the packet scheduling depends on *time slot*

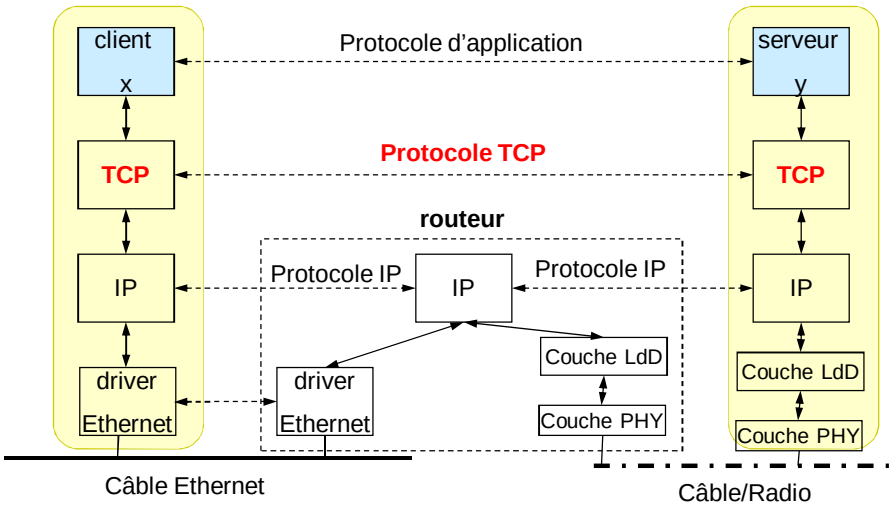
Chapitre 8

Protocole TCP

(Transmission Control Protocol)

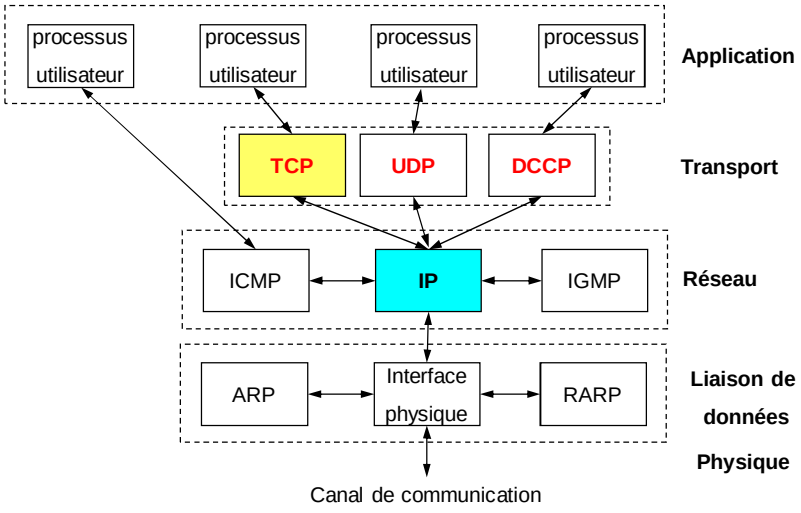
1. Généralités

Architecture TCP/IP



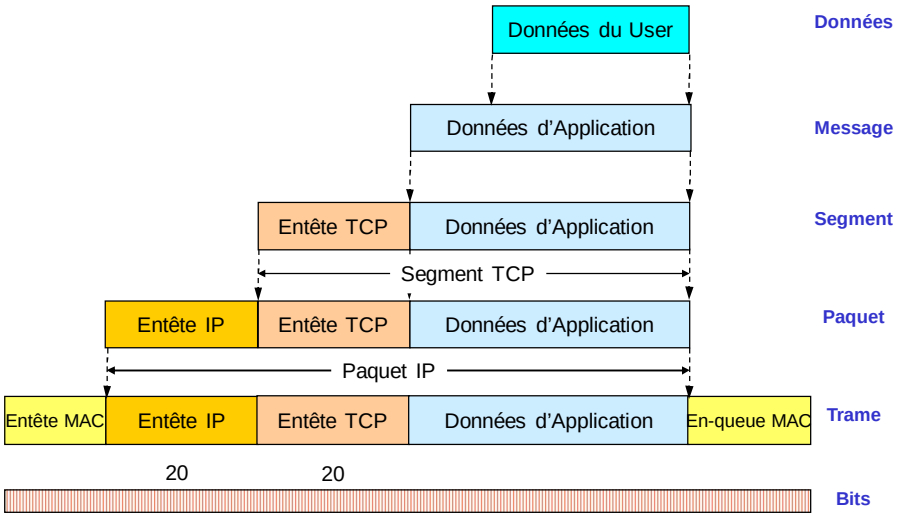
1. Généralités

Architecture TCP/IP



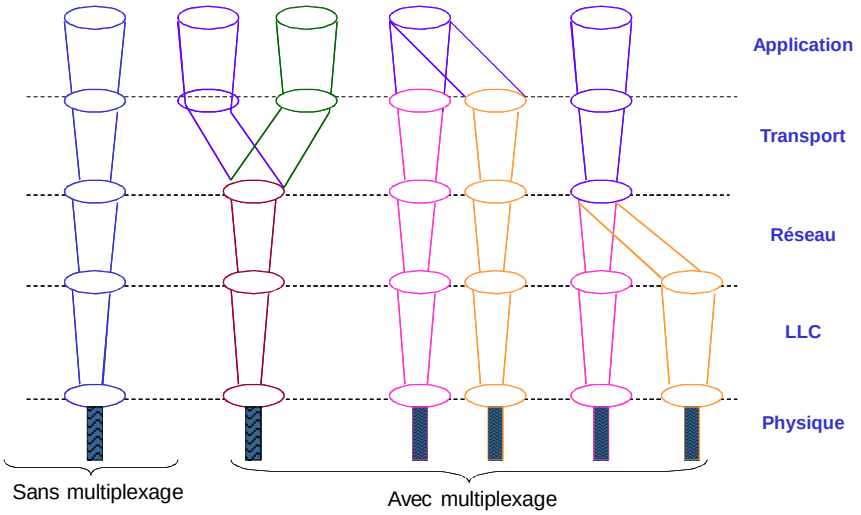
1. Généralités

Encapsulation



1. Généralités

Multiplexage (contexte général)



1. Généralités

Fonctions relevant du niveau Transport

- **Transport de bout en bout** de messages
- **Fragmentation/réassemblage** de messages
- **Contrôle d'erreurs (perte de segments, erreur d'entête TCP)**
- **Contrôle de flux (contrôle aux extrémités)**
- **Contrôle congestion (contrôle à l'intérieur du réseau)**
- **Séquencement de** de paquets et livraison ordonnée de messages
- **Multiplexage** de connexion
- **Sécurité** (si les niveaux inférieurs ne sont pas sécurisés)

1. Généralités

Protocoles de transport et QoS

- **Paramètres de QoS**
  - Temps d'établissement de connexion
  - Probabilité d'échec de connexion
  - Débit de la connexion
  - Temps de transit de bout en bout
  - Taux d'erreurs
  - Sécurisation de la connexion
  - Priorité pour les données urgentes ou critiques
  - Probabilité de résiliation de connexion par le provider
- **QoS : non gérée actuellement par TCP, UDP…**

1. Généralités

Protocoles de transport OSI

- **OSI a défini 5 classes de TP (Transport Protocol)**
  - TP0 : Pas de multiplexage, Pas de reprise sur erreurs
  - TP1 : Pas de multiplexage, Reprise sur erreurs signalées par le niveau Réseau
  - TP2 : Multiplexage, Avec ou sans contrôle de congestion, Pas de reprise sur erreurs
  - TP3 : Multiplexage, Avec ou sans contrôle de congestion, Reprise sur erreurs signalées
  - TP4 : Multiplexage, Avec ou sans contrôle de congestion, Reprise sur erreurs signalées et non signalées
- **TP classe 0 : adapté aux réseaux fiables**
- **TP classe 4 : adapté aux réseaux non fiables (ex. IP)**

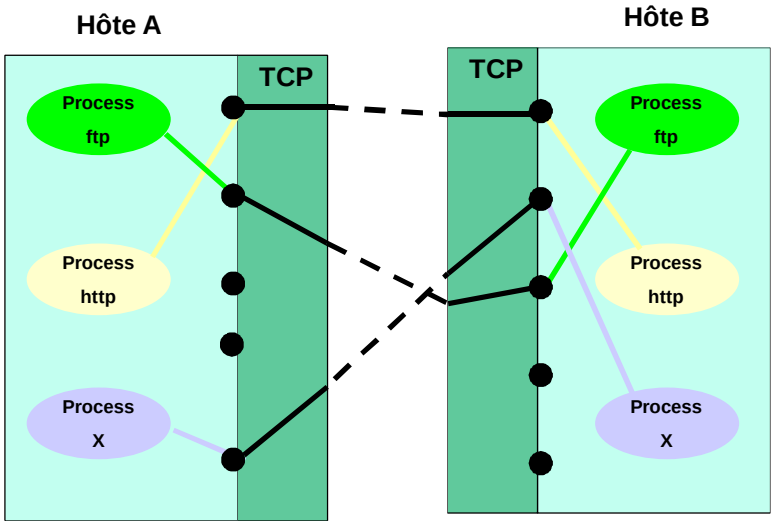
1. Généralités

Protocoles de transport TCP/IP

- ***UDP*** *(User Datagram Protocol)* **~ TP classe 0**
  - Défini en 1980 (RFC 768)
  - Très simple : aucun contrôle d'erreurs ou de congestion
  - Adapté aux réseaux fiables ou bien si la fiabilité n'est pas requise
  - Agressif pour le réseau (peu recommandé en général)
- ***TCP*** *(Transmission Control Protocol)* **~ TP classe 4**
  - Défini en 1981 (RFC 793)
  - Complexe : connexions fiables, contrôle de flux, contrôle de congestion
  - Adapté aux réseaux non fiables
  - Très adaptatif (très recommandé en général)
- ***DCCP*** *(Datagram Congestion Control Protocol)* **~ TP classe 2**
  - Défini en 2006 (RFC 4336)
  - Complexité moyenne : connexions non fiables, avec contrôle de congestion
  - Corrige le principal défaut de UDP (l'agressivité)

1. Généralités

Concept de *Port* TCP



1. Généralités

Concept de *Port* TCP

- Port : « guichet » d'accès aux services applicatifs
- Quadruplet < #Port source, #Port destination, @IP source, @IP destination >
  ➔ identification sans ambiguïté des flux
- (#Port, @IP) = Socket
- (Socket_source, Socket_Destination) = connexion TCP

- Numéros de port codés sur 16 bits ➔ 64 k ports
- Ports réservés (*ftp*, *http*,…) : numéros inférieurs à 1024,
- Ports libres (attention à la sécurité sur ces ports)

1. Généralités

Concept de *Port* TCP

- **Pourquoi utiliser des ports ?**
  - Classer les applications par catégorie
  - Allocation et gestion de ressources (CPU, mémoire, nombre de threads…)
  - Sécurité :
    - Contrôler ou interdire les accès sur certains ports
    - Reconnaître les flux (http, ftp…) et détecter les intrusions

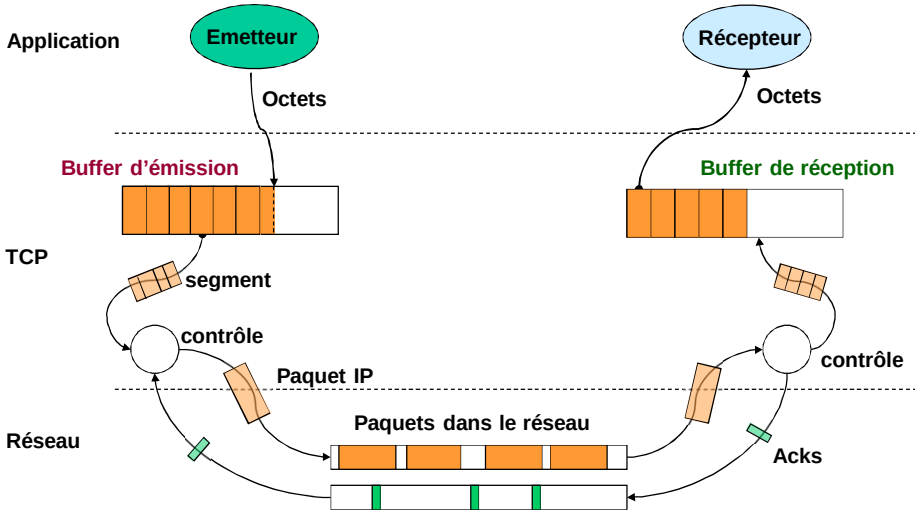
1. Généralités

Principe général de traitement des messages par TCP

- TCP découpe en segments les données applicatives à envoyer.
- A l'émission d'un segment, TCP-émetteur enclenche un temporisateur et attend que l'autre extrémité ait acquitté la réception du segment. Si l'acquittement n'est pas reçu avant épuisement du temporisateur, le segment est retransmis.
- A la réception d'un segment, TCP-récepteur envoie ou non un acquittement (on acquitte au moins toutes les x unités de temps)
- TCP-récepteur remet dans l'ordre les données reçues (si nécessaire) avant de les passer à l'application
- TCP-récepteur rejette les segments dupliqués
- TCP réalise du contrôle de flux et du contrôle de congestion

1. Généralités

Buffers de TCP



1. Généralités

Flot vs Message

- **Mode flot (*bit stream*)**
  - Mode de TCP
  - Il n'y a pas de frontière entre les bits générés par l'application source.
  - La source dépose en 'continu' ou non des flots de bits dans le buffer TCP
  - TCP extrait un certain nombre de bits consécutifs pour former un segment et l'envoie
- **Mode message**
  - Mode de UDP
  - A chaque message de l'application correspond un segment UDP.
  - La source dépose ses messages un par un dans le buffer UDP
  - UDP extrait les segment un par un et les envoie.

1. Généralités

Interface TCP (interface sockets)

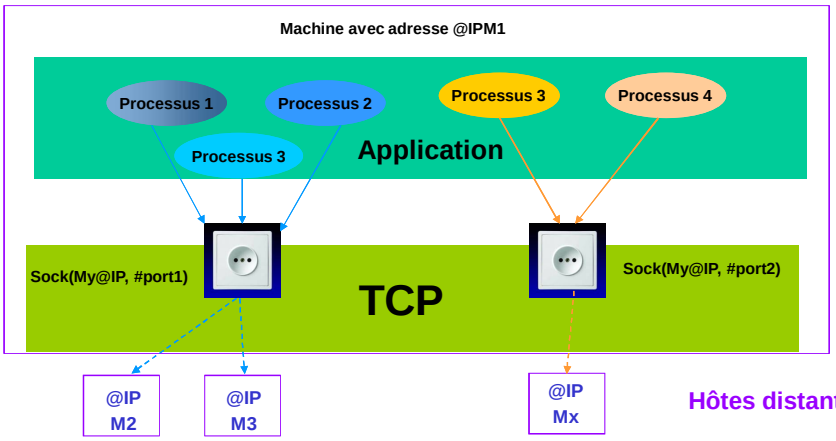
- **OPEN** (local port, socket distante, mode actif/passif, ...) → nom local de connexion
- **SEND** (nom local de connexion, adresse de buffer, nombre d'octets, indicateur d'urgence, timeout...)
- **RECEIVE** (nom local de connexion, adresse de buffer, nombre d'octets) → nombre d'octets, indicateur d'urgence
- **CLOSE** (nom local de connexion)
- **STATUS** (nom local de connexion) → Infos d'état
- **ABORT** (nom local de connexion)

Toute la complexité de TCP est cachée aux applications. Elle apparaît uniquement quand on s'intéresse aux performances.

1. Généralités

Multiplexage selon TCP

- **Objectif :**
  Permettre à plusieurs processus d'applications de partager une socket.



1. Généralités

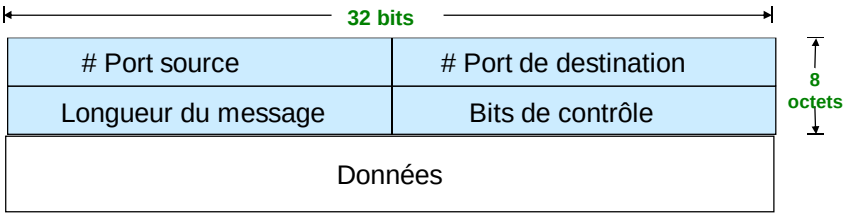
Exemple de multiplexage avec TCP

- **Sans multiplexage de connexion**
  1. Lancer le web browser
  2. Taper l'URL d'une page
  3. Le browser ouvre une connexion TCP pour télécharger la page
  4. Le browser ouvre une 2ème connexion pour ramener une image de la page
  5. Le browser ouvre une 3ème connexion pour gérer le son associé

- **Avec multiplexage de connexion**
  1. Lancer le web browser
  2. Taper l'URL d'une page
  3. Le browser ouvre une connexion TCP pour télécharger la page
  4. Le browser utilise la même connexion pou la page, l'image et le son

2. Format de segment TCP

Segment UDP



$$RUdp = \frac{TIU}{EtM + EIP + EUdp + TIU + EqM} = \frac{TIU}{EtM + 20 + 8 + TIU + EqM}$$

RUdp : rendement de UDP TIU: Taille information utile EUdp: Entête UDP EIP: Entête IP

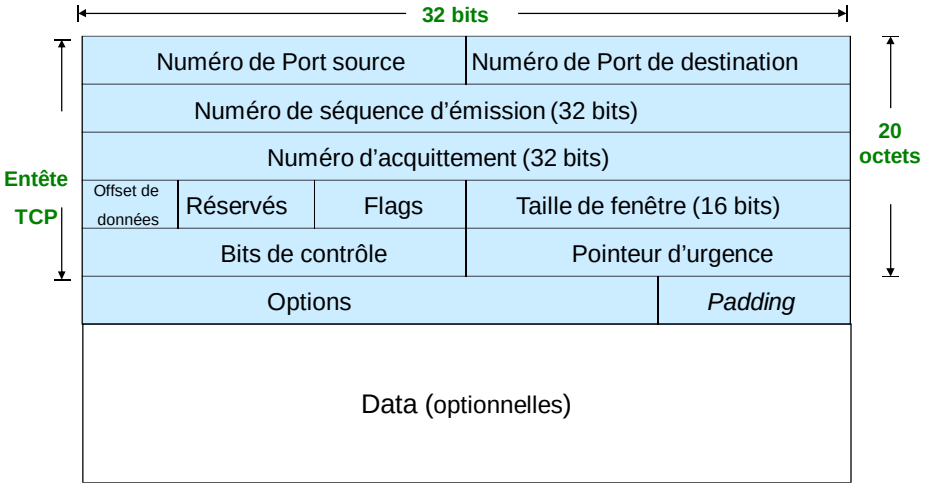
EtM : Entête MAC EqM : Enqueue MAC

$$RUdp\ (Ethernet) = \frac{TIU}{Preambule + EtM + 20 + 8 + TIU + EqM} =$$

$$\frac{TIU}{8 + 14 + 20 + 8 + TIU + 4} = \frac{TIU}{54 + TIU}$$

2. Format de segment TCP

Segment TCP



2. Format de segment TCP

Segment TCP

- Port source et Port destination : indiquent les ports utilisés par les applications.
- Numéro de séquence d'émission : numéro du premier octet de données dans le segment (sauf pour un segment avec SYN=1). Si le bit SYN est à 1 (c.-à-d. si le segment est une demande de connexion), le numéro de séquence signale au destinataire que le prochain segment de données qui sera émis commencera à partir de l'octet *Numéro de séquence d'émission* + 1.
- Numéro d'acquittement : indique le numéro du prochain octet attendu par le destinataire. Si dans le segment reçu FIN=1 et #Seq= x, alors le #Ack renvoyé est x+1 (x est interprété comme étant le numéro de l'octet FIN et que cet octet est acquitté).
- Offset de données : des options (de taille variable) peuvent être intégrées à l'entête et des données de bourrage peuvent être rajoutées pour rendre la longueur de l'entête multiple de 4 octets. L'Offset indique la position relative où commencent les données.
- Taille de fenêtre : indique le nombre d'octets que le destinataire peut recevoir. si Fenêtre = *F* et que le segment contient un Numéro d'acquittement = *A*, alors le récepteur accepte de recevoir les octets numérotés de A à A + F -1.
- Bits de contrôle : séquence de contrôle (CRC) portant sur l'entête de segment.

2. Format de segment TCP

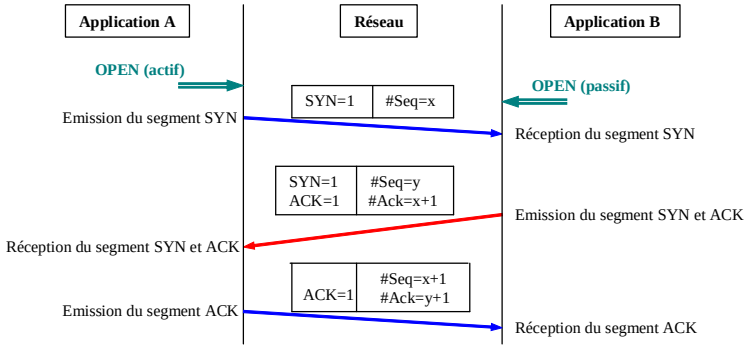
Segment TCP

- Flags (URG, ACK, PSH, RST, SYN, FIN)
  - **URG = 1 si le segment contient des données urgentes et = 0 sinon.**
  - **ACK = 1 indique que le numéro d'acquittement est valide et il peut être pris en compte par le récepteur. ACK = 0 si l'accusé de réception est non valide.**
  - **PSH = 1 indique que les données doivent être remises à l'application dès leur arrivée et de ne pas les stocker dans une file d'attente.**
  - **RST = 1 pour demander la réinitialisation d'une connexion.**
  - **SYN = 1 et ACK = 0 servent à demander l'établissement de connexion.**
  - **SYN = 1 et ACK = 1 servent à accepter une demande de connexion.**
  - **FIN = 1 indique que l'émetteur n'a plus de données à émettre et demande de rompre la connexion de son côté.**
- Pointeur d'urgence : indique l'emplacement (numéro d'octet) des données urgentes dans un segment. Il es valable uniquement si le bit URG=1.
- Options (taille variable) : options nécessitant des traitements particuliers.

3. Ouverture et fermeture de connexion TCP

Ouverture de connexion TCP

- Poignée de mains à 3 phases

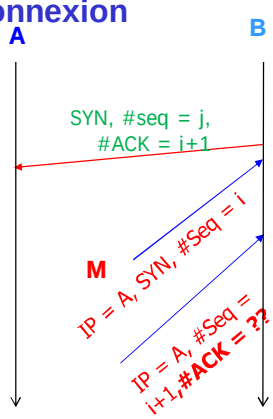


- Robustesse aux pertes de paquets et paquets tardifs durant la phase d'établissement de connexion.

3. Ouverture et fermeture de connexion TCP

Pourquoi choisir des numéros de séquences aléatoires à l'établissement de connexion

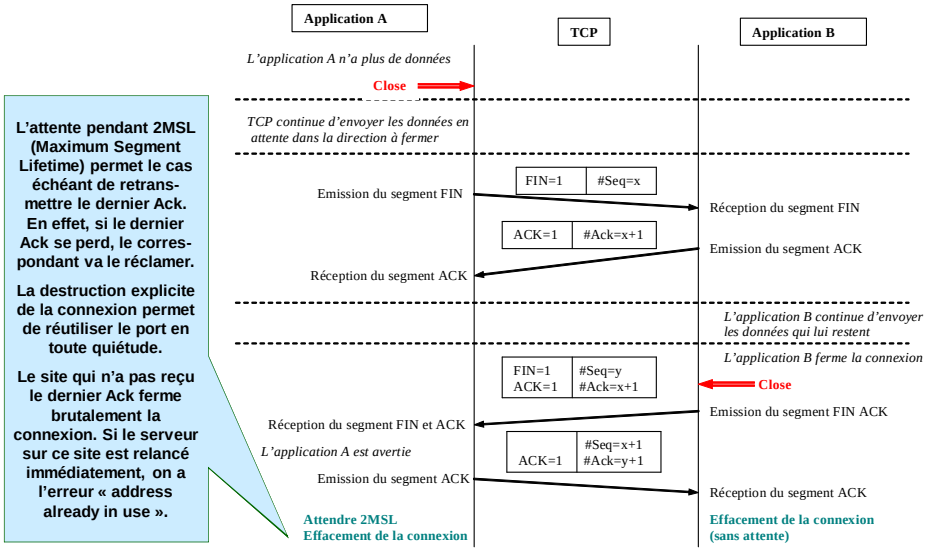
- Supposons que B a confiance en A à partir de l'@IP de A
  - e.g., accepter les demandes de création de compte issues de A
- Un attaquant M veut se faire passer pour A
  - M ne souhaite pas recevoir des données issues de B mais seulement lui envoyer des données pour créer un compte sur B
- M peut-il établir une connexion avec B en se faisant passer pour A?



Si M ne peut pas intercepter les messages entre A et B (pour connaître les numéros de séquence), il ne pourra pas se faire passer pour A une fois la connexion entre A et B établie, à condition que A et B choisissent des numéros de séq aléatoires.

3. Ouverture et fermeture de connexion TCP

Fermeture de connexion TCP



L'attente pendant 2MSL (Maximum Segment Lifetime) permet le cas échéant de retrans-mettre le dernier Ack. En effet, si le dernier Ack se perd, le corres-pondant va le réclamer.

La destruction explicite de la connexion permet de réutiliser le port en toute quiétude.

Le site qui n'a pas reçu le dernier Ack ferme brutalement la connexion. Si le serveur sur ce site est relancé immédiatement, on a l'erreur « address already in use ».

4. Contrôle d'erreurs

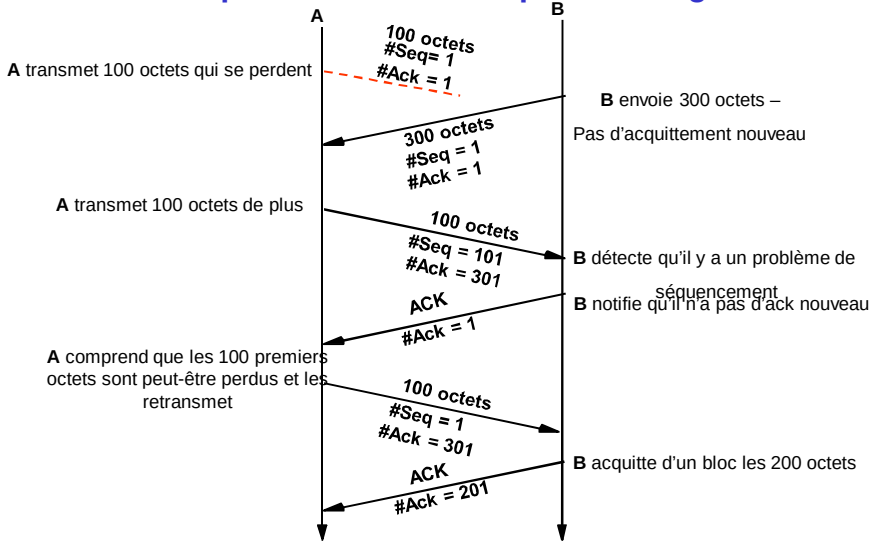
Principe de base du contrôle d'erreur

- Emission de segment suivi d'un armement de temporisateur (timer)
- Utilisation de numéro de séquence en émission
- On numérote les octets et non les segments
- Si un Ack est reçu avant le déclenchement du timer : OK
- Deux mécanismes de retransmission utilisés conjointement :
  - **Retransmission sur Timeout (mécanisme usuel)**
  - **Retransmission rapide (mécanisme utilisé quand le délai réel de transfert est faible comparé à la valeur du timer)**

    Si l'émetteur reçoit trois Ack portant le même numéro d'acquittement inférieur à celui attendu, il retransmet le segment non acquitté sans attendre la fin de temporisation. En effet, si le récepteur reçoit le segment k, mais pas le segment k-1, il renvoie l'Ack correspondant au segment k-2 tant qu'il reçoit des segments autres que le k-1)

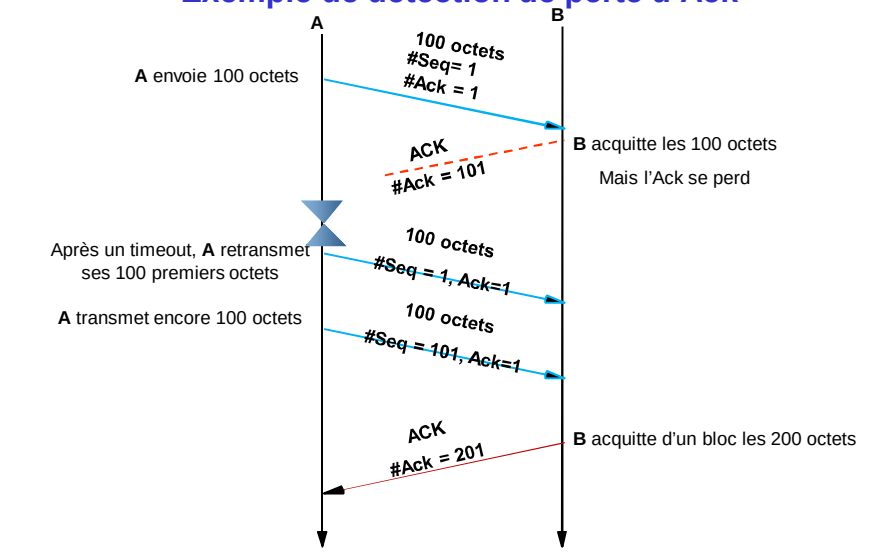
4. Contrôle d'erreurs

Exemple de détection de perte de segment



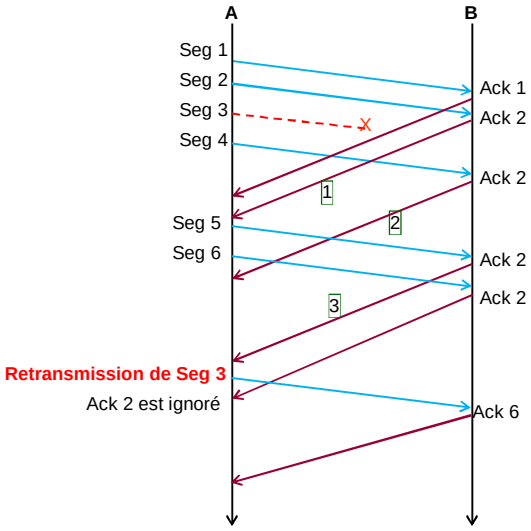
4. Contrôle d'erreurs

Exemple de détection de perte d'Ack



4. Contrôle d'erreurs

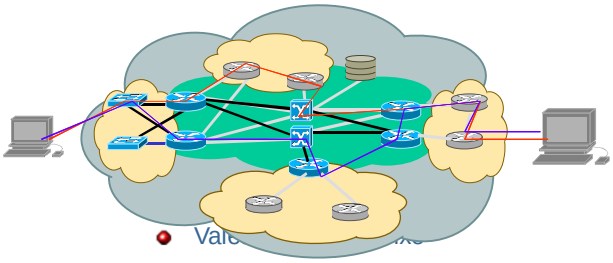
Exemple de retransmission rapide



4. Contrôle d'erreurs

Valeur d'armement du temporisateur

- Le temps de traversée du réseau est variable d'un segment à l'autre



- Valeur fixe
  - **Valeur trop basse : détection de fausses pertes et retransmissions inutiles**
  - **Valeur trop élevée : beaucoup d'attente avant de décider de retransmettre en cas de perte effective**
- TCP utilise un algorithme adaptatif de calcul de la valeur du time-out (être à l'écoute du réseau et fixer la valeur du timer en conséquence)
- Problème : compromis entre la précision de l'état du réseau et le coût de l'algorithme

4. Contrôle d'erreurs

Algorithme de Jacobson

- On part avec une valeur de *RTTestimé* (RTT: round trip time) par défaut
- A chaque réception d'Ack, on détermine le temps qu'a mis l'Ack pour être reçu, *NouveauRTT*
- A chaque réception de nouveau Ack, ré-estimer la valeur du RTT par :

$$RTTestimé = (\alpha * RTTestimé) + (1 - \alpha) NouveauRTT$$

- La valeur d'armement du timer, dite RTO (retransmission TimeOut) est calculée par la formule suivante qui évite des valeurs trop élevées ou trop basses suite aux estimations :

$$RTO = Min \{BorneSupRTO, Max\{BorneInfRTO, \beta * RTTestimé\}\}$$

- *BorneInfRTO*, *BorneSupRTO*, α et β sont fixées par configuration. α <1 et β >1.
- Beaucoup d'implantations de TCP utilisent **α = 0,875 et β = 2**

4. Contrôle d'erreurs

Problème avec l'algorithme de Jacobson

- Idéal pour le calcul du RTO : on reçoit un Ack pour CHAQUE segment
- Inconvénient : on ne peut plus bénéficier des Ack groupés
- TCP réel
  - **un Ack peut être associé à 1 segment, plusieurs segments, un morceau de segment ou à des morceaux contigus de segments.**
  - Cas de retransmission :
    - **Quand TCP retransmet un segment et puis il reçoit un acquittement : est-ce que cet Ack correspond au segment initial ou bien au segment retransmis ? TCP n'a aucun moins de distinguer les deux cas.**
    - **Associer l'Ack au segment le plus ancien peut conduire à une surestimation du *NouveauRTT* si plusieurs tentatives de retransmissions ont été effectuées.**
    - **Associer l'Ack au dernier segment émis peut conduire à une sous-estimation du *NouveauRTT*.**

4. Contrôle d'erreurs

Algorithme de Karn

- Une des solutions utilisées dans la pratique pour remédier au problème avec l'algorithme de Jacobson est connue sous le nom d'algorithme de Karn :
  - **Ne pas mettre à jour la valeur de *RTTestimé* en cas de retransmission**
  - **A chaque de retransmission : calcul d'une valeur dite *RTOaugmenté* par la formule suivante (λ vaut généralement 2 et RTO est la dernière valeur de RTO fournie par l'algorithme de Jacobson) :**

$$RTOaugmenté = RTO^* \lambda$$

  - **Armer le timer avec la valeur *RTOaugmenté*.**
  - **Dans la pratique, après *n* retransmissions consécutives, *RTOaugmenté* vaut RTO^*2^n (augmentation exponentielle)**

5. Contrôle de congestion

Principe de base

- Les applications doivent s'adapter aux conditions du réseau et non le contraire
  - **Quand le réseau est sous-chargé, TCP émetteur augmente le débit**
  - **Quand le réseau est jugé surchargé, TCP émetteur réduit le débit**
- Problème avec les retransmissions :
  - **Un utilisateur non averti (ou malicieux) pourrait se dire « je transmets avec un débit élevé et en cas de perte, je retransmets ».**
  - **Sans précautions, les retransmissions aggravent la congestion. En effet, la congestion de certains routeurs conduit à la perte de segments (car ils sont rejetés par des routeurs saturés). Ensuite, les nœuds d'extrémité qui ont perdu leurs segments retransmettent ce qui augmente la charge du réseau et donc à plus de pertes et ainsi de suite jusqu'à ce que le réseau se bloque complètement.**
  - L'application émettrice doit aussi tenir compte de l'application réceptrice (crédit)
  - Conséquence : le débit de l'émetteur dépend de la charge du réseau et du crédit que lui accorde le récepteur

5. Contrôle de congestion

Principes de base

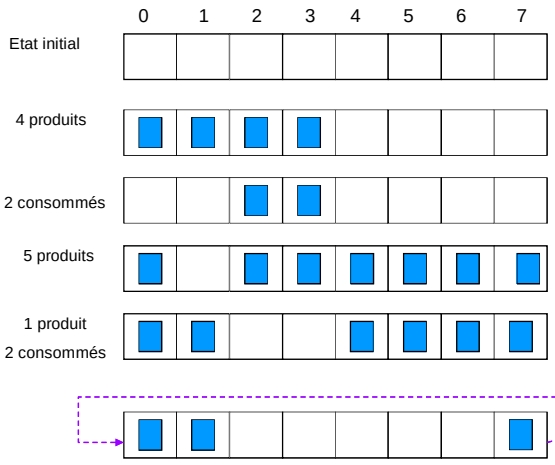
- **Structures de données utilisées par TCP**
  - Fenêtres glissantes (stocker les segments avant leur transmission, avant de les passer à l'application et pour contrôler les Ack)
  - Fenêtre de crédit (pour ne pas saturer le récepteur)
  - Fenêtre de congestion de l'émetteur (notée Cwd : congestion window) : c'est la taille maximum (en octets) que TCP-émetteur peut émettre avant d'être obligé d'attendre un Ack. Cwd n'a pas de valeur fixe (comme pour la couche liaison de données) mais une valeur dynamique.

Hypothèse de TCP : si la source ne reçoit pas d'Ack, la cause la plus probable est une perte de segment due à une congestion d'un des routeurs traversés

- **Hypothèse non vraie dans le cas des réseaux sans fils**

5. Contrôle de congestion

Rappel sur les buffers circulaires



	Producteur	Consommateur
Etat initial	CP = 8	CC = 0
	IxP = 0	IxC = 0
4 produits	NP = 4	NC = 4
	IxP = 4	IxC = 0
2 consommés	NP = 6	NC = 2
	IxP = 4	IxC = 2
5 produits	NP = 1	NC = 7
	IxP = 1	IxC = 2
1 produit 2 consommés	NP = 2	NC = 6
	IxP = 2	IxC = 4

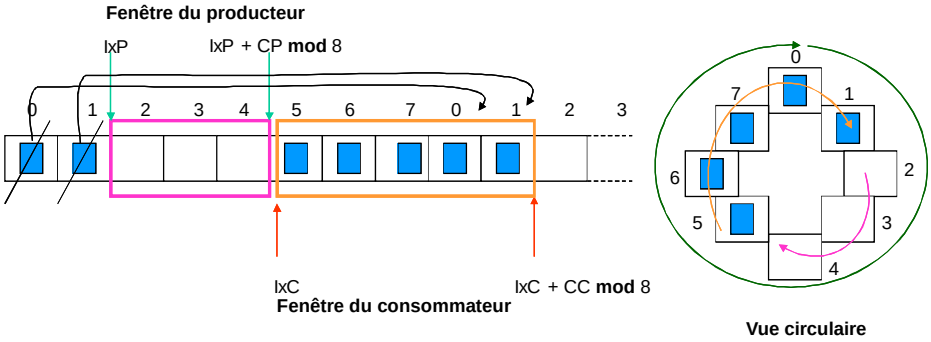
Gestion circulaire

CP : capacité de production CC : capacité de consommation IxP : indice de la case de la case livre

IxC : indice de la case de début de consommation

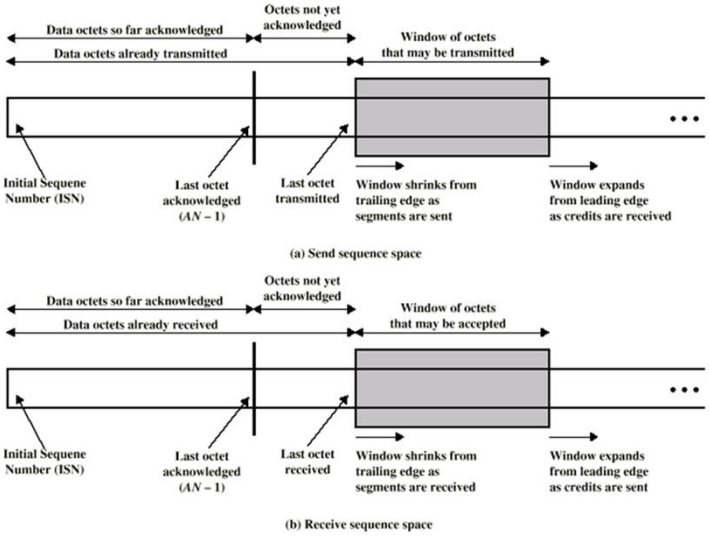
5. Contrôle de congestion

Rappel sur les buffers circulaires



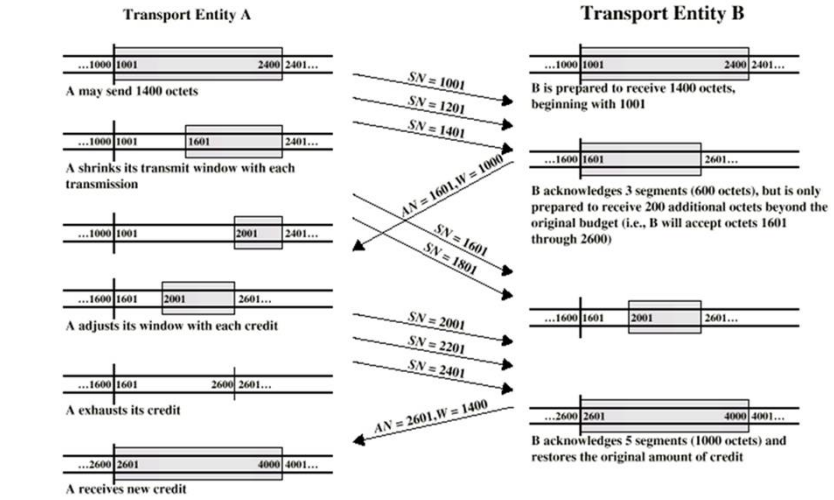
5. Contrôle de congestion

Fenêtres glissantes



5. Contrôle de congestion

Exemple de fonctionnement de fenêtres glissantes



SN: Numéro de séquence à l'émission AN : Numéro d'acquittement W : Fenêtre

5. Contrôle de congestion

Stratégie « Additive increase – Multiplicative decrease »

« Démarrage lent – Diminution dichotomique » ou « Augmentation lente – Réduction drastique »

- Le nombre d'octets que l'émetteur peut transmettre à un instant donné est limité à une quantité dite *Fenêtre Autorisée* :

  Fenêtre autorisée = Min {Fenêtre de contrôle de flux, Fenêtre de congestion }

  Fenêtre de contrôle de flux = Crédit – nombre d'octets non encore acquittés

- Démarrer la transmission avec une valeur de Cwd égale à *Cwd_min* (qui est un paramètre de configuration de réseau et qui correspond à un segment)

- Si l'Ack revient avant la fin du timer, augmenter la fenêtre de congestion

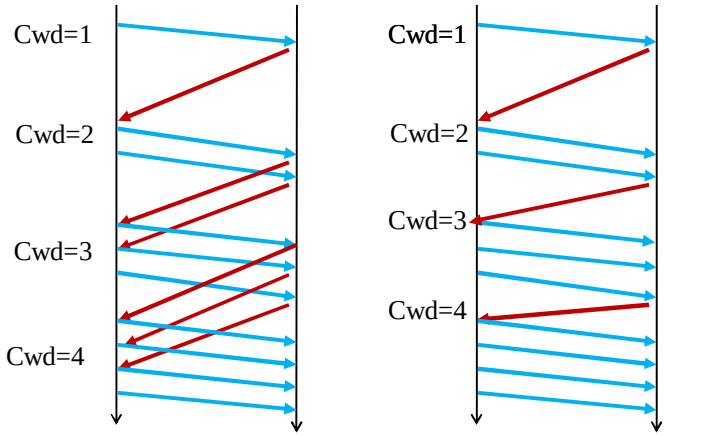
  Cwd = Cwd + TailleSegment

- Si l'Ack ne revient pas, réduire de moitié la fenêtre de congestion

  Cwd = Cwd/2

5. Contrôle de congestion

Exemple de « Additive increase »

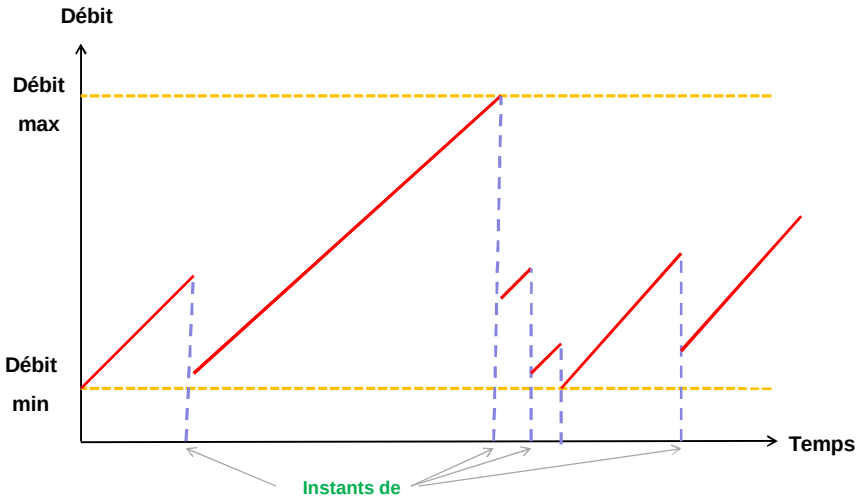


Ack segment par segment

Ack par bloc de segments

5. Contrôle de congestion

Exemple de changement de débit



6. Autres sur TCP

Syndrome de la fenêtre stupide

- Situation qui arrive lorsque les données sont passées à TCP source :
  - Soit en très petite quantité (ex. octet par octet) – Dans ce cas, l'application Source est très lente. TCP émetteur envoie des segments de données contenant très peu de données (ex. 1 octet de données par segment).
  - Soit en gros blocs, mais l'application côté récepteur lit les données octet par octet (ou en petite quantité) – Dans ce cas, l'application Destinataire est lente. TCP récepteur envoie un Ack pour chaque octet délivré à l'application Destinataire.
- Dans les deux cas : gaspillage de bande passante
- Solution de Nagle: Retarder la transmission des segments de données pour envoyer des segments avec une taille minimale
- Solution de Clark : Retarder la transmission des Acks et acquitter plusieurs octets en même temps

6. Autres sur TCP

TCP avancés

- **TCP : Reno, New Reno, Vegas, Tahoe…**
  - Algorithmes plus élaborés pour l'estimation du RTT et calcul du RTO
  - Algorithmes plus élaborés pour le contrôle de congestion
- **TCP pour les réseaux sans fils**
- **TCP « light » (pour les réseaux de capteurs…)**

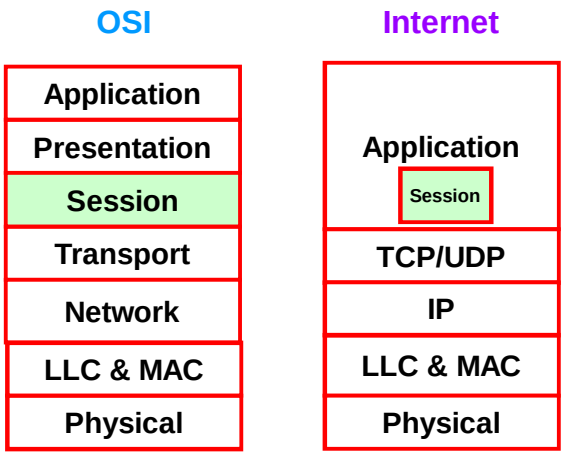
Chapitre 9.1

Couche Session

(selon le modèle OSI)

1. Introduction

Où sommes-nous dans les couches ?



1. Introduction

Pannes et anomalies dans les systèmes répartis

- **Pannes de sites (stations)**
  - Pannes matérielles
    - RAM ou CPU ⇨ données perdues
    - Disque (secteurs disques endommagés) ⇨ données perdues ou corrompues
    - Coupures d'alimentation ⇨ Perte de tout ce qui est temporaire
  - Pannes du logiciel (tout peut arriver depuis l'OS jusqu'aux applications) ⇨ perte de données
- **Pannes de réseaux**
  - Pannes (matérielles ou logicielles) de routeurs, commutateurs et passerelles
  - Arrêts inopinés (non attendus par les utilisateurs) de routeurs, commutateurs et passerelles
  - Coupures de ligne de communication

1. Introduction

Gestion des anomalies par les couches de communication

- **Couches de communication** : MAC, LLC, Réseau et Transport
- **Anomalies gérées**
  - Erreurs de transmission
  - Pertes de trames, paquets ou trames
  - Arrivée dans le désordre de paquets ou messages
- **Principe commun : numérotation + Ack + retransmission**

Les pannes ne sont pas prises en compte par les couches de communication

1. Introduction

Exemple pour comprendre l'intérêt de la couche Session

- Un utilisateur connecté par un modem à 50 kb/s veut télécharger un film codé sur 1 G octets.
- Durée de téléchargement $= \frac{10^9 * 8}{50 * 10^3} \text{sec} = 16 * 10^4 \text{ sec} = \frac{16 * 10^4}{3600} h \approx 44.44h$
- Un administrateur de BD connecté par un modem à 50 kb/s veut sauvegarder sa BD de 100 G octets sur un site de stockage.
- Durée de téléchargement = 4444 heures = 185 jours

Que se passe t-il s'il y a une panne pendant le transfert ?

➔ Perte d'un temps important

1. Introduction

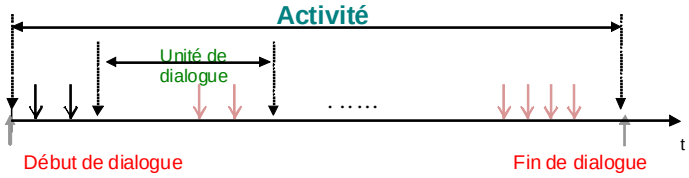
Pourquoi faut-il une couche session ?

- Objectifs : fournir aux entités de présentation les moyens nécessaires pour organiser et synchroniser leurs dialogues et pour gérer les échanges de données volumineuses
- **Mécanismes de la couche session**
  - Pose de point de reprise
  - Suspension des échanges (suite à des anomalies ou pannes)
  - Reprise des échanges

2. Eléments de la couche session

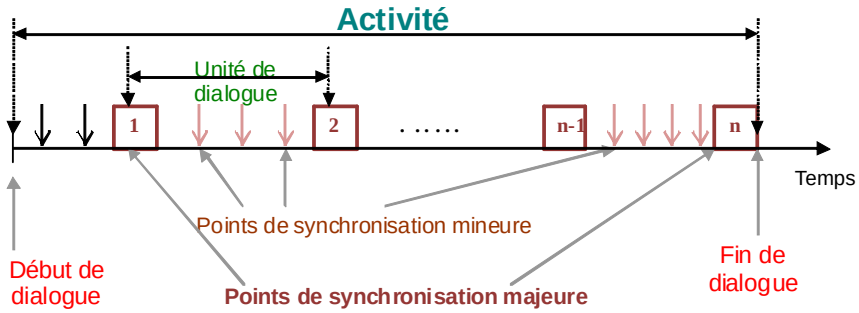
Activité, unité de dialogue

- **Activité** = une ou plusieurs **unités de dialogue**
- **Unité de dialogue**
  - C'est un ensemble d'opérations d'échange de messages
  - C'est l'utilisateur qui choisit le niveau de détail de ses unités de dialogue
  - Exemples d'unités de dialogue
    - Transaction sur une base de données
    - Transfert de 1000 enregistrements d'un fichier
    - Transfert d'une table d'une BD,
    - Lecture de 5 minutes de musique
    - Lecture d'un acte d'une pièce de théâtre



2. Eléments de la couche session

Activité, unité de dialogue, points de reprise



Point de reprise, Point de synchronisation ou Checkpoint

2. Eléments de la couche session

Points de reprise

- Synchronisation mineure
  - Pour gérer les arrêts de la communication dus à des anomalies/pannes du réseau ou arrêt brutal du correspondant
  - Reprise à chaud
- Synchronisation majeure
  - Pour gérer les pannes du correspondant avec perte de données sur disque
  - Reprise à froid
- Attributs d'un point de reprise
  - Un numéro de série, Un Id de session
  - Un nombre d'octets validés par le point de reprise
  - Une estampille
  - …
- Sauvegarde des points de reprise
  - Dans un fichier temporaire (synchro mineure) : journal de points de reprise
  - Dans un fichier permanant avec éventuellement des copies multiples (synchro majeure)

2. Eléments de la couche session

Pose de point de synchronisation

- Lorsque les données envoyées ont été acquittées par le niveau inférieur (TCP ou autre), la pose de point de reprise peut commencer
- L'un des deux correspondants peut déclencher l'opération de pose de point de reprise
- Pour l'émetteur de données
  - Sauvegarde du dernier point de reprise
  - Le cas échéant effacement des données déjà transférées et validées
- Pour le récepteur de données
  - Sauvegarde du dernier point de reprise
  - Validation de la sauvegarde des données reçues

2. Eléments de la couche session

Reprise après arrêt/coupure de session

Si la session se termine normalement, tous les fichiers de sauvegarde des points de reprise et des données transférées sont supprimés. Sinon ils sont utilisés lors d'une reprise.

- Les deux correspondants reprennent une session suspendue
- Les deux correspondants utilisent leurs fichiers de sauvegarde de points de reprise et de données

La couche session de ne spécifie pas comment sont réalisées les opérations de sauvegarde et d'utilisation des informations sauvegardées.

C'est un problème d'implantation.

2. Eléments de la couche session

Contrôle alterné, jeton de contrôle

- Dès qu'il y a synchronisation, il faut définir les règles de contrôle
- Contrôle décentralisé : chacun des partenaires exécute les opérations qu'il souhaite de manière unilatérale
- Contrôle alterné : les opérations de transmission de données, de synchronisation ne sont faites que par un seul des partenaires à la fois
- Utilisation de jetons pour synchroniser les partenaires

- Types de jeton
  - Jeton de données (qui a le droit démettre des données ?)
  - Jeton de libération de session (qui a le droit de fermer la session ?)
  - Jeton de synchro mineure (qui a le droit de poser des point de syn min ?)
  - Jeton de synchro majeure (qui a le droit de poser des point de syn maj ?)

C'est le concepteur d'application qui choisit les types de jeton et la manière de les utiliser selon ses besoins.

3. Services de session

Besoins et contraintes

- **Spécificités des applications**
  - Rares sont les applications qui ont besoin de synchronisation majeure
  - Très peu d'applications ont besoin de gérer des activités de communication parallèles
  - Très peu d'applications ont besoin de synchronisation des échanges réalisée par la couche inférieure
- **Contraintes**
  - Permettre l'interopérabilité entre couches
  - Permettre l'interopérabilité entre sites distants
  - Ne pas alourdir les systèmes par des fonctions inutiles
- **Solution**
  - Regrouper les services en unités fonctionnelles selon des besoins
  - Les unités fonctionnelles sont choisies en option (sauf une unité qui est obligatoire, l'unité noyau)

3. Services de session

Services de session

- **Unité fonctionnelle noyau**
  - S-CONNECT : demande d'établissement de session
  - S-DATA : demande d'envoi de message
  - S-RELEASE : demande de libération de session
  - S-U-ABORT : demande d'avortement de session par l'utilisateur
  - S-P-ABORT: indication d'avortement de session à cause d'anomalie irrécupérable signalée par la couche inférieure

3. Services de session

Services de session

- **Unité fonctionnelle Contrôle en alternance avec jeton**
  - S-TOKEN-GIVE : passage du jeton
  - S-TOKEN-PLEASE : demande de jeton
- **Unité fonctionnelle de Synchronisation mineure**
  - S-SYNC-MINOR : réaliser un point de synchronisation mineure
  - S-TOKEN-GIVE, S-TOKEN-PLEASE
- **Unité fonctionnelle de Synchronisation majeure**
  - S-SYNC-MAJOR : réaliser un point de synchronisation majeure
  - S-TOKEN-GIVE, S-TOKEN-PLEASE

3. Services de session

Services de session

- **Unité fonctionnelle Gestion d'activité**
  - S-ACTIVITY-START : début d'activité
  - S-ACTIVITY-INTERRUPT : suspension d'activité
  - S-ACTIVITY-RESUME : reprise d'activité après suspension
  - S-ACTIVITY-DISCARD : abandon d'activité
  - S-ACTIVITY-END : fin d'activité
  - S-TOKEN-GIVE, S-TOKEN-PLEASE, S-CONTROL-GIVE

3. Services de session

Session et QoS

- **Spécification des besoins en QoS**
  - délai maximum d'établissement de connexion de session
  - probabilité d'échec d'établissement de connexion de session
  - débit nécessaire à la session
  - temps de transfert
  - taux d'erreurs résiduelles
  - probabilité d'incident de transfert
  - délai de libération de connexion de session
  - probabilité d'échec de libération de connexion de session
  - protection de connexion de session
  - priorité de connexion de session
  - …

4. Conclusion

- Les services fournis par la couche session sont utiles à certaines applications, pas à toutes les applications Réseau
- Ces services
  - Sont réalisés par une couche à part entière : Modèle OSI
  - Sont des services de la couche Application : Modèle TCP/IP
- La mise en œuvre de ces services fait appel à des compétences en
  - Gestion de fichiers Journaux
  - Gestion de fichiers avec copies multiples

Chapitre 9.2

Introduction à SIP

(Session Initiation Protocol)

1. Introduction

Concept de session

- **Session** : période pendant laquelle un ensemble d'entités communique ou coopère via un réseau.
- **Session multimédia** : période de communication de flux multimédia entre un groupes d'entités.
- Exemples de session
  - Téléconférence
  - Conférence téléphonique
  - Appel téléphonique

1. Introduction

Concept de session

- **Description de session** : spécification des infos liées à une session (sujet de la session, type de média, durée de session, règles de sécurité…)
- **Annonce de session** : mécanisme (protocole) par lequel la description de session est communiquée aux participants potentiels
- Protocoles de session
  - Approche OSI ➔ Couche Session
  - Approche IETF ➔ Protocole SIP (de niveau Application)
  - Approche ITU ➔ Protocole H.323 (de niveau Application)

1. Introduction

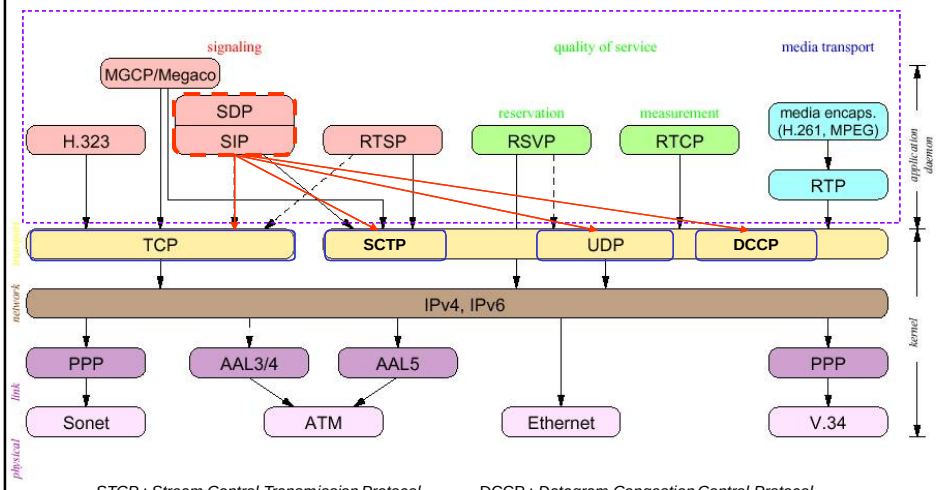
SIP en bref

- SIP : Session Initiation Protocol
- Protocole 'phare' pour la gestion de session dans le monde Internet
- Pour Internet, SIP est un protocole de niveau Application
- RFC consacrés à SIP
  - Premier RFC sur SIP : RFC 2543 – Mars 1999
  - Version actuelle : RFC 3261 (juin 2002) – 269 pages – plusieurs fois étendue
  - En Mars 2009 : 82 RFC contiennent SIP dans leur titre (prise en compte de la sécurité, diversité des flux multimédia, diversité des réseaux et protocoles de transport…
- SDP : Session Description Protocol
- Utilisé par SIP pour décrire les paramètres de session
- RFC consacrés à SDP
  - Premier RFC sur SDP : RFC 2327 - 1998
  - Version actuelle : RFC 4566, Juillet 2006
  - En mars 2009 : 21 RFC contiennent SDP dans leur titre

H.323 : Concurrent de SIP développé et promu par l'ITU

1. Introduction

SIP en bref



STCP : Stream Control Transmission Protocol

DCCP : *Datagram Congestion Control Protocol*

RTSP : Real Time Streaming Protocol

RTCP : Real time Transport Control Protocol

1. Introduction

SIP en bref

- En général, l'objectif de SIP est de rendre plus facile (transparent) le déploiement d'applications multimédia via IP. Atteindre le « ALL-over-IP »
- Applications actuelles de SIP
  - **Flux continus**
    - * Téléconférence
    - * Téléphonie
    - * Distribution de contenu multimédia (streaming)
  - **Flux événementiels**
    - * Messagerie instantanée
    - * Présence (ex. contrôle d'éclairage ou d'intrusion dans les habitations) : quand l'événement arrive, on avertit l'usager abonné à l'évènement
- Les messages SIP sont transportés par un protocole de transport (TCP, RTP, UDP…)
- SIP est largement inspiré de HTTP (mode requête-réponse)

1. Introduction

SIP en bref

- **5 fonctionnalités de base de SIP**
  - *Localisation de l'appelé* : détermination de l'endroit où se trouve l'appelé
  - *Disponibilité de l'utilisateur* : déterminer si l'utilisateur appelé souhaite s'engager dans la communication
  - *Capacités de l'appelé* : déterminer si les capacités (en termes de codec et autres) de l'appelé sont suffisantes pour engager la communication. Il peut y avoir négociation des capacités pour s'adapter la session
  - *Etablissement de l'appel (Call setup)* : 'sonnerie', mise en correspondance des deux interlocuteurs
  - *Suivi d'appel (Call handling)* : transfert de données, maintien de la session et terminaison

1. Introduction

SIP en bref

- SIP permet de fixer les paramètres de session
  - Identification des partenaires
  - Identification des médias
  - …
- SIP gère des sessions point à point (unicast) ou multipoint (multicast)
- SIP permet de modifier les paramètres de session
  - Ajout ou retrait de média
  - Ajout (invitation) ou retrait de membre dans une session multicast
- SIP permet de gérer la mobilité des usagers
- SIP permet de rediriger les appels

1. Introduction

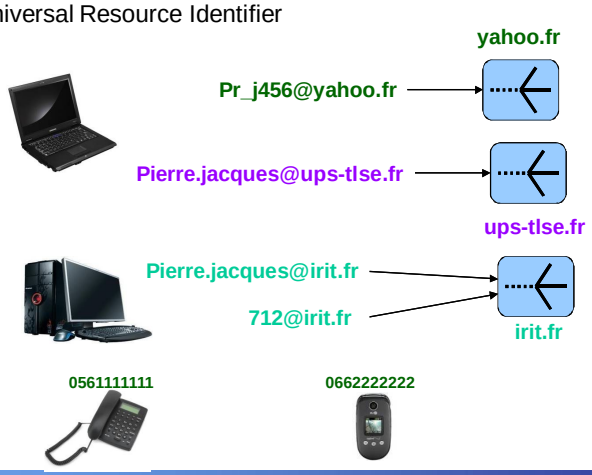
SIP en bref

- Deux aspects importants liés à une session de média session
  - Codage de média
    - Utilisation d'un codec
    - Codecs usuels : G.711, G.723.1, G.729, AMR …
  - Transport de média
    - Utilisation d'un protocole de transport (UDP, TCP, SCTP, DCCP, RTP…)
    - RTP est le protocole généralement associé à SIP pour les flux multimédia
    - RTP est fondé sur l'estampillage de messages et le rejet de messages tardifs

2. Entités SIP et leurs interactions

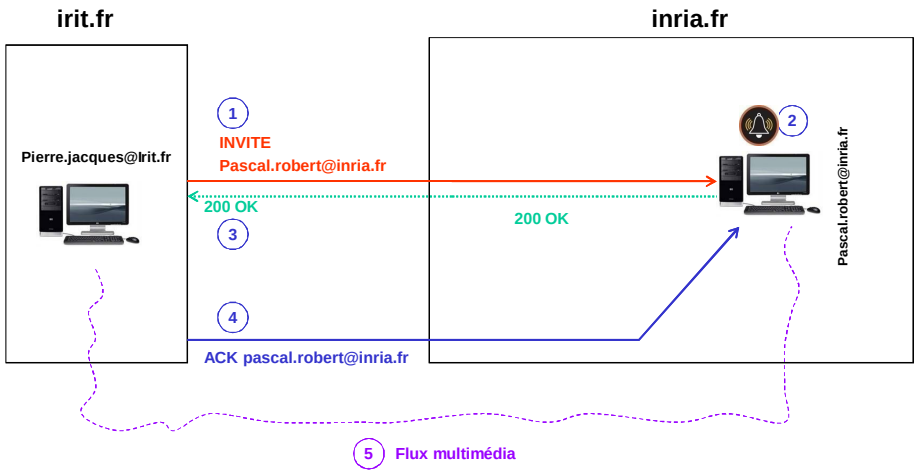
Adressage des abonnés

- N identités pour un même abonné/utilisateur
- URI : Universal Resource Identifier



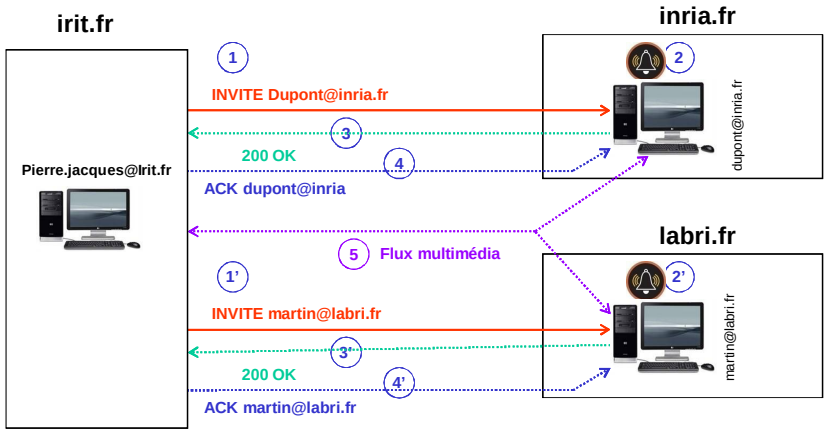
2. Entités SIP et leurs interactions

SIP en mode pair à pair (sans intermédiaire SIP)



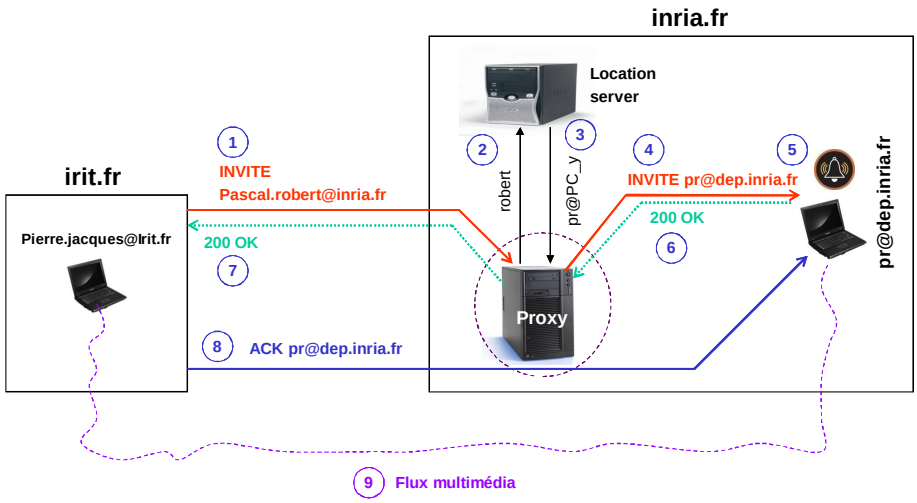
2. Entités SIP et leurs interactions

SIP en mode multipoint (sans intermédiaire SIP)



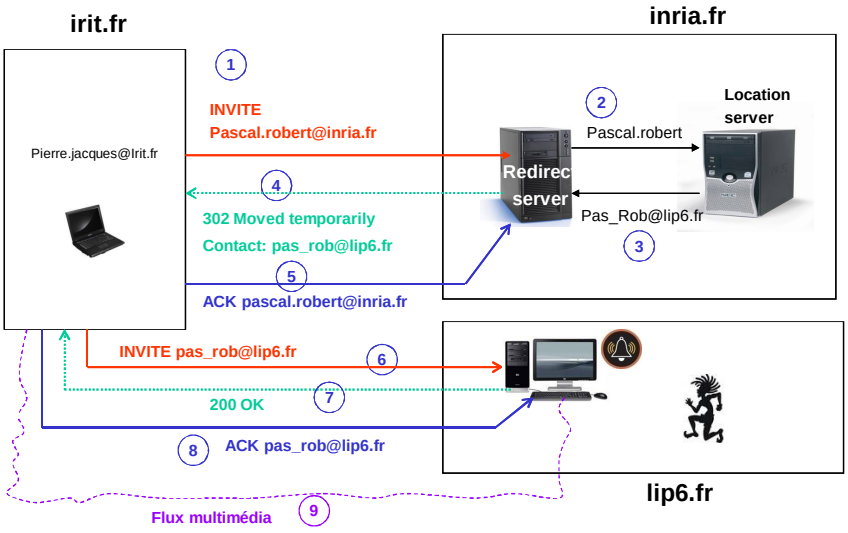
2. Entités SIP et leurs interactions

SIP avec proxy



2. Entités SIP et leurs interactions

SIP en mode redirection



2. Entités SIP et leurs interactions

Entités de SIP

- SIP : basé sur le modèle Client/serveur (comme HTTP)
- **Entités SIP**
  - Agent Client (appelé UAC : user agent client) : entité, qui se trouve sur tout équipement, ayant pour rôle d'envoyer les requêtes et recevoir les réponses
  - Agent Serveur (appelé aussi UAS : user agent server) : entité, qui se trouve sur tout équipement SIP, ayant pour rôle de générer et d'envoyer les réponses
  - Serveur proxy
  - Serveur de redirection
  - Registre et Service de localisation
  - Passerelles SIP vers des réseaux non-conformes à SIP

- Les serveurs sont des fonctions (appareils logiques) qui peuvent être déployées ou non sur des appareils physiques distincts.

2. Entités SIP et leurs interactions

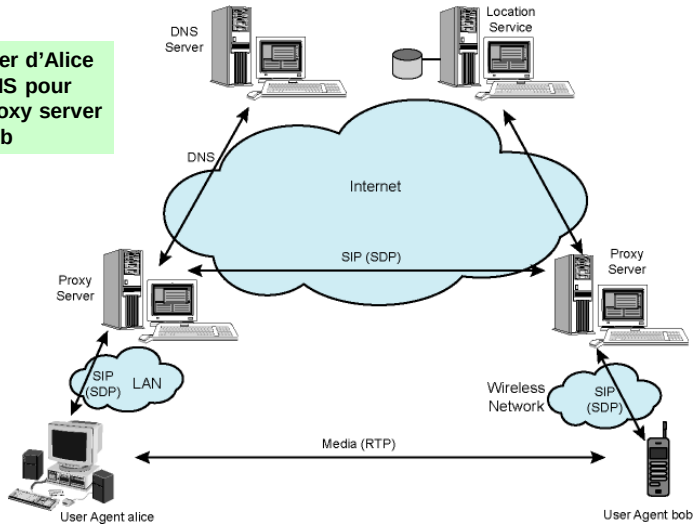
Entités de SIP

- **Serveur Proxy**
  - Entités qui agissent en tant que clients ou serveurs pour faciliter la tâche des agents utilisateur Clients
  - Les proxies ont surtout un rôle de 'routage' (i.e. envoyer la requête est envoyée vers une entité proche de l'usager cible).
  - Ils servent aussi à mettre en lace des politiques d'accès/sécurité (quels usagers peuvent appeler ?...)
- **Serveur de redirection** : utilisé pendant la phase d'initiation d'appel pour déterminer l'adresse de l'appareil appelé. Avec l'info retournée par le serveur de redirection, l'UAC de l'appareil appelant est redirigé vers une URI alternative pour contacter l'UAS correspondant.
- **Registre** : entité qui sert à traiter les requêtes d'enregistrement des infos sur les usagers (adresse SIP, adresse IP de l'usager…) – c'est une sorte de répertoire. Les infos sont stockées sur le Service de localisation
- **Service de localisation** (pseudo DNS)
  - Maintient une base de données des mappings entre adresses SIP et identificateurs d'utilisateur
  - utilisé par le serveur proxy ou serveur de redirection pour obtenir des infos sur la localisation de l'appelé

2. Entités SIP et leurs interactions

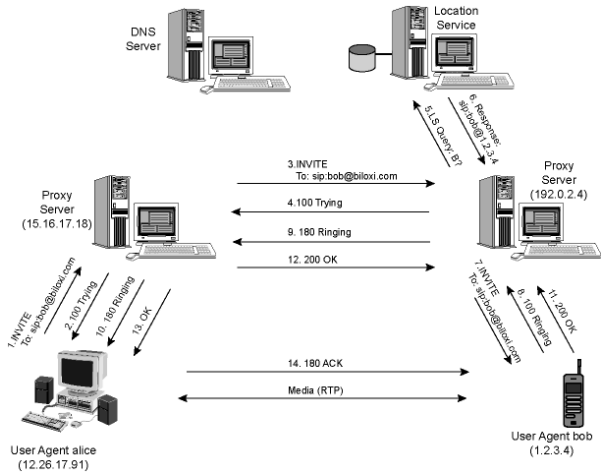
Entités de SIP

Le proxy server d'Alice utilise le DNS pour retrouver le proxy server de Bob



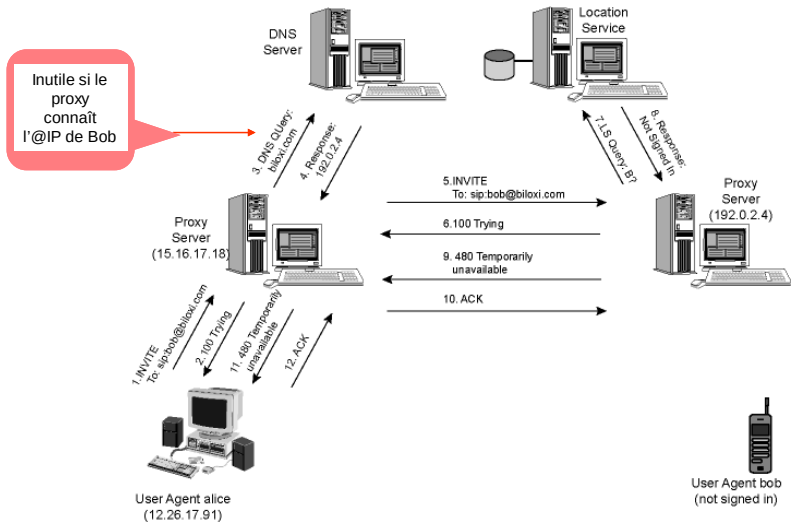
2. Entités SIP et leurs interactions

Exemple 1 – Etablissement d'appel (avec succès)



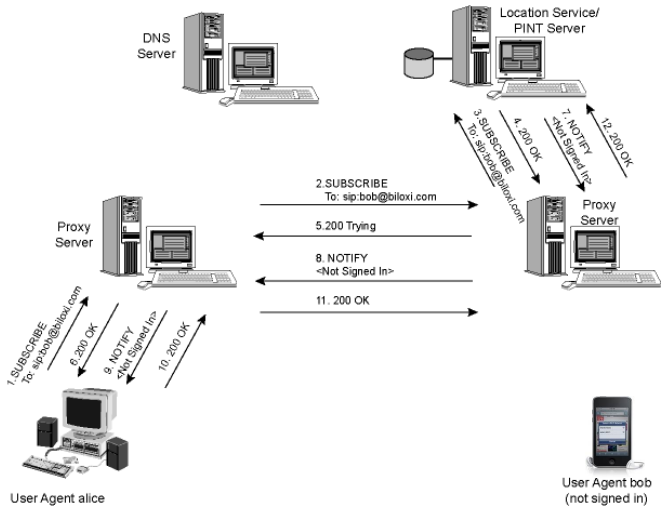
2. Entités SIP et leurs interactions

Exemple 2 – Etablissement d'appel (avec échec)



2. Entités SIP et leurs interactions

Exemple 3 – Présence (1 – souscription)



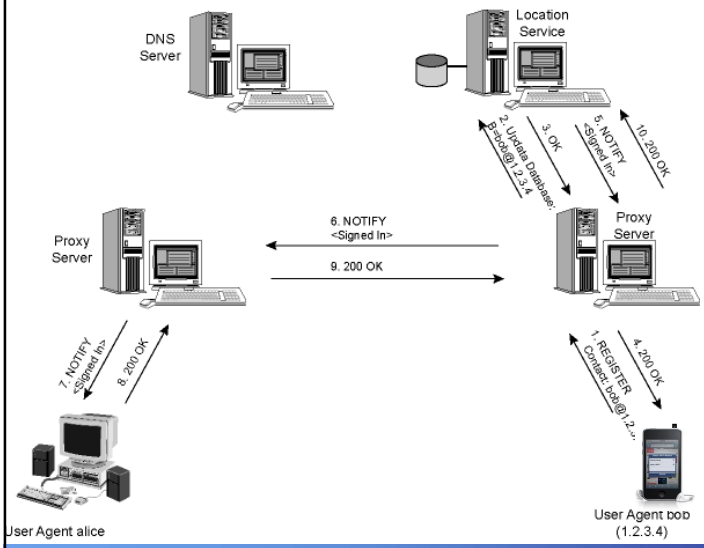
Alice veut communiquer avec Bob qui n'est pas disponible.

Elle s'abonne auprès du Proxy de Bob pour qu'il l'avertisse quand Bob devient joignable.

Les requêtes SUBSCRIBE et NOTIFY utilisées dans l'échange ne sont pas des requêtes standards de SIP. Il s'agit d'extensions de SIP pour la téléphonie.

2. Entités SIP et leurs interactions

Exemple 3 – Présence (2 – Enregistrement et notification)



Bob devient joignable.

Il s'enregistre auprès de son proxy.

Le proxy met à jour la base de données.

Le proxy joue aussi le rôle de REGISTRE

Le proxy notifie à Alice que Bob est maintenant joignable.

3. Requêtes et réponses SIP

Format de messages SIP

méthode (Requête) ou **Réponse**

Méthode URL SIP/2.0	SIP/2.0 Etat Raison

Via:	SIP/2.0 protocole host:port
From:	Id du user source
To:	Id du user destination
Call-Id:	local_id@host
CSeq:	numéro de séquence méthode
Content-length:	longueur d'entête
Content-type:	type de média

Entête de message

V=	
O=	Description de médias avec le protocole SDP
C=	
…...	

Corps de message

3. Requêtes et réponses SIP

Requêtes (méthodes) SIP

- **INVITE** : demande d'établissement de session entre agents utilisateurs
- **ACK** : confirmation de l'échange précédent
- **BYE** : terminaison de session
- **CANCEL** : annulation de requête pendante sans mettre fin à la session
- **OPTIONS** : demande d'informations sur le profil (capacités) de l'appelé, sans initialisation de session
- **REGISTER** : demande d'un agent utilisateur pour enregistrer son adresse IP et URL courantes pour recevoir les appels.

- Une requête SIP est spécifiée sur une ligne selon la forme suivante :

```
<Méthode> <URI> <SP> <SIP-Version>  <retourChariot>
<Méthode> ::= INVITE | ACK | BYE | CANCEL | OPTIONS | REGISTER
```

Exemple :

INVITE sip:picard@societe.com SIP/2.0

3. Requêtes et réponses SIP

Réponses SIP

- **1**xy (*Informational*) : requête bien reçue, traitement de requête en cours
- **2**xy (*Success*) : requête précédente reçue, acceptée et traitée
- **3**xy (*Redirection*) : autre action à entreprendre pour compléter la requête
- **4**xy (*Client error*) : requête contenant une erreur de syntaxe ou non valide pour le serveur cible
- **5**xy (*Server error*) : échec du serveur à traiter une requête (jugée valide pour ce serveur)
- **6**xy (*Global failure*): requête invalide pour tout serveur

- Une réponse SIP est spécifiée sur une ligne selon la forme suivante :

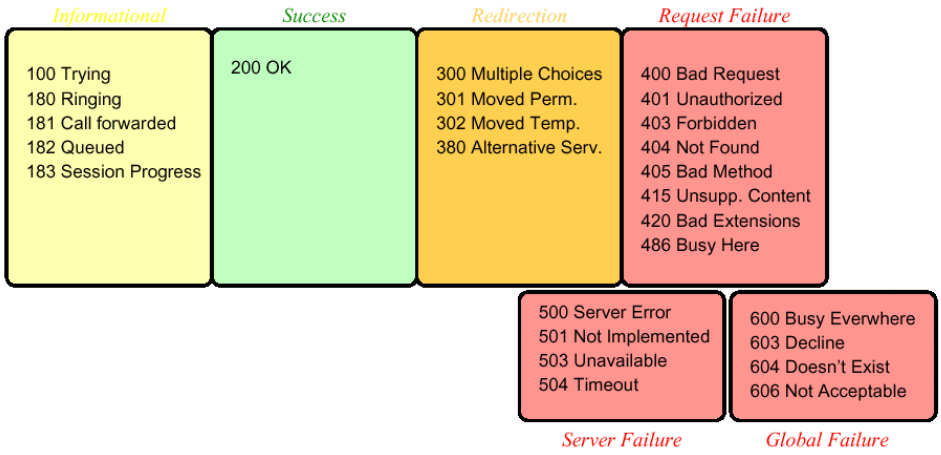
```
<SIP-Version> <SP status-code> <SP reason> <Carriage return>
```

Exemple :

SIP/2.0 404 Not Found // le premier (4) caractère du code indique la classe de réponse

3. Requêtes et réponses SIP

Codes Réponses SIP



3. Requêtes et réponses SIP

Attribut VIA et routage

- Chaque requête inclut un champ **VIA** qui contient le chemin (partiel) pris par la requête
- L'agent Client indique son adresse dans le champ VIA
- Chaque Proxy qui traite la requête rajoute son adresse au champ VIA
  - Pour permettre aux réponses de prendre le même chemin que les requêtes
  - Pour éviter les boucles de routage
  - Pour avertir les firewalls qui vont relayer les réponses
- L 'agent Serveur recopie le contenu du champ VIA dans la réponse, puis renvoie la réponse dans le sens inverse du chemin de la requête

3. Requêtes et réponses SIP

Exemples d'entête de message SIP

```
INVITE sip:picard@societe1.com SIP/2.0
Via: SIP/2.0/UDP host.societe2.com:5060
From: Pierre Jules <sip:pierre.jules@societe2.com>
To: Jean Luc Picard <sip:picard@societe1.com>
Call-ID: 314159@host.societe1.com
CSeq: 1 INVITE
```

Numéro de séquence de requête

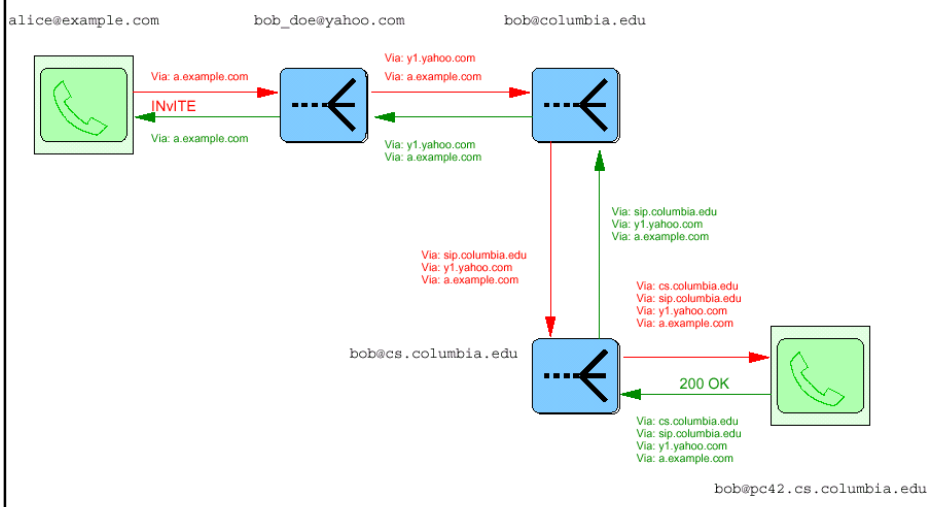
```
INVITE sip:robert@societe3.com SIP/2.0
Via: SIP/2.0/UDP 12.26.17.91:5060
Max-Forwards: 10
To: robert <sip:robert@societe3.com>
From: Jules <sip:jules@societe1.com
Call-ID: a84b4c76e66710@12.26.17.91
CSeq: 314159 INVITE
Contact: <sip:jules@societeVisitee.com>
Content-Type: application/sdp
Content-Length: ...
```

Nombre max de sauts

Jules indique qu'il faut le contacter ailleurs que dans sa société

3. Requêtes et réponses SIP

Exemple de route SIP multi-sauts



3. Requêtes et réponses SIP

Protocole SDP (RFC 4566)

- Session Description Protocol (SDP) = protocole pour décrire les paramètres de session
- Les paramètres de session permettent aux membres de session de se joindre ou non à la session en fonction des médias proposés
- La description de session inclut notamment les éléments suivants
  - Un ou plusieurs média (audio, vidéo, data…)
  - Une ou n adresses de destination
  - Port (TCP, UDP….) utilisé pour chaque média
  - Instant de début et fin de session
  - Règles de sécurité à appliquer à la session

- La description de paramètre se fait selon le format

  <description de paramètre> = [*] <valeur>

  * : désigne une valeur optionnelle

3. Requêtes et réponses SIP

Protocole SDP

- Numéro de version de SIP : « v=… »
- Identification de l'initiateur de session : « o=… »
  - nom de user
  - session id
  - type de réseau (IN : internet…)
  - type d'adresse (IP4 ou IP6),
  - adresse IP unicast de la machine d'initialisation de session
- Nom de session : « s=… »
- Infos sommaires sur la session : « i*=… »
- URL de description de session : « u*=… »
- Adresse mail : « e*=… »
- Numéro de téléphone : « p*=… »
- Description de la connexion de données **:** « c*=… »
  - Type de réseau : IN pour Internet
  - Type d'adresse : IP4 ou IP6
  - Adresse de connexion

3. Requêtes et réponses SIP

Protocole SDP

- Bande passante proposée pour supporter la session : « b*=… »
- Aspects temporels : on spécifie une liste d'éléments
  - Instants (en sec depuis 1900) de début et fin de session : « t=… »
  - Répétition de la session : « r*=… »
- Ajustements d'horaires en cas de fuseaux horaires multiples : « z*=… »
- Clé de cryptage : « k*=… »
- Autres attributs de session : « a*=… »
- Description d'un ou plusieurs médias avec les éléments suivants :
  - Nom du média et adresse de transport : **« m=… »**
    - Type de media (texte, audio, vidéo, message)
    - Port de communication pour la session
    - Protocole de transport (RTP/AVP, RTP/SAVP, UDP)
    - Format de media :
  - Titre du média : **« i*=… »**

3. Requêtes et réponses SIP

Protocole SDP – Exemples de corps de message

```
v=0
o=Jules 2890844527 2890844527 IN IP4 10.0.0.1
s=MusiqueFloyd
i=envoi du dernier tube de Floyd
c=IN IP4 10.0.0.1
t= 10xxx  11xxx
m=audio 4122 RTP/AVP 0 8
```

Un seul média

```
v=0
o=robert 2890844526 2890842807 IN IP4 10.47.16.5
s= Film SDP
i= Principaux concepts pour comprendre le protocole SIP
u=http://www.societe.com/cours/sdp.pdf
e=jean.pierre@societe.com (Jean Pierre)
c=IN IP4 224.2.17.12/127
t=2873397496 2873404696
m=audio 49170 RTP/AVP 0
m=video 51372 RTP/AVP 99
```

Deux médias

3. Requêtes et réponses SIP

Exemples de messages SIP avec entête et corps

Message de requête

```
INVITE sip:jules@a.com SIP/2.0
Via: ...
From: guy@b.com
To: sip:jules@a.com
Call-Id: 212@a.com
CSeq: 15 INVITE
Content-type: application/sdp
```

```
v=0
o= ...
c= IN IP4 x.a.com
m= audio 3456 RTP
m=video 4000 RTP
```

Message de réponse

```
SIP/2.0 200 OK
Via: ...
From: sip:jules@a.com
To: guy@b.com
Call-Id: 212@a.com
CSeq: 15 INVITE
Content-type: application/sdp
```

```
v=0
o= ...
c= IN IP4 x.a.com
m= audio 3456 RTP
m=video 0 RTP
```

Accepte l'audio et rejette la vidéo

4. Conclusion

Nouveaux marchés pour la téléphonie

- Beaucoup de fabricants d'équipements de téléphonie proposent des appareils compatibles SIP (i.e. SIP est intégré dans les appareils) : Nokia, Samsung…
- Les fabricants de passerelles et routeurs (Cisco, Nortel…) et les fabricants de serveurs intègrent SIP dans leurs produits
- Les fournisseurs d'accès à Internet intègrent aussi SIP
- Mise en place de PABX SIP dans les entreprises
  Simplifier la recherche des personnes au sein d'une entreprise (plus besoin de standardiste pour dire où se trouve X ou Y et si Z peut appeler X entre 15h et 16h…)

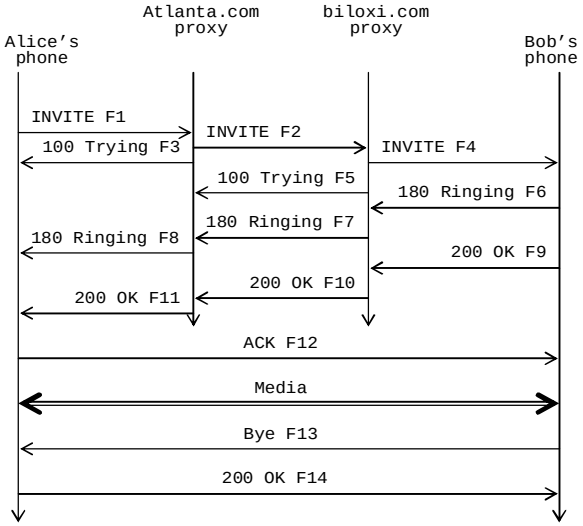
Téléphoner via Internet

4. Conclusion

Terminaux SIP

5. Exemple long (tiré du RFC 3261)

Diagramme des messages



5. Exemple long (tiré du RFC 3261)

F1 INVITE Alice -> atlanta.com proxy
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142
(Alice's SDP not shown)

F2 100 Trying atlanta.com proxy -> Alice
SIP/2.0 100 Trying
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
;received=192.0.2.1
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Content-Length: 0

F3 INVITE atlanta.com proxy -> biloxi.com proxy
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP bigbox3.site3.atlanta.com;
branch=z9hG4bK77ef4c2312983.1
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
;received=192.0.2.1
Max-Forwards: 69
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142
(Alice's SDP not shown)

F4 100 Trying biloxi.com proxy -> atlanta.com proxy
SIP/2.0 100 Trying
Via: SIP/2.0/UDP bigbox3.site3.atlanta.com;
branch=z9hG4bK77ef4c2312983.1;received=192.0.2.2
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
;received=192.0.2.1
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Content-Length: 0

5. Exemple long (tiré du RFC 3261)

F5 INVITE biloxi.com proxy -> Bob
INVITE sip:bob@192.0.2.4 SIP/2.0
Via: SIP/2.0/UDP server10.biloxi.com;branch=z9hG4bK4b43c2ff8.1
Via: SIP/2.0/UDP bigbox3.site3.atlanta.com;
branch=z9hG4bK77ef4c2312983.1 ;received=192.0.2.2
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
;received=192.0.2.1
Max-Forwards: 68
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142
(Alice's SDP not shown)

F6 180 Ringing Bob -> biloxi.com proxy
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP server10.biloxi.com; branch=z9hG4bK4b43c2ff8.1
;received=192.0.2.3
Via: SIP/2.0/UDP bigbox3.site3.atlanta.com;
branch=z9hG4bK77ef4c2312983.1;received=192.0.2.2
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
;received=192.0.2.1
To: Bob <sip:bob@biloxi.com>;tag=a6c85cf
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
Contact: <sip:bob@192.0.2.4>
CSeq: 314159 INVITE
Content-Length: 0

F7 180 Ringing biloxi.com proxy -> atlanta.com proxy
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP
bigbox3.site3.atlanta.com;branch=z9hG4bK77ef4c2312983.1
;received=192.0.2.2
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
;received=192.0.2.1
To: Bob <sip:bob@biloxi.com>;tag=a6c85cf
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
Contact: <sip:bob@192.0.2.4>
CSeq: 314159 INVITE
Content-Length: 0

F8 180 Ringing atlanta.com proxy -> Alice
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
;received=192.0.2.1
To: Bob <sip:bob@biloxi.com>;tag=a6c85cf
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
Contact: <sip:bob@192.0.2.4>
CSeq: 314159 INVITE
Content-Length: 0

5. Exemple long (tiré du RFC 3261)

F9 200 OK Bob -> biloxi.com proxy
SIP/2.0 200 OK
Via: SIP/2.0/UDP server10.biloxi.com;branch=z9hG4bK4b43c2ff8.1 ;received=192.0.2.3
Via: SIP/2.0/UDP bigbox3.site3.atlanta.com;branch=z9hG4bK77ef4c2312983.1 ;received=192.0.2.2
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8 ;received=192.0.2.1
To: Bob <sip:bob@biloxi.com>;tag=a6c85cf
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Contact: <sip:bob@192.0.2.4>
Content-Type: application/sdp
Content-Length: 131
(Bob's SDP not shown)

F10 200 OK biloxi.com proxy -> atlanta.com proxy
SIP/2.0 200 OK
Via: SIP/2.0/UDP bigbox3.site3.atlanta.com;branch=z9hG4bK77ef4c2312983.1 ;received=192.0.2.2
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8 ;received=192.0.2.1
To: Bob <sip:bob@biloxi.com>;tag=a6c85cf
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710 CSeq: 314159 INVITE
Contact: <sip:bob@192.0.2.4>
Content-Type: application/sdp
Content-Length: 131
(Bob's SDP not shown)

5. Exemple long (tiré du RFC 3261)

F11 200 OK atlanta.com proxy -> Alice
SIP/2.0 200 OK
Via: SIP/2.0/UDP pc33.atlanta.com;
branch=z9hG4bKnashds8 ;received=192.0.2.1
To: Bob <sip:bob@biloxi.com>;tag=a6c85cf
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Contact: <sip:bob@192.0.2.4>
Content-Type: application/sdp
Content-Length: 131
(Bob's SDP not shown)

F12 ACK Alice -> Bob
ACK sip:bob@192.0.2.4 SIP/2.0
Via: SIP/2.0/UDP
pc33.atlanta.com;branch=z9hG4bKnashds9
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>;tag=a6c85cf
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 ACK
Content-Length: 0

F13 BYE Bob -> Alice
BYE sip:alice@pc33.atlanta.com SIP/2.0
Via: SIP/2.0/UDP 192.0.2.4;branch=z9hG4bKnashds10
Max-Forwards: 70
From: Bob <sip:bob@biloxi.com>;tag=a6c85cf
To: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 231 BYE
Content-Length: 0

F14 200 OK Alice -> Bob
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.2.4; branch=z9hG4bKnashds10
From: Bob <sip:bob@biloxi.com>;tag=a6c85cf
To: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 231 BYE
Content-Length: 0

Chapitre 10

Représentation de données : Standards ASN.1 et XDR

1. Généralités

Hétérogénéité des systèmes informatiques

- **Diversité des processeurs** ➔ différentes représentations en mémoire des nombres

  - *Big-endian* : les octets sont numérotés de gauche à droite [0 1 2 3]

  Eg. Processeurs Motorola 68000, *Sun*

  - *Little-endian* : les octets sont numérotés de droite à gauche [3 2 1 0]

  Eg. Processeur X86

  Eg. La valeur Héxa 0xA0B70708 est stockée

	0	1	2	3	numéros des octets	
Big-endian :	A0	B7	07	08	MSB	LSB
Little-endian :	08	07	B7	A0	LSB	MSB

1. Généralités

Hétérogénéité des systèmes informatiques

- Diversité des langages de programmation
  - Entiers : Short, long, double…
  - Flottants : taille de l'exposant ? De la mantisse ?
  - Indices des tableaux : [0 .. 99], [1 .. 100], [-50 .. 49] ….
- Diversité des codes de caractères :
  - Codes ASCII (avec bit de parité, sans, sur 7+1 bits, 8+1 bits…)
  - Code UT8 (caractères chinois, japonais… tenant sur 1, 2, 3 ou 4 octets)
  - Autres codes (EBCDIC…)

1. Généralités

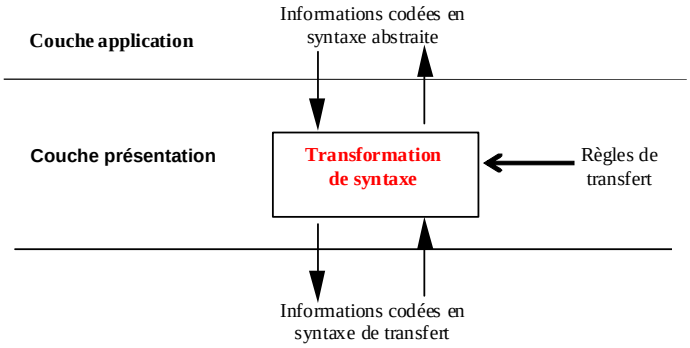
Hétérogénéité des systèmes informatiques

N*(N-1)/2 conversions (traduire par le client pour chaque serveur)

Impraticable si N est élevé (sinon il faudrait pour chaque application-réseau une version pour chaque serveur spécifique)

1. Généralités

Principe général d'une représentation commune



2. Services de Présentation

Services de la couche Présentation OSI

Primitive	Fonction	Mode
P-CONNECT	Etablissement de connexion de présentation	Confirmé
P-DATA	Emission de données normales	Non confirmé
P-EXPEDITED-DATA	Emission de données urgentes	Non confirmé
P-TYPED-DATA	Emission de données typées	Non confirmé
P-RELEASE	Libération de connexion de présentation	Confirmé
P-U-ABORT	Avortement de connexion par l'utilisateur	Non confirmé
P-P-ABORT	Avortement de connexion par le fournisseur de service	Non confirmé
P-P-EXCEPTION-REPORT	Notification d'anomalie par le fournisseur de service	Non confirmé
P-U-EXCEPTION-REPORT	Notification d'anomalie par l'utilisateur	Non confirmé
P-ALTER-CONTEXT	Gestion de contexte	Confirmé

2. Services de Présentation

Services de la couche Présentation OSI

Primitive	Fonction	Mode
P-TOKEN-GIVE	Passage de jeton	Non confirmé
P-TOKEN-PLEASE	Demande de jeton	Non confirmé
P-CONTROL-GIVE	Contrôle du jeton	Non confirmé
P-SYNC-MINOR	Pose de point de synchronisation mineure	Confirmé
P-SYNC-MAJOR	Pose de point de synchronisation majeure	Confirmé
P-RESYNCHRONIZE	Resynchronisation	Confirmé
P-ACTIVITY-START	Début d'activité	Non confirmé
P-ACTIVITY-RESUME	Reprise d'activité	Non confirmé
P-ACTIVITY-INTERRUPT	Interruption d'activité	Non confirmé
P-ACTIVITY-END	Fin d'activité	Confirmé
P-ACTIVITY-DISCARD	Annulation d'activité	Confirmé

Services mis directement en correspon-dance avec les services de Session de même noms.

2. Services de Présentation

Unités fonctionnelles de la couche Présentation OSI

- Unité fonctionnelle = moyen
  - de regrouper les services
  - d'implanter les services selon les besoins

- Unité *Noyau* (P-CONNECT, P-DATA, P-RELEASE, P-U-ABORT, P-P-ABORT)
- Unité *Gestion de contexte* (P-ALTER-CONTEXT)
- Unité *Négociation de libération de connexion* (P-RELEASE, P-TOKEN-GIVE, P-TOKEN-PLEASE)
- Unité *Half duplex* (P-TOKEN-GIVE, P-TOKEN-PLEASE)
- Unité *Données urgentes* (P-EXPEDITED-DATA)
- Unité *Données typées* (P-TYPED-DATA)
- Unité *Données de capacités* (P-CAPABILITY-DATA)

2. Services de Présentation

Unités fonctionnelles de la couche Présentation OSI

- Unité *Synchronisation mineure* (P-SYNC-MINOR, P-TOKEN-GIVE, P-TOKEN-PLEASE)
- Unité *Synchronisation majeure* (P-SYNC-MAJOR, P-TOKEN-GIVE, P-TOKEN-PLEASE)
- Unité *Synchronisation resynchronisation* (P-RESYNCHRONIZE)
- Unité *Synchronisation Exceptions* (P-U-EXCEPTION-REPORT, P-P-EXCEPTION-REPORT)
- Unité *Gestion d'activités* (P-ACTIVITY-START, P-ACTIVITY-RESUME, P-ACTIVITY-INTERRUPT, P-ACTIVITY-DISCARD, P-ACTIVITY-END, P-TOKEN-GIVE, P-TOKEN-PLEASE, P-CONTROL-GIVE)

3. Introduction à ASN.1

ASN.1 : c'est quoi ?

- ASN.1 : Abstract Syntax Notation #1
- Langage formel développé par ITU-T and ISO (norme internationale)
- Première norme en 1984 (CCITT X.409)
- Définition d'une structure générique de données indépendante de toute technique de codage et représentation de données
- Définition de types de données communs tenant compte des langages de programmation existants et futurs : permettre la définition de format de messages échangés entre entités distantes
- Définition de règles de codage des données (BER : basic encoding rules et PER : packet encoding rules) : permettre la représentation des messages en octets (ou bits) reconnaissables par les sites qui dialoguent

3. Introduction à ASN.1

Grands acteurs utilisant ASN.1

- Audio & Vidéo sur Internet
  AT&T, Intel, IBM, Microsoft, 3COM
- Commerce électronique
  American Express, GTE, MasterCard, VISA
- Téléphonie
  AT&T, MCI, Motorola, Nokia, Sprint
- Aviation
  FAA, ICAO
- Industrie automobile
  Ford, Mercedes Benz, Mitsubishi
- Gestion de réseaux
  Bull, Compaq, Hewlett-Packard, Sun
- Routeurs
  Bay Networks, Cisco, Racal, Xyplex

3. Introduction à ASN.1

Normes internationales

- ITU-T Rec. X.680 | ISO/IEC 8824-1 – Basic ASN.1 Notation
- ITU-T Rec. X.681 | ISO/IEC 8824-2 – Information Object Classes
- ITU-T Rec. X.682 | ISO/IEC 8824-3 – Constraints
- ITU-T Rec. X.683 | ISO/IEC 8824-4 – Parameterization
- ITU-T Rec. X.690 | ISO/IEC 8825-1
  Basic Encoding Rules (BER)
  Canonical Encoding Rules (CER)
  Distinguished Encoding Rules (DER)
- ITU-T Rec. X.691 | ISO/IEC 8825-2
  Packed Encoding Rules (PER)

3. Introduction à ASN.1

Eléments de base

- **Module**
- **Types de données**
- **Codage de données**

- **ASN.1 ➔ Règles syntaxiques à respecter**

3. Introduction à ASN.1

Concept de module ASN.1

```
<Nom_module> DEFINITIONS::=
BEGIN
  EXPORTS
  IMPORTS
  <ListeDefinitions>
END
```

```
Mod1 DEFINITIONS::=
BEGIN
  IMPORTS t1, t2;
  EXPORTS t3, t4;
  t3 ::= INTEGER ;
  t4 ::= SEQUENCE …
   …
END
```

- EXPORTS : spécifie les définitions exportées
- IMPORTS : spécifie les définitions importées d'autres modules
- ListeDefinitions : spécifie les définitions de types et macros

3. Introduction à ASN.1

Types ASN.1

- **Types de base**
  - BOOLEAN, INTEGER, REAL, ENUMERATED, NULL
  - BIT STRING, OCTET STRING, CHARACTER STRING, IA5STring, xxxString,
  - UTCTime /* Temps UTC et généralisé */
- **Constructeurs de types**
  - SEQUENCE : structure ordonnée de valeurs de types généralement différents (enregistrement “à la Pascal”)
  - SEQUENCE OF : liste ordonnée de 0 ou n valeurs de même type (c.à.d. tableaux dynamiques et listes).
  - SET : structure non ordonnée de valeurs de types généralement différents
  - SET OF : liste non ordonnée de valeurs de même type (eg. multi-ensemble)
  - CHOICE : sélection de parties alternatives

3. Introduction à ASN.1

Exemples de définition de types ASN.1

```
T_couleur ::= ENUMERATED {noir(0), marron(1), vert(3), bleu(4)} ;
T_age  ::= INTEGER (0..99);
T_num_telephone ::= SEQUENCE SIZE(10) OF INTEGER (0 .. 9)
User1 T_personne  ::= SEQUENCE {
        Nom    IA5String (SIZE(1..128)),
        Age     T_age,
        CouleurYeux T_couleur,
        Telephone T_num_telephone,
        Adresse IA5String OPTIONAL    }

T_tierce ::= SEQUENCE OF INTEGER  ; /* l'ordre d'arrivée est important */

T_ContenuFichier ::= CHOICE
          {  texte IA5String, binaire BIT STRING, Vide NULL } ;
T_coordonnees ::= SET { x INTEGER, y INTEGER, z INTEGER };
T_ensemble_points ::= SET OF T_coordonnees ;
```

3. Introduction à ASN.1

Exemples d'utilisation de types ASN.1

```
Couleur1 T_couleur ::= noir;
Age1 T_age ::= 25;
Tel1 T_num_telephone ::= {0, 5, 6, 1, 5, 5, 7, 2, 5, 6};

User1 T_personne ::= {"DUPONT", Age1, Couleur1, Tel1} }
User2 T_personne ::= {"MARCHAND", 29, vert,
   {0, 5, 6, 1, 2, 3, 4, 5, 6, 7},  "37 rue Jean-Jaures, Toulouse "} }

ArriveeTierce_du_jeudi_10mars T_tierce ::= {12, 9, 7}
ArriveeTierce_du_jeudi_12mars T_tierce ::= {}  // aucune arrivée

Point1 T_coordonnées ::= {10, 2, 3};
Point2 T_coordonnees ::= {0, 0, 0};
Point3 T_coordonnees ::= {0, 4, 5};
Forme1 T_ensemble_points ::= {Point1, Point2, Point3};
```


3. Introduction à ASN.1

Exemples de définition de types ASN.1

-- On considère un protocole de lecture de fichier à distance.

-- L'accès se fait via un nom et un mot de passe. Si la personne qui souhaite se connecter est inconnue ou bien si le système est occupé, un message de refus est renvoyé à cette personne.

-- Si le fichier existe, les données (sous forme de chaîne d'octets) sont envoyées au demandeur, sinon une erreur est signalée.

-- A la fin de transfert, une demande de déconnexion est envoyée et cette demande est acquittée.

-- Les deux messages liés à la phase de déconnexion ne contiennent aucune informations, leur présence suffit au protocole.

-- Les types nécessaires à ce protocole sont décrits en ASN.1 et placés dans un module appelé M_AccesFichier.

3. Introduction à ASN.1

Exemples d'utilisation de types ASN.1

```
M_AccesFichier DEFINITIONS ::= BEGIN
   AccesSimpleFichier ::= CHOICE
        {  SeConnecter         PDUConnexion,
           ResultatConnexion   PDUResultatConnexion,
           SeDeconnecter       PDUDeconnexion,
           AckDeconnexion      PDUAckConnexion,
           ObtenirFichier      PDUDemandeFichier,
           ResultatFichier     PDUResultatFichier} ;
 PDUConnexion ::= SEQUENCE {nom IA5String, Mot_passe IA5String} ;
 PDUResultatConnexion ::= CHOICE  { Acceptee IA5String,
                       Rejetee INTEGER {AccesInvalide(0), SystemeOccupe(1)}} ;
 PDUDeconnexion ::= NULL ; -- PDU sans informations
 PDUAckConnexion ::= NULL ; -- PDU sans informations
 PDUDemandeFichier ::= IA5String ; -- Nom de fichier
 PDUResultatFichier ::= CHOICE
  { Fichier SEQUENCE { NomFIchier IA5String, ContenuFichier OCTET STRING},
   Erreur INTEGER {NonTrouve(0), FichierOccupe(1)}} ;
END
```


3. Introduction à ASN.1

Tags de types ASN.1

- A chaque type utilisé dans un module ASN.1 est associée (souvent par défaut) une étiquette (tag) permettant le décodage du type par le récepteur sans ambiguïté. La classe de tag permet de déterminer le domaine de visibilité dans lequel toutes les étiquettes doivent être uniques.
- `<Tag > ::= "[" [<classe de tag>] <nombre> "]"`

Quatre classes de tags

- **UNIVERSAL** : type d'usage général défini au niveau ISO, ITU… C'est pris par défaut quand aucun tag n'est spécifié. C'est la plus utilisée.
- **Spécifique à un contexte** : le domaine de visibilité est celui du constructeur (SEQUENCE, SET ou CHOICE) qui englobe le type à tagger. Cette classe est indiquée par « vide » et c'est la valeur par défaut, quand rien n'est indiqué comme classe avant le numéro du tag.
- **Deux classes très peu utilisées dans la pratique:** **APPLICATION** (utilisée pour une d'application donnée), **PRIVATE** (utilisée pour un utilisateur donné, une organisation donnée, un métier donné, un pays particulier…)

3. Introduction à ASN.1

Tags de types ASN.1

<Universal tags> ::= "[" UNIVERSAL <nombre> "]"

1 : BOOLEAN	2 : INTEGER	3 : BIT STRING	4 : OCTET STRING
5 : NULL	6 : OBJECT IDENTIFIER		7 : ObjectDescriptor
8 : EXTERNAL	9 : REAL	10 : ENUMERATED	16 : SEQUENCE, SEQUENCE OF
17 : SET, SET OF	18 : NumericString	19 : PrintableString	20 : TeletexString, T61String
21 : VideotexString	22 : IA5String	23 : UTCTime	24 : GeneralizedTime
25 : GraphicString	26 : VisibleString	27 : GeneralString	
28 : UniversalString	29 : CHARACTER STRING		30 : BMPString

```
Poids Real;     /*est équivalent à      Poids [UNIVERSAL 9] REAL;

/* Utilisation de tags spécifiques au contexte  */
FinRepas  ::= Choice { fromage [0] IA5String,
                       dessert [1] IA5String }
```


3. Introduction à ASN.1

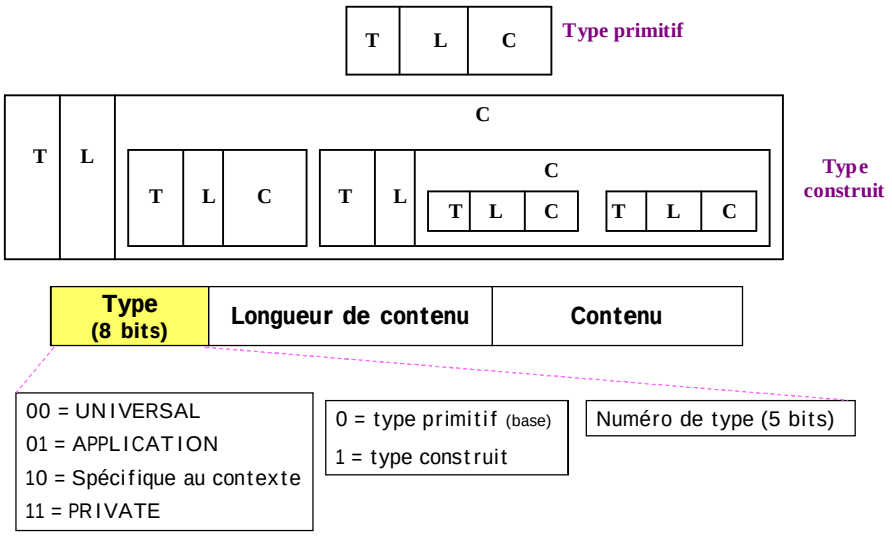
Syntaxes de transfert

- Codage : séquence d'octets représentant une valeur d'un type
- Syntaxe de transfert : forme avec laquelle les informations sont échangées entre applications
- Règles de codage : règles utilisées pour le codage propres à chaque syntaxe de transfert
- Autres fonctions des syntaxes de transfert : compression, chiffrement…

- **Deux syntaxes de transfert**
  - BER (basic encoding rules)
  - PER (packet encoding rules)

3. Introduction à ASN.1

Syntaxe de transfert de base : BER



3. Introduction à ASN.1

Syntaxe de transfert de base : BER

- **Forme primitive employée pour**
  - BOOLEAN, INTEGER, REAL, NULL, OBJECT IDENTIFIER,
  - ENUMERATED (*), BIT STRING (*), OCTET STRING (*)
  - Chaînes de caractères : NumericString, PrintableString, TeletexString, T61String, VideotexString, IA5String, GraphicString, VisibleStringn, GeneralString, : UniversalString, CHARACTER STRING, BMPString (*)
  - UTCTime, GeneralizedTime

  (*) peut dans certains cas être codé sous forme construite

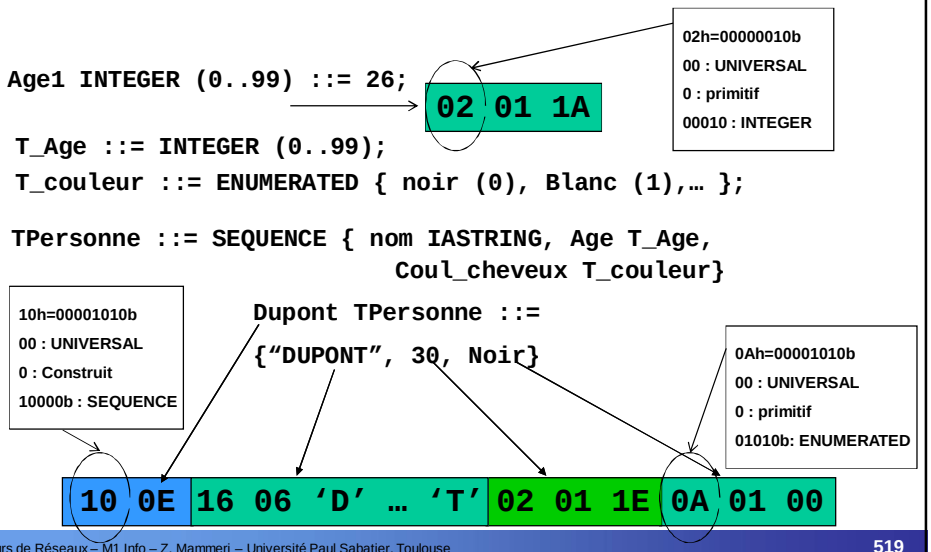
- **Forme construite (ou récursive)**

  SEQUENCE, SEQUENCE OF, SET, SET OF

- **Champ longueur (L)**
  - Courte (<128) : sur 1 octet, premier bit de l'octet = 0 suivi de la taille sur 7 bits
  - Longue (>128) : sur n octets dont le premier contient '1' suivi du nombre d'octets pour coder la taille et la taille elle-même sur n-1 octets.

3. Introduction à ASN.1

Exemples de codage par la BER



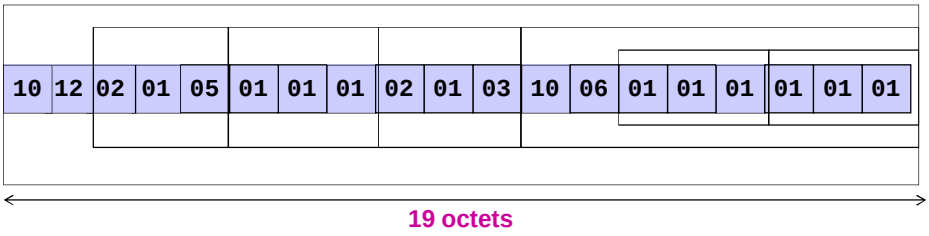
3. Introduction à ASN.1

Syntaxe de transfert par codage compact : PER

- **Inconvénients de la BER**

  Un surcoût important (le champs type et taille représentent 50% des infos transmises en moyenne)

```
v SEQUENCE {a INTEGER (0..7), b BOOLEAN, c INTEGER (0..3),
            d SEQUENCE {d1 BOOLEAN, d2 BOOLEAN }}
          ::= {5, TRUE, 3, {TRUE, TRUE}}
```



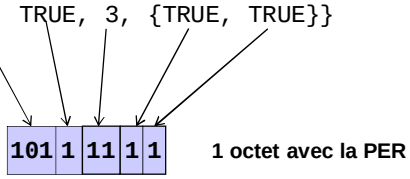
3. Introduction à ASN.1

Syntaxe de transfert par codage compact : PER

- **Apports de la PER (Packet Encoding Rules)**

  Gain de bande passante (en limitant la taille de l'info transmise)

```
v SEQUENCE {a INTEGER (0..7), b BOOLEAN, c INTEGER (0..3),
    d SEQUENCE {d1 BOOLEAN, d2 BOOLEAN }} ::=
            {5, TRUE, 3, {TRUE, TRUE}}
```



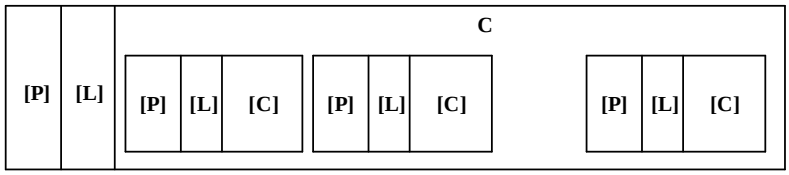
1 octet avec la PER

- **PER utilise le codage IMPLICITE** (contrairement à la BER qui utilise le codage EXPLICITE)

3. Introduction à ASN.1

Syntaxe de transfert par codage compact : PER

- **Format de codage PER**
  - Au lieu du codage TLC (Type, Longueur, Contenu) de la BER, on utilise le codage [P][L][C] (éventuellement un préambule, éventuellement une longueur et éventuellement un contenu)
  - Les étiquettes ne sont pas transmises
  - La longueur n'est indiquée que si elle n'est pas déduite de SIZE ou autre
  - On produit une chaîne de bits optimisée et alignée sur frontière d'octet.
  - L'optimisation nécessite une attention lors de la spécification des types : on doit utiliser les contraintes de sous-typage (avec SIZE…)



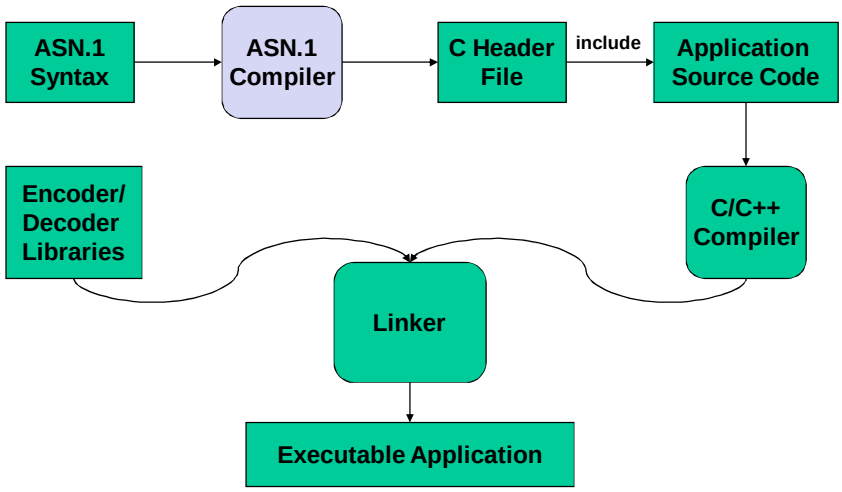
3. Introduction à ASN.1

Syntaxe de transfert par codage compact : PER

- **Codage d'entier borné par la PER**
  - Un nombre entier N ∈ [Min.. Max]
  - N peut prendre Max – Min valeurs différentes
  - Au lieu de coder la valeur de N, on code sa différence par rapport à Min.
  - Le nombre de bits pour coder la différence est toujours plus petit que celui pour coder une valeur
- **Codage d'entier semi borné par la PER**
  - Un nombre entier N ∈ [Min, ∞]
  - La valeur de $\lceil Log_{256}(N- Min) \rceil$ est codée sur un nombre minimum d'octets dont la longueur est spécifiée dans l'infos transmise
- **Codage d'autres formes d'entier**

3. Introduction à ASN.1

Workflow de développement sous ASN.1



4. Introduction à XDR

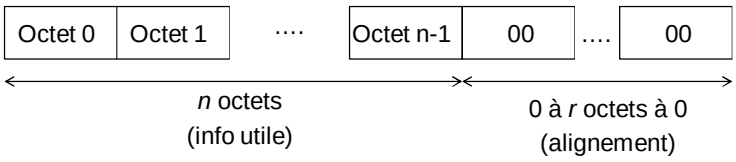
XDR en bref

- XDR : eXternal Data Representation
- Protocole introduit par *Sun Microsystems* pour être utilisé avec RPC
- XDR est devenu un standard de l'IETF (RFC1832 en 1995 màj par RFC 4506 en 2006)
- Aujourd'hui XDR est un standard de facto dans Internet
- XDR propose des types et constructeurs de type équivalents à ceux de ASN.1
- Le codage de XDR s'apparente au codage PER (codage implicite) : l'émetteur et le récepteur disposent des mêmes fichiers entêtes contenant les types utilisés.
- XDR est plus performant que ASN.1+BER
- XDR est moins performant que ASN.1+PER (car avec XDR toute valeur, y compris le booléen, est codée sur 32 bits !)

4. Introduction à XDR

Règle générique de codage en XDR

- Toute valeur est codée sur un nombre d'octets multiple de 4
- Représentation en *Big-endian* (MSB …. LSB)



n octets
(info utile)

0 à *r* octets à 0
(alignement)

$n + r = 0 \bmod 4$ et $0 \leq r \leq 3$

4. Introduction à XDR

Types de valeurs en XDR

- **Types simples**

Type	Nombre d'octets
int	**4**
unsigned int	**4**
hyper int	**8**
hyper unsigned int	**8**
float	**4**
double	**8**
quadruple	**16**
bool	**4**
enum {}	**4**

4. Introduction à XDR

Types de valeurs en XDR

- **Types structurés**

Type	Nombre d'octets	Description
opaque	***n+r***	Chaîne de n octets avec alignement
string	***n+r***	Chaîne de n caractères avec alignement
array	***n*s +r***	Tableau de n éléments s avec alignement s : taille d'élément
struct		enregistrement
union switch … case		Sélection (choice)
void	**0**	Élément vide
const	***n***	Constante

↑

n fixe ou variable

4. Introduction à XDR

XDR en bref

```
const foo = 1000;
struct square_in {
  long  foo1;
  opaque foo2[200];
  opaque foo3<300>;
  int foo4[400];
  int foo5<500>;
};
```

test.x

rpcgen

```
#ifndef _TEST_H_RPCGEN
#define _TEST_H_RPCGEN
#define RPCGEN_VERSION  199506
#include <rpc/rpc.h>
#define foo 1000
struct square_in { long foo1;
      char foo2[200];
      struct { u_int foo3_len;
         char *foo3_val; } foo3;
      int foo4[400];
      struct { u_int foo5_len;
            int *foo5_val; } foo5; };
....
```

test.h

4. Introduction à XDR

Exemple d'utilisation de XDR

- Description de fichier simple

```
const MAXUSERNAME = 32;      /* Longueur maxi du nom d'utilisateur */
const MAXFILELEN = 65535;    /* Taille maxi de fichier */
const MAXNAMELEN = 255;      /* Longueur maxi de nom de fichier */
     enum typedecontenu { TEXT = 0, /* Fichier ASCII */
          DATA = 1, /* Données brutes */ EXEC = 2 /* Fichier exécutable */ };
/* Informations additionnelles selon le type de fichier */
union typefichier switch (typedecontenu genre) {
     case TEXT: void;      /* Pas d'informations supplémentaires */
     case DATA: string createur<MAXNAMELEN>; /* Créateur de données */
     case EXEC: string interpreteur<MAXNAMELEN>; /*
       interpréteur de programme */ };
   struct file {/* structure de fichier */
     string nomfichier <MAXNAMELEN>; /* nom de fichier  */
     typefichier type;               /* type de fichier */
     string proprietaire <MAXUSERNAME>; /* propriétaire du fichier */
          opaque contenu <MAXFILELEN>;      /* contenu du fichier */
     };
```

4. Introduction à XDR

Exemple d'utilisation de XDR

- **Soit un utilisateur "Jean" qui a un fichier nommé "progmJava " contenant un programme Java erroné qui contient un seul mot "(quit)".**
- **Ce fichier peut être codé à l'aide de 48 octets :**

Offset	Octets en Hexa	ASCII	Commentaires
0	00 00 00 09	....	-- Longueur du nom de fichier = 9
4	73 69 6c 6c	prog	-- Nom du fichier
8	79 70 72 6f	mJav	-- .....
12	67 00 00 00	a...	-- ... complété par 3 octets à 0
16	00 00 00 02	....	-- Type de fichier est EXEC = 2
20	00 00 00 04	....	-- Longueur de l'interpréteur = 4
24	6c 69 73 70	Java	-- nom de l'interpréteur
28	00 00 00 04	....	-- longueur du propriétaire = 4
32	6a 6f 68 6e	Jean	-- nom du propriétaire
36	00 00 00 06	....	-- longueur des données du fichier = 6
40	28 71 75 69	(qui	-- octets de données du fichier
44	74 29 00 00	t)..	-- ... complétés par 2 octets à 0

Chapitre 11

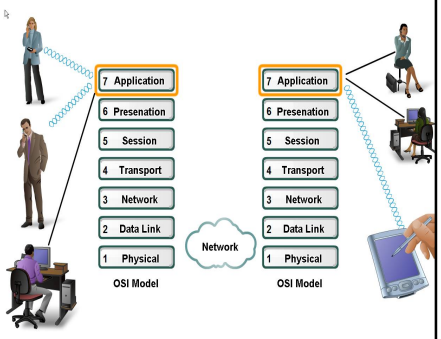
Couche Application

Concepts communs

1. Généralités

Rôles de la couche Application

- Couche Application = source et destination finales de toutes les données échangées entre utilisateurs (humains ou machines)
- C'est la couche qui fournit les interfaces pour la communication entre les utilisateurs
- Elle spécifie les formats des messages échangées entre processus d'application
- Elle ne fournit pas les règles d'implantation



1. Généralités

Classes d'applications

- Grand public
  - E-mail
  - Web
  - Messagerie instantanée
  - Partage de fichier (P2P…)
  - Jeux en réseau
  - Vidéo à la demande
  - Streaming vidéo
  - VoIP (téléphonie)
  - Vidéoconférence
  - Visioconférence
- Informatique pour informaticiens
  - Utilisation de terminal distant
  - Transfert de fichiers
  - Système de fichier réparti
  - Répertoire réseau
  - Gestion de réseau
- Spécialisées
  - Bourse, téléachat, publicité
  - Santé
  - Transport, embarqué
  - Nucléaire, industrie
  - Météo
  - Calcul scientifique

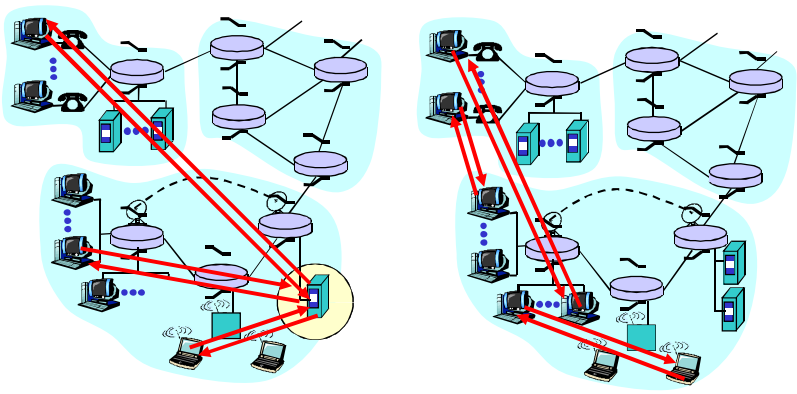
1. Généralités

Architectures et contrôle des applications

- Architectures (point de vue possession des données/ressources)
  - Client-serveur
    - Passage 'obligé' par une entité connue/fixe (le serveur) qui stocke les ressources/données
    - Avantage : simplicité d'utilisation et de gestion
    - Inconvénient : difficulté de passage à l'échelle
  - Pair à pair (P2P)
    - Chaque nœud est client et serveur à la fois
    - Avantage : décentralisation totale (bonne *scalability)*
    - Inconvénient : difficulté de gestion (localisation et synchronisation)
  - Hybride
    - Certaines fonctions gérées en CS et d'autres en P2P
    - Exemples
      - *Napster* (recherche de fichier centralisée et transfert de fichier décentralisé)
      - *Instant messaging* (chat décentralisé et localisation centralisée des usagers)

1. Généralités

Architectures et contrôle des applications



Client-serveur P2P

1. Généralités

Concernant les serveurs

- Confusion/ambiguïté
  - Serveur = machine qui offre un service (des services)
  - Serveur = processus d'application qui offre un service (des services)
- Serveur ➔ un démon pour accepter les requêtes des clients
- Problèmes liés à la conception de serveur
  - Conception de contenu et ergonomie associée
  - Mise en œuvre des fonctions requises par les clients
  - Tolérance aux fautes du serveur (redondance…)
  - Dimensionnement (analyse de performances) : quelles quantités de ressources logicielles et matérielles sont nécessaires ?
  - Gestion de la sécurité (authentification, cryptage…)
  - …

1. Généralités

Architectures et contrôle des applications

- Contrôle
  - Centralisé
    - Avantage : simplicité de gestion du contrôle
    - Inconvénient : pas/peu de tolérance aux fautes
  - Réparti/décentralisé
    - Avantage : tolérance aux fautes
    - Inconvénient : complexité de gestion
  - Hybride (mixte)
    - Certains aspects sont gérés en centralisé, d'autres en réparti

1. Généralités

Compétences requises pour la conception des applications

Les standards/normes ne disent pas comment implanter les applications Réseau.

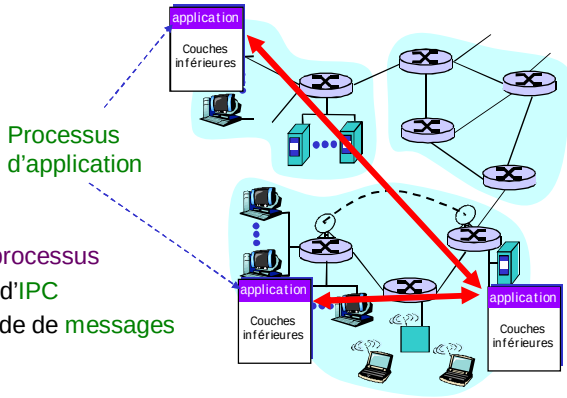
Les concepteurs doivent avoir des compétences autres que celles en Réseaux.

- Systèmes d'exploitation : Gestion des IT logicielles et matérielles, Gestion de processus, Synchronisation
- Gestion de données : SGF, SGBD
- Sécurité
- Tolérance aux fautes et pannes
- IA et algorithmique avancée
- Ordonnancement et équilibrage de charge
- Ergonomie et Compétences-métier
- Autres …..

1. Généralités

Structure générale de la couche Application

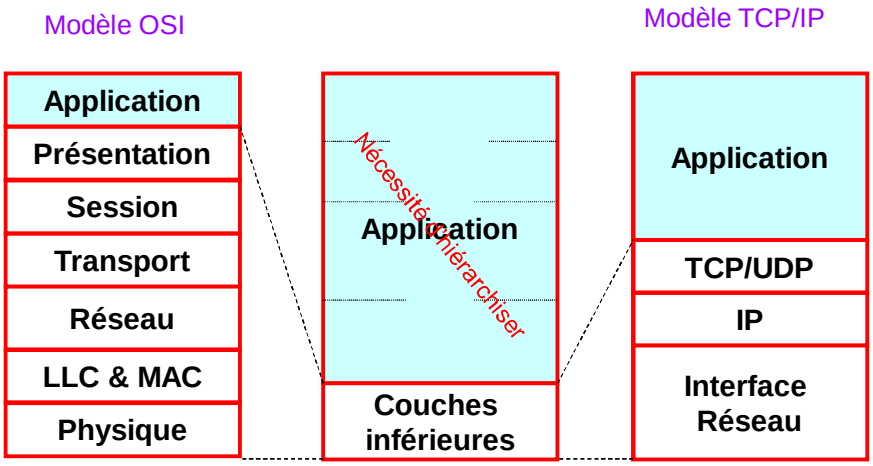
- Application répartie/distribuée
  - = Application fonctionnant sur un réseau = Application Réseau
  - = Ensemble de processus d'application qui communique/coopère



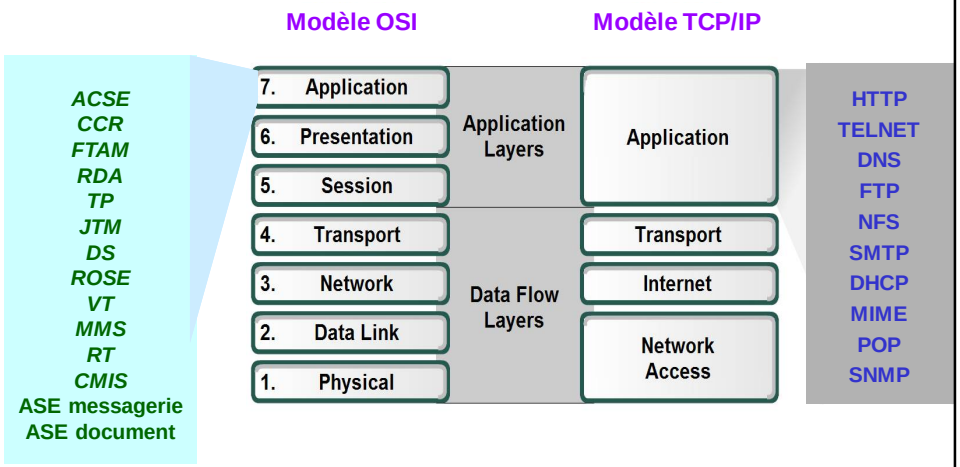
- Communication inter-processus
  - En local : à l'aide d'IPC
  - A distance : à l'aide de messages

2. Couche Application dans les modèles ISO et TCP/IP

Inadéquation des modèles à 7 et 5 couches

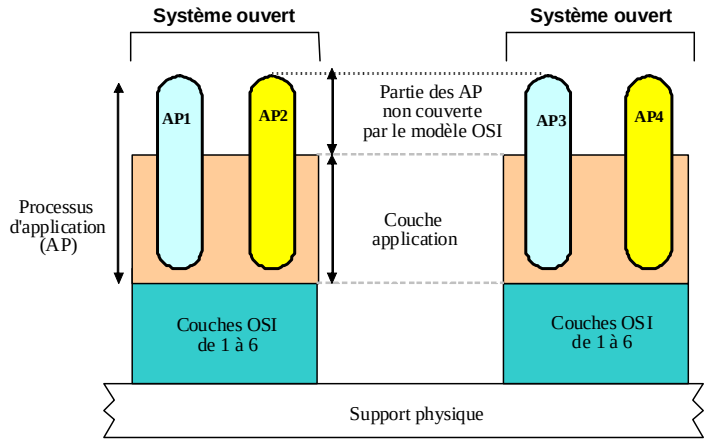


2. Couche Application dans les modèles ISO et TCP/IP



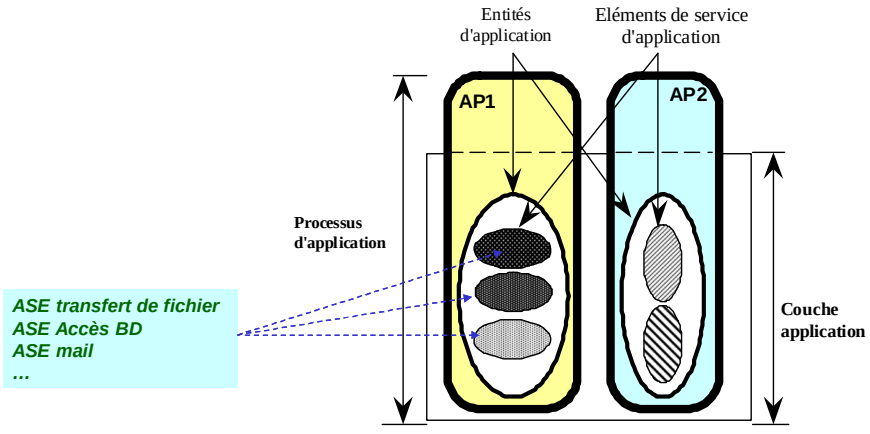
2. Couche Application dans les modèles ISO et TCP/IP

Structure générale de la couche Application selon la norme ISO 9545



2. Couche Application dans les modèles ISO et TCP/IP

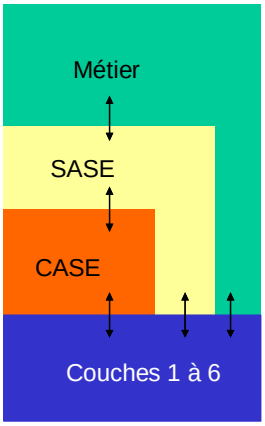
Structure générale de la couche Application selon la norme ISO 9545



2. Couche Application dans les modèles ISO et TCP/IP

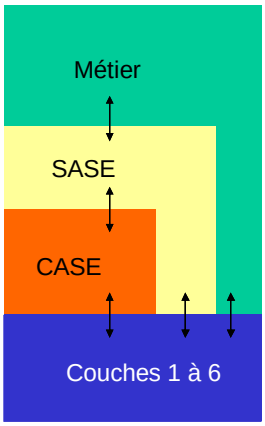
Hiérarchisation des protocoles de niveau Application

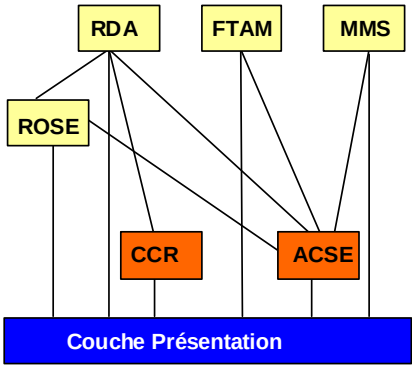
- CASE : *Common application service elements*
  - ACSE, CCR, ROSE, RT
- SASE : *Specific application service elements*
  - *RT*, *FTAM*, CMIS, *RDA, TP*, *JTM*, *DS*, *ROSE*, *VT*, *MMS*
  - ASE orientés messagerie, ASE orientés documents
- Autres :
  - A définir par métier/corporation…



2. Couche Application dans les modèles ISO et TCP/IP

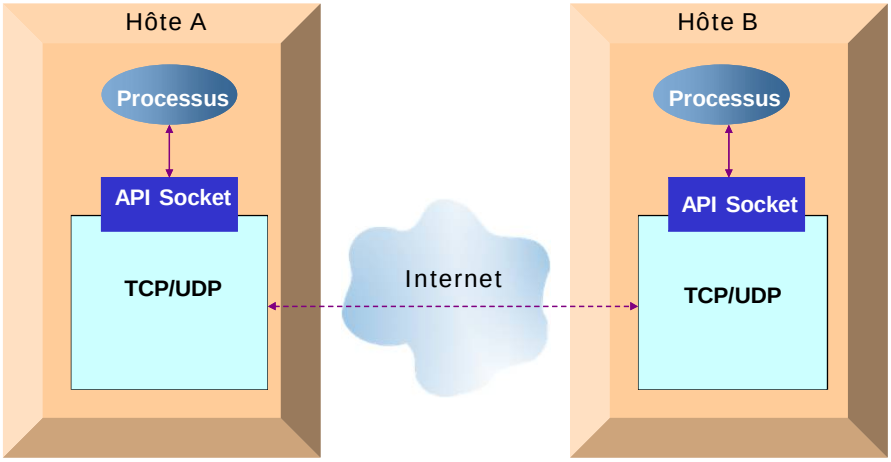
Exemple de liens entre services ISO



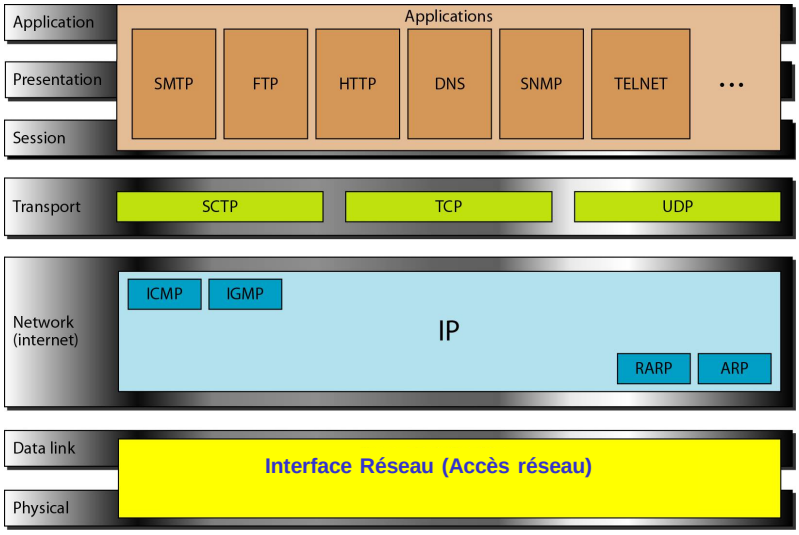


2. Couche Application dans les modèles ISO et TCP/IP

Vue/architecture simplifiée selon le modèle TCP/IP



2. Couche Application dans les modèles ISO et TCP/IP



2. Couche Application dans les modèles ISO et TCP/IP

Applications et protocoles d'application typiques dans Internet

Application	Protocole d'application	Protocole de transport
e-mail	SMTP [RFC 821]	TCP
Accès distant à un terminal	TELNET [RFC 854]	TCP
Web	HTTP [RFC 2068]	TCP
Transfert de fichier	FTP [RFC 959]	TCP
Streaming multimédia	Propriétaire (e.g. RealNetworks)	TCP ou UDP
Serveur de fichier distant	NFS	TCP ou UDP
Téléphonie sous IP	Propriétaire (e.g., Vocaltec, Skype)	Typiquement UDP