iutenligne

Le catalogue de ressources pédagogiques
de l'enseignement technologique universitaire.

I.U.T. de Mulhouse – G.E.I.I.

RES3 - Réseaux

CM 6 – TD 5 :
Réseaux Wireless
Réseau Wifi

IUT Institut Universitaire de Technologie de Mulhouse

Planning

- *CM 1 : Généralités Réseaux*
- *CM 2 : Topologie et supports de transmission*
  - *TD 1 : Débit et technologie ADSL*
- *CM 3 : Codage des informations et contrôle d'intégrité*
  - *TD 2 : Codage des informations et contrôle d'intégrité CRC*
- *CM 4 : Modèle OSI / Ethernet*
- *CM 5 : Couches transport et réseau (TCP/IP)*
  - *TD 3 : Analyse de trames Ethernet / Adresse IP et masque de sous-réseaux*
  - *TD 4 : Adressage IP / Routage IP*
- **CM 6 : Réseaux WLAN et sécurité**
  - TD 5 : Réseaux Wifi et sécurité
- CM 7 : Réseaux et bus de terrain
  - TD 6 : Réseaux et bus de terrain
    - TP 1 : Technologie ADSL
    - TP 2 : Analyse de trames et Encapsulation Ethernet
    - TP 3 : Configuration d'un réseau IP / Routage IP / Wifi
    - TP 4 : Réseaux et bus de terrain
    - TP 5 : TP Test
- CM 8 : Contrôle de connaissances

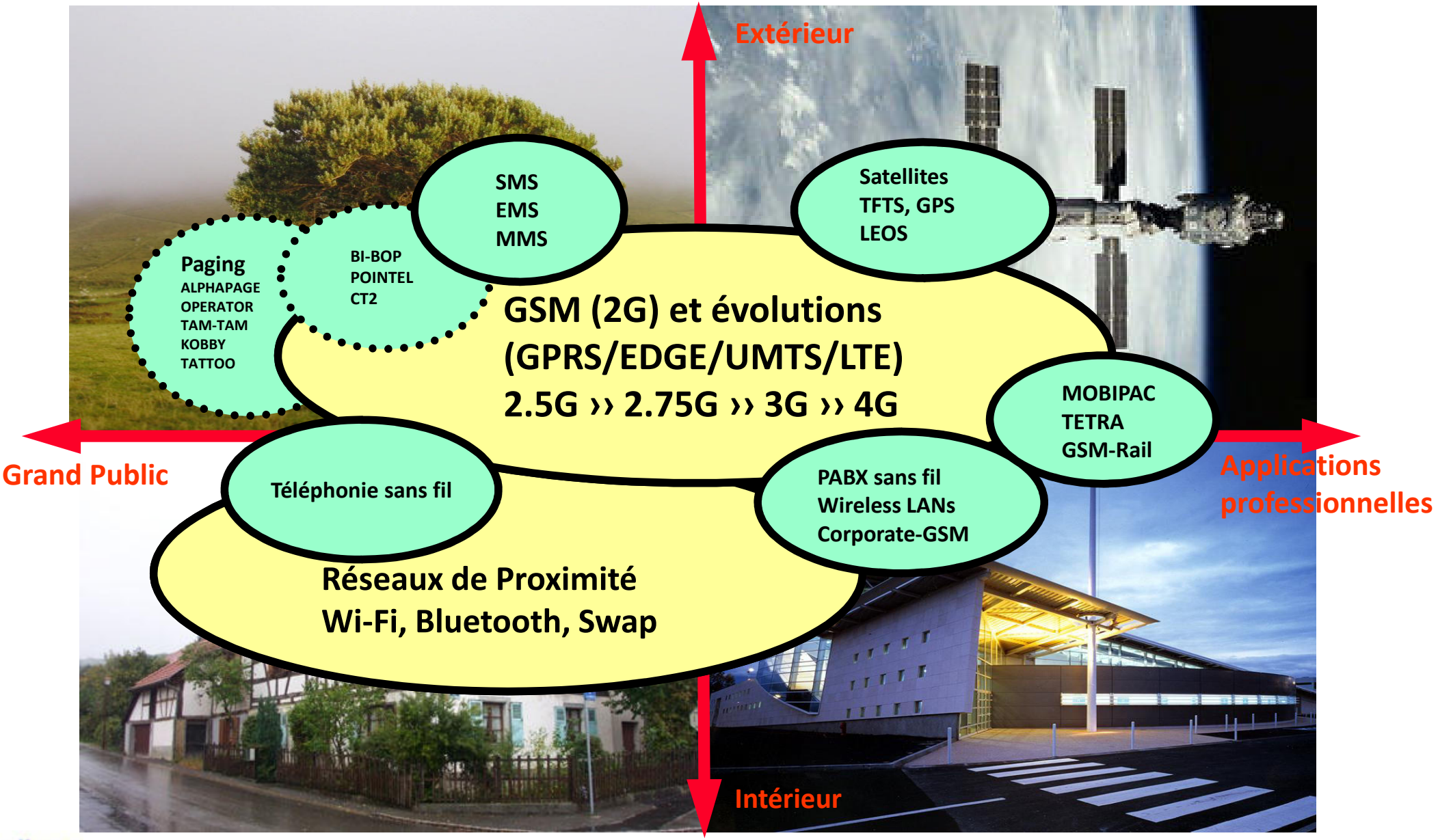
Jean-François ROTH
Enseignant Vacataire IUT de Mulhouse
Formateur/Consultant en réseaux et télécoms depuis 1999
Jean-Francois.ROTH@UHA.fr
JeanFrancoisROTH@MSN.com

Sommaire

- Réseaux Wireless
  - Réseaux sans-fil et mobiles
    - Introduction
  - Panorama des réseaux mobiles
    - Réseaux 1G
    - Réseaux satellites
    - Réseaux 2G
      - GSM
    - Réseaux 2.5G/2.75G
      - GPRS/EDGE
    - Réseaux 3G
      - UMTS
    - Réseaux 4G
      - LTE et LTE Advanced
    - Evolutions
  - Réseau Wifi
      - Introduction à la norme 802.11
      - Fonctionnement
      - Sécurité
      - Wifi vs Bluetooth

- Introduction
  - Définition d'un réseau sans-fil (Wireless LAN ou WLAN)
    - Réseau où au moins deux terminaux se connectent et communiquent entre eux par voie hertzienne, directement ou indirectement, en permettant un déplacement du terminal
  - La préhistoire…
    - Réseaux 1G : téléphonie sans fil et réseaux de pagging
  - Hier…
    - Réseaux 2G : GSM (Global System for Mobile communications)
    - Réseaux 2.5G : GPRS (General Packet Radio System)
    - Réseaux 2.75G : EDGE (Enhanced Data Rates for Global Evolution)
  - Aujourd'hui…
    - Réseaux satellites
    - Réseaux 3G : UMTS (Universal Mobile Telecommunications System)
    - Réseaux sans-fil: Wifi, WiMax, Bluetooth, …
    - Réseaux 4G : LTE (Long Term Evolution)
  - Demain….
    - Réseaux 4G : LTE Advanced

Panorama des réseaux mobiles



Panorama des réseaux mobiles

- Réseaux 1G : téléphonie sans fil
  - Service de téléphonie dans une zone réduite
  - Applications
    - Poste domestique (résidentiel)
    - Réseau public de quartier : service télépoint, POINTEL, BI-BOP, TELEPOINT
      - Remplacé par la téléphonie mobile
    - PABX sans fil (entreprise)
  - Limitations
    - Usage résidentiel seulement
    - Modulation analogique
    - Pas de transmission de données
    - Fréquences limitées (20 - 40mhz)
- Réseaux 1G : réseaux de pagging
  - Réception de messages courts sur un terminal mobile
    - Alphapage, Eurosignal, Tam-tam, Tatoo, Kobby, Textnet....
    - Environ 1,7 millions d'utilisateurs au total fin 97… plus rien en 2000 !
      - Remplacé par la téléphonie mobile (SMS/MMS)

Panorama des réseaux mobiles

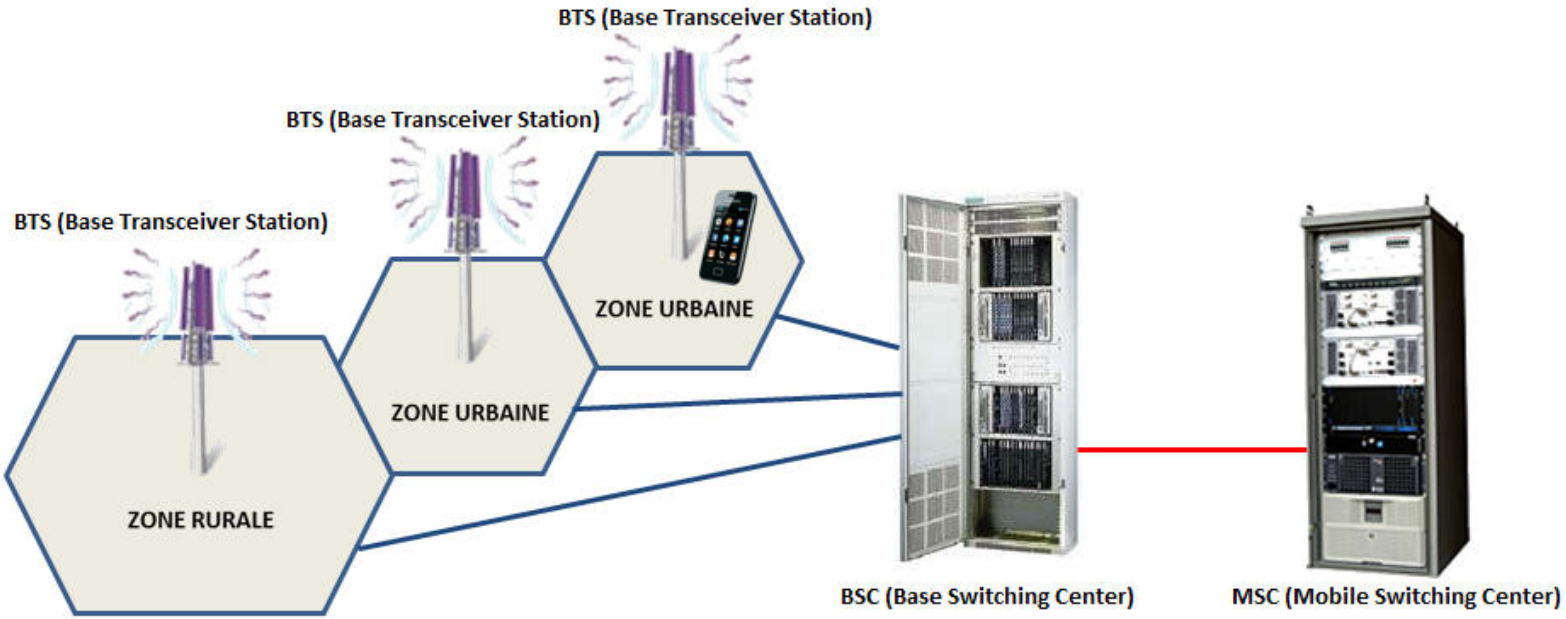
- Réseaux satellites
  - GEOS (Geostationary Earth Orbital Satellite)
    - Orbite géostationnaire : 35786 km
    - Temps aller-retour de l'onde radio : ~260ms
    - Utilisation : domaine de la diffusion vidéo et de l'accès à l'Internet, satellites météorologiques
    - Avantage : maintient de la position fixe dans le ciel
      - Une station au sol est en permanence dans la zone de couverture du satellite
    - Inconvénients : altitude élevée entrainant un temps de latence du signal aller-retour considérable et un satellite géostationnaire n'est plus visible au dessus d'une latitude de 70°
  - MEOS (Medium Earth Orbital Satellite)
    - Orbite : de 2000 à 35000 km
    - Temps aller-retour de l'onde radio : ~ 100ms
    - Possibilité d'ajuster les caractéristiques des orbites en fonction de l'utilisation du satellite
    - Utilisation : GPS (Global Positioning System) avec des orbites de l'ordre de 20000 km d'altitude
  - LEOS (Low Earth Orbital Satellite)
    - Orbite : de 200 à 2000 km
    - Temps aller-retour de l'onde radio : inférieur à 10ms
    - Utilisation : Globalstar (téléphonie), Irridium (utilisé par des agences de l'ONU)

Panorama des réseaux mobiles

- Réseaux 2G : GSM
  - Global System for Mobile Communications
    - Système public de communications mobiles européen mis en place début des années 90
    - Caractéristiques
      - Bonne qualité de transmission de la parole sans perte de signal lors de la mobilité (Handover)
      - Coûts des terminaux et services associés le plus bas possible
      - Faible consommation
      - Possibilités de Roaming International
    - Réseau basé sur une architecture en cellules
      - Macro Cellules
        - Zones à population dispersée (diamètre de 10 à 30km) : voiture, train,….
      - Micro Cellules
        - Zones à population très denses (diamètre de 100 à 300m); Usage: piétons
        - Permet l'optimisation des canaux de transmission et une meilleure précision de localisation
      - Pico Cellules
        - Réservé aujourd'hui aux réseaux de proximité (> 10m)
        - Concept repris dans l'UMTS
      - Cellules sélectives
        - Les cellules n'ont pas toujours besoin d'une couverture de 360 degrés
      - Cellules "parapluie"
        - Regroupement de cellules pour éviter un nombre trop important de commutations entre cellules

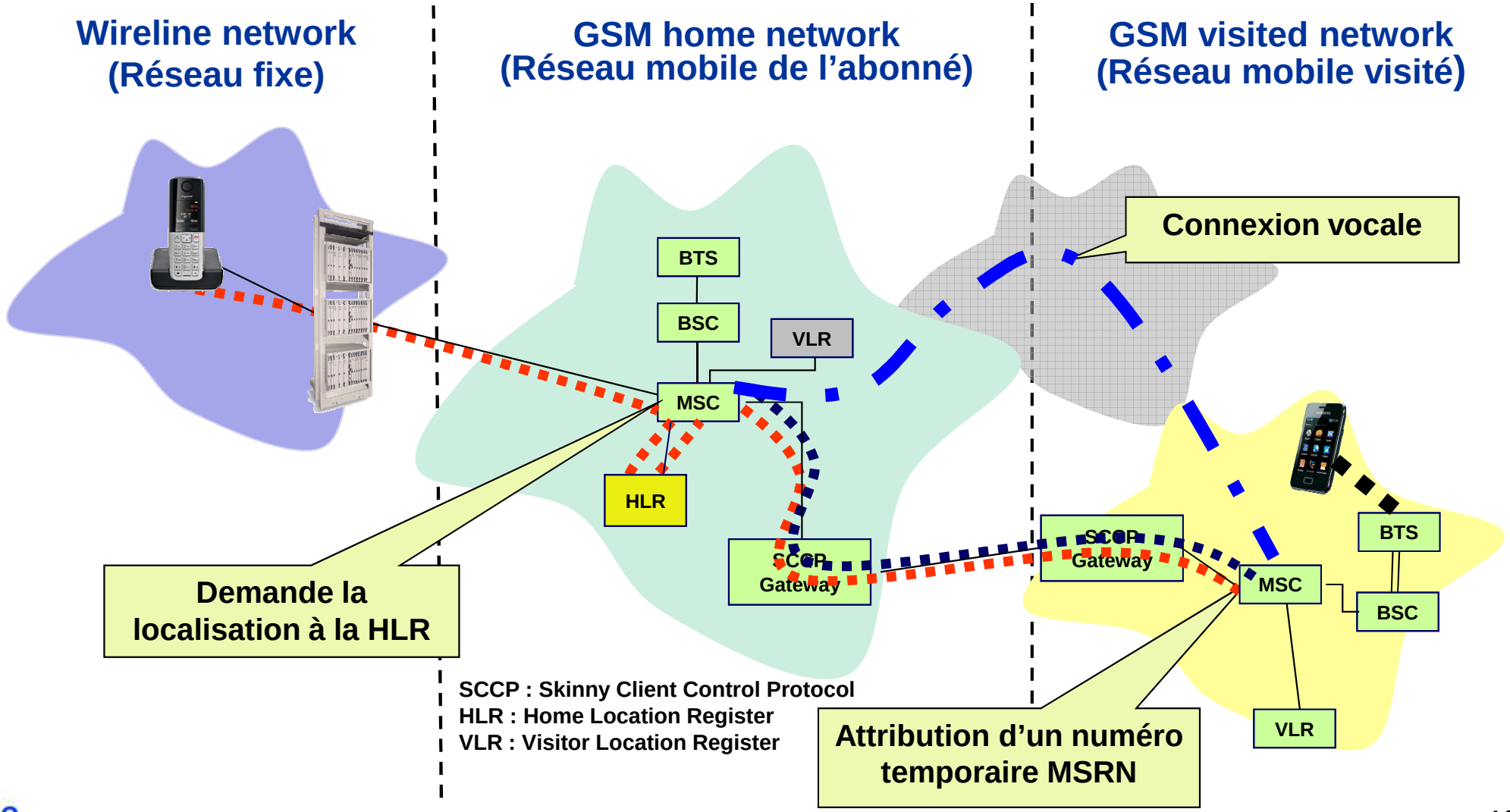
Panorama des réseaux mobiles

- Réseaux 2G : GSM
  - Fonctionnalités associées
    - La mobilité
      - Mécanisme permettant de déplacer l'accès au réseau en fonction de la position de l'utilisateur….
    - Le handover
      - Mécanisme permettant le transfert automatique d'une transaction en cours d'une cellule vers une cellule, sans perturber la communication en cours
    - Le roaming
      - Mécanisme permettant d'offrir les mêmes services de télécommunications mobiles à des clients (ou roamers) abonnés à d'autres réseaux ou dans d'autres pays (roaming international)



Panorama des réseaux mobiles

- Réseaux 2G : GSM
  - Mobilité



Panorama des réseaux mobiles

- Réseau 2.5G : GPRS
  - General Packet Radio Service
    - Service à valeur ajoutée pour le transfert de données dans les réseaux mobiles GSM
      - Permet à l'utilisateur d'accéder à des services de données
    - Solution intermédiaire avant la technologie UMTS encore utilisée actuellement
    - Commutation de paquets :
      - Superpose une infrastructure paquet au réseau GSM
    - Efficacité spectrale :
      - Optimise l'utilisation des ressources radio en ne les affectant que lorsque l'utilisateur en a besoin…
    - Compatible avec le standard nord-américain Time Division Multiple Access (TDMA)
  - Débit
    - Débits théoriques maximum : 171.2 kb/s
    - Débits réels < 50 kb/s
  - Connectivité
    - Permet des connexions instantanées avec mise en communication immédiate
    - Assimilé à une fonction du type : "toujours connecté"
  - Applications : l'Internet partout
    - Supporte les fonctionnalités de l'Internet Mobile et l'interopérabilité avec l'Internet sur le web
      - Facilite les applications du type data-oriented

Panorama des réseaux mobiles

- Réseau 3G : UMTS
  - Universal Mobile Telecommunications System
    - Réseaux et services mobiles de troisième génération (3G) pour le transfert des données
    - De couverture mondiale, avec des normes compatibles partout
    - Norme définie par l'International Telecommunications Union dans le cadre du projet IMT-2000
  - Permet d'offrir de l'information large-bande via les IP réseaux fixes, satellites et mobiles
    - Applications gourmandes en débits: e-commerce, jeux,…
  - Propose des services
    - A coût réduit (…)
    - A débits élevés : 2Mb/s théoriques
    - A couverture programmable (dimension des cellules)
    - A accès universel : Multimédia (voix/données)
  - Accélère la convergence entre les télécoms, les NTIC et l'audio-visuel
    - Pour proposer de nouveaux services générateurs de revenus pour les opérateurs
    - Pour payer les investissements considérables nécessaires…
  - Vise un marché de masse, haute qualité et haut débit, dans les communications mobiles multimédia
    - Plus de 500 millions d'utilisateurs début 2010…

Panorama des réseaux mobiles

- Réseau 3.99G : LTE
  - Long Term Evolution (ou super 3G)
    - Fait partie de la norme UMTS et permet le transfert des données
    - Proche de la norme 4G (4ème génération)
      - Sans satisfaire toutes les spécifications imposées pour la norme notamment en terme de bande passante utilisée
    - Utilisant des bandes passantes de 1,5MHz à 20MHz
    - Permettant un débit de l'ordre de 100Mbit/s en Downlink (vers le mobile)
      - Les réseaux 4G utiliseront une bande passante minimale de 100MHz pour un débit allant jusqu'à 1 Gbit/s
      - LTE sera réellement une norme de 4G dans sa version 3GPP 10 appelée LTE Advanced

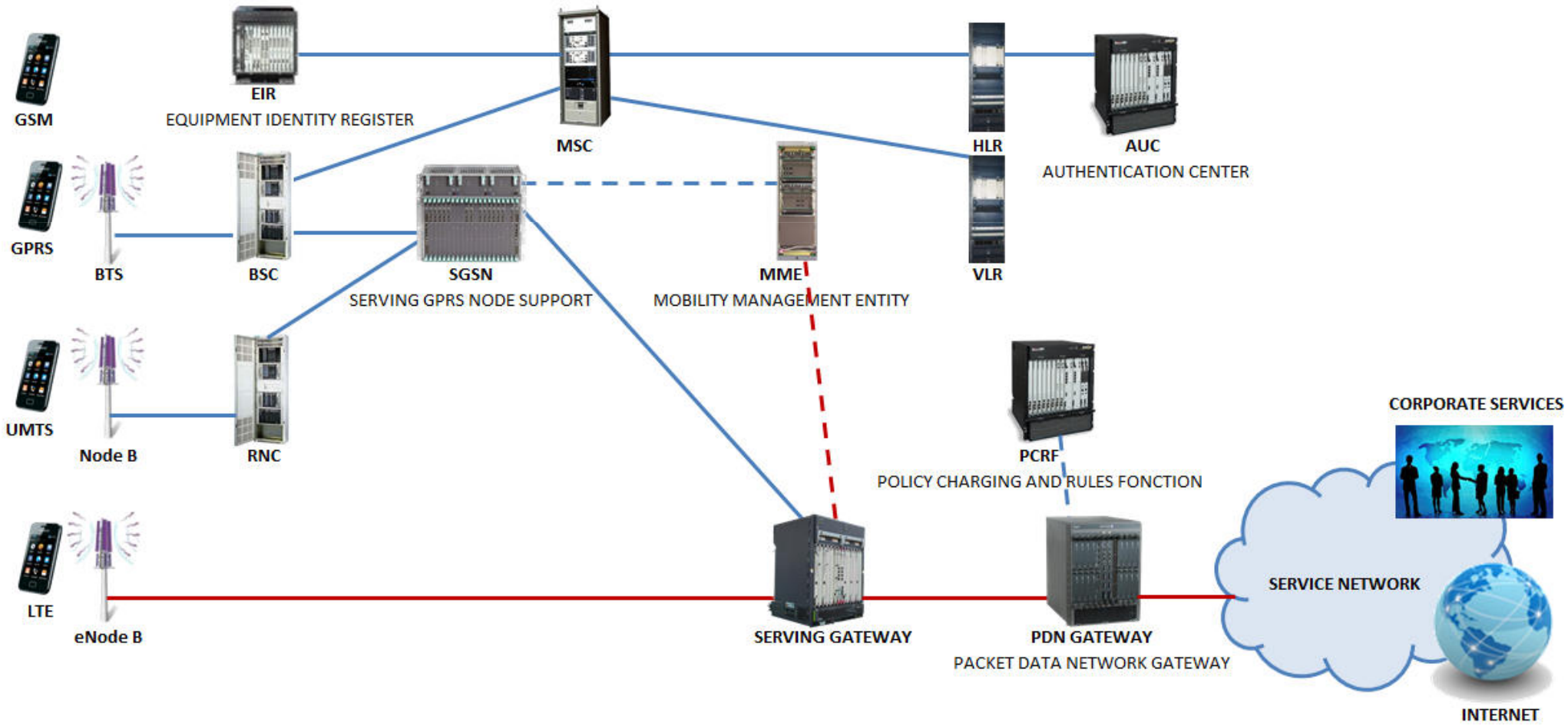
	Débit lien radio descendant (Mbit/s)	Débit lien radio montant (Mbit/s)	Latence (ms)	Version des spécifications
LTE	100	50	environ 10	3GPP 8
LTE-Advanced	1000	500	environ 5	3GPP 10

  - Caractéristiques
    - Débit descendant allant jusqu'à 326,4 Mbit/s
    - Débit de chargement allant jusqu'à 86,4 Mbit/s
    - Taux de transfert de données au bord de la cellule de 2 à 3 fois l'UMTS
    - Efficacité spectrale (nombre de bits transmis par seconde par hertz du transporteur) 3 fois plus élevée que la version la plus évoluée de l'UMTS
    - RTT (Round Trip Time) de moins de 10ms (contre 200ms pour l'UMTS)

- Réseau 3.99G : LTE
  - Fonctionnement
    - Liaison descendante : modulation OFDMA (Orthogonal Frequency Division Multiple Access)
      - Apporte une optimisation dans l'utilisation des fréquences en minimisant les interférences
    - Liaison montante : modulation SC-FDMA (au lieu de W-CDMA pour l'UMTS)
    - Utilisation de bande passante variable de 1,25 à 20 MHz pour chaque utilisateur
      - Permettant une plus grande souplesse par rapport à la valeur fixe de 5MHz en W-CDMA pour l'UMTS
    - Application flexible à différentes bandes de fréquence
      - GSM, W-CDMA UMTS et de nouvelles bandes à 2,6 GHz…
    - Excellent support en mouvement : hautes performances jusqu'à 350 km/h
      - Voire jusqu'à 500 km/h en fonction de la bande de fréquence utilisée
    - Recours à des techniques d'antennes multiples (également utilisées pour le Wifi ou le Wimax)
      - Permet de multiplier les canaux de communication parallèles, augmentant le débit total et la portée
  - Basé sur deux modes de multiplexage
    - Multiplexage de fréquences (FDD - Frequency Division Duplexing) :
      - L'émission et la réception se font à des fréquences différentes
    - Multiplexage temporel (TDD - Time Division Duplexing) :
      - L'émission et la réception transitent à une même fréquence, mais à des instants différents
    - FDD est mis en œuvre dans les équipements télécoms dans la plupart des réseaux LTE
    - TDD fonctionne sur des bandes de fréquences distinctes attribuées ultérieurement

Panorama des réseaux mobiles

- Evolutions
  - Architecture du réseau GSM et de ses évolutions



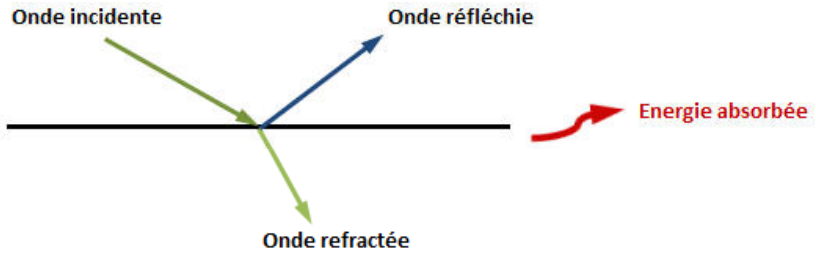
Introduction à la norme Wifi

- Présentation de la norme 802.11
  - Norme plus connue sous le nom de "Wifi" ou "Wi-Fi"
    - Protocole réseau sans fil
    - Permet à des équipements de se connecter et d'échanger des données par voie radio
    - Permet des débits élevés à de grandes distances (plusieurs centaines de mètres)
      - 11 Mbit/s théoriques dans sa version B (norme adoptée en septembre 1999)
      - 54 Mbit/s théoriques dans sa version G
      - 300 Mbit/s théoriques dans sa version N
    - Intègre au moins un protocole de sécurité au niveau liaison WEP (Wired Equivalent Privacy)
      - Très simple à administrer et à utiliser mais très peu sûr
  - Usages
    - Etendre un réseau existant : pont Wifi
    - Partager une ressource : switch, serveur, imprimante, accès internet, …
    - Réaliser un portail d'accès authentifié : Hot-Spot
    - Utiliser des objets communiquant : lecteur de flux RSS, localisation, Karotz, NAO, …
    - Déployer un réseau urbain alternatif aux opérateurs : les villes Internet…
    - Accéder à une ressource en mobilité : serveur de données, serveur e-mail, équipements spécifiques dans les hôpitaux, …

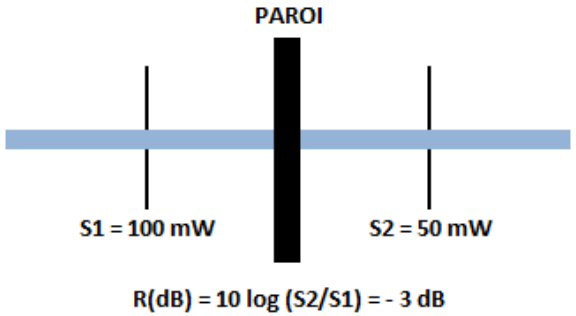
Introduction à la norme Wifi

- Présentation de la norme 802.11
  - Avantages
    - Facilité de déploiement
    - Interopérabilité avec les réseaux filaire
    - Débits relativement adaptés à un usage professionnel
    - Grande souplesse et faible structure (chantier, exposition, locaux temporaires, …)
    - Structure non intrusive (monuments historiques, sites classés, …)
    - Grande mobilité
    - Faible coût d'acquisition
  - Inconvénients
    - Limites des ondes radio
    - Sensibles aux interférences (micro-ondes, autres réseaux, …)
    - Occupation progressive des bandes des fréquence : autorégulation
    - Réglementation (fréquences et puissances d'émission contrôlées par l'Etat)
    - Variations importantes de débit, celui-ci étant :
      - Mutualisé : partagé entre les utilisateurs
      - Variable : entre trois fois et dix fois inférieur au filaire
      - Dépendant : lié aux conditions d'usage (norme, marque, distance, protocole de sécurité, …)
    - Aspects sanitaires (accumulation des ondes et l'inconnu des effets à long terme)
    - Sécurité (nécessite de déployer des solutions de sécurité adaptées)

- Notions de propagation radio
  - Les ondes radio
    - Se propagent en ligne droite dans plusieurs directions depuis leur source d'émission
    - Leur vitesse dans le vide est de 3.10^8 m/s
    - Lorsqu'elle rencontre un obstacle, une onde est divisée et son énergie est répartie



  - Gain et atténuation
    - Amplification : la puissance du signal d'une onde est amplifiée en étant capté par une antenne
    - Atténuation : une partie de l'énergie d'une onde est absorbée en traversant un obstacle
    - L'atténuation (ou gain) est le rapport entre la puissance du signal avant et après modification
      - Attenuation : R (dB) = 10 x log (S2/S1)



R(dB) = 10 log (S2/S1) = - 3 dB

Fonctionnement

- Absorption des ondes
  - L'énergie d'une onde électromagnétique est progressivement dégradée au cours de sa propagation dans l'air
    - L'onde électromagnétique propagée rencontre des électrons qu'elle va exciter
    - Ces électrons vont, à leur tour, réémettre du rayonnement perturbant le signal et l'atténuant
  - Les signaux se dégradent avec la distance et les obstacles
    - Limitation de la portée
    - Limitation du débit de la liaison
- Fréquences associées
  - La norme 802.11 utilise la bande de fréquence des 2,4 GHz
    - 14 canaux de transmissions sont utilisables dans cette bande de fréquence
      - Plusieurs réseaux peuvent cohabiter au même endroit à condition de ne pas interférer l'un avec l'autre

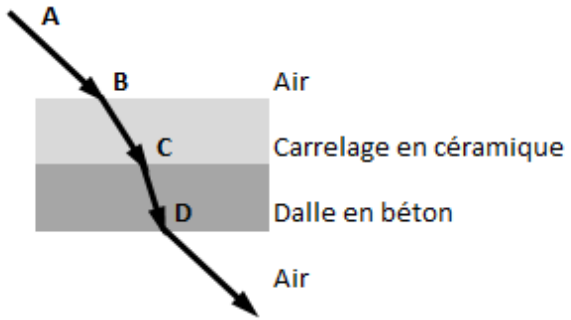
CANAL	1	2	3	4	5	6	7	8	9	10	11	12	13	14
FREQUENCE	2412 Mhz	2417 Mhz	2422 Mhz	2427 Mhz	2432 Mhz	2437 Mhz	2442 Mhz	2447 Mhz	2452 Mhz	2457 Mhz	2462 Mhz	2467 Mhz	2472 Mhz	2477 Mhz

- Cas perturbant
  - Fréquence
    - La fréquence moyenne de la porteuse du Wifi est de 2,437 GHz
    - La fréquence de résonance de l'eau est de 2,45 GHz
  - Longueur d'onde
    - La longueur d'onde du Wifi est de 12,31 cm
    - Le quart d'onde (taille des objets absorbant l'énergie de cette onde) est de 3,05 cm
  - Chemins multiples (Multipath)
    - Par réflexions successives, une onde peut atteindre une station en empruntant des chemins multiples et générer des interférences
    - La présence de deux antennes sur un point d'accès permet de contrôler et de séparer les signaux
  - Eléments absorbant l'énergie d'un signal Wifi
    - Les éléments contenant de l'eau
      - Feuilles de papier, …
    - Les éléments d'un taille proche de 3 cm
      - Bijoux, fèves, …

- Cas perturbant liés au Wifi
  - Perturbation liée au(x) milieu(x) traversé(s)
    - Affaiblissement pour la bande de fréquences 2,4 GHz

Matériaux	Affaiblissement	Exemples
Air	Négligeable	Champ libre
Bois	Faible	Porte, plancher, cloison
Plastique	Faible	Cloison
Verre	Faible	Vitres non teintées
Verre teinté	Moyen	Vitres teintées
Eau	Moyen	Aquarium, fontaine
Etre vivants	Moyen	Foule, animaux, humains, végétation
Briques	Moyen	Murs
Plâtre	Moyen	Cloisons
Céramique	Elevé	Carrelage
Papier	Elevé	Rouleaux de papier
Béton	Elevé	Murts porteurs, étages, piliers
Verre blindé	Elevé	Vitres pare-balles
Métal	Très elevé	Béton armé, miroirs, armoire métallique, cage d'ascenseur

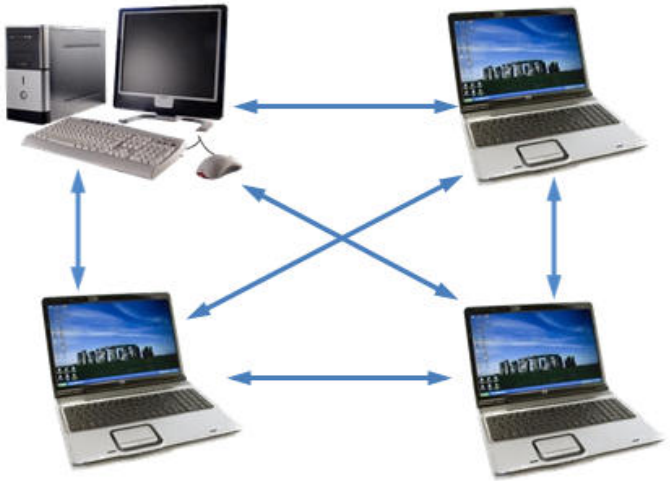
    - Réfraction pour la bande de fréquences 2,4 GHz



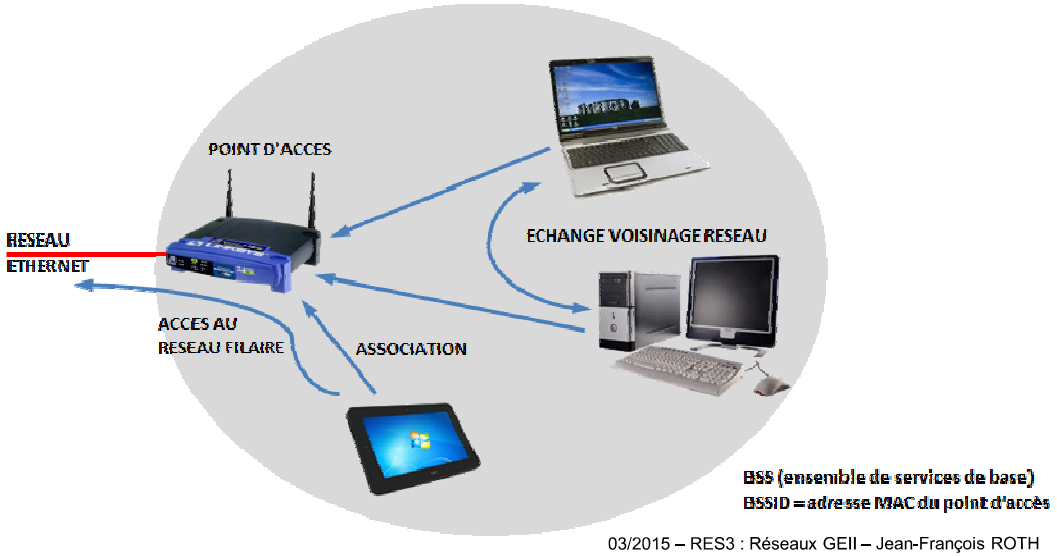
- Relation entre ondes, fréquences et portée
  - Augmentation de la fréquence
    - Augmentation du phénomène d'absorption
    - Diminution de la portée (distance de couverture du réseau)
      - Les transmissions radiophoniques se font sur des fréquences d'une centaine de MHz
    - Augmentation potentielle du débit de données
  - Augmentation de la puissance
    - Augmentation de la portée
    - Diminution de la durée de vie des batteries
- Puissance Isotrope Rayonnée Equivalente (PIRE)
  - Puissance effective rayonnée en sortie d'antenne
    - Limitée à 100 mW à l'extérieur et à l'intérieur en France
    - Une puissance de 100 mW correspond à 20 dBm
    - La perte est estimée à 1 dB par mètre en moyenne
  - Formules de calcul
    - PIRE (dBm) = puissance en sortie AP (dBm) + gain d'antenne (dBi) – pertes câbles (dB)
    - PIRE (dBm) = puissance en sortie AP (dBm) + gain d'antenne (dBi)

Fonctionnement

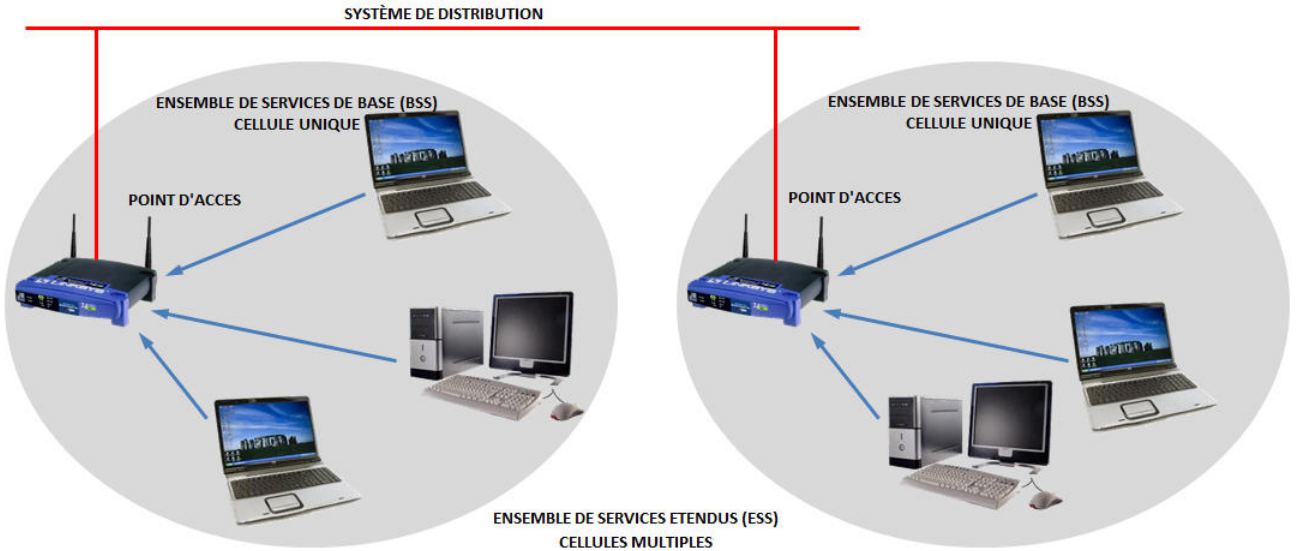
- Topologie "Ad'hoc"
  - Chaque adaptateur joue successivement le rôle d'Access Point (AP) et de client
    - Les machines communiquent ensemble en point à point (peer to peer)
  - N'intègre pas nativement de protocole de routage
  - La portée du réseau est limitée aux portées de chaque paire
  - Ensemble de services de base indépendant ou IBSS (Independant Base Set Service)
    - Adapté aux réseaux temporaires lorsqu'aucun Access Point est disponible
    - Connexion entre postes correspondant à un câble croisé en Ethernet



- Topologie infrastructure
  - Chaque station se connecte à un point d'accès ou Access Point (AP)
    - Le point d'accès est en mode serveur et les stations en mode client
    - Le point d'accès offre un ensemble de services de base ou BSS (Basic Set Service)
      - Le BSS est caractérisé par son BSSID correspondant à l'adresse MAC du point d'accès
  - Nécessite une association et optionnellement une authentification
    - Jusqu'à 100 stations peuvent être associées à un point d'accès
  - Connexion à la ressource Ethernet (Bridge IP)
  - Communication avec les autres stations (IP)
  - Le support de transmission et le débit radio sont partagés entre les stations
    - Un point d'accès Wifi équivaut à un Hub (ou concentrateur) Ethernet



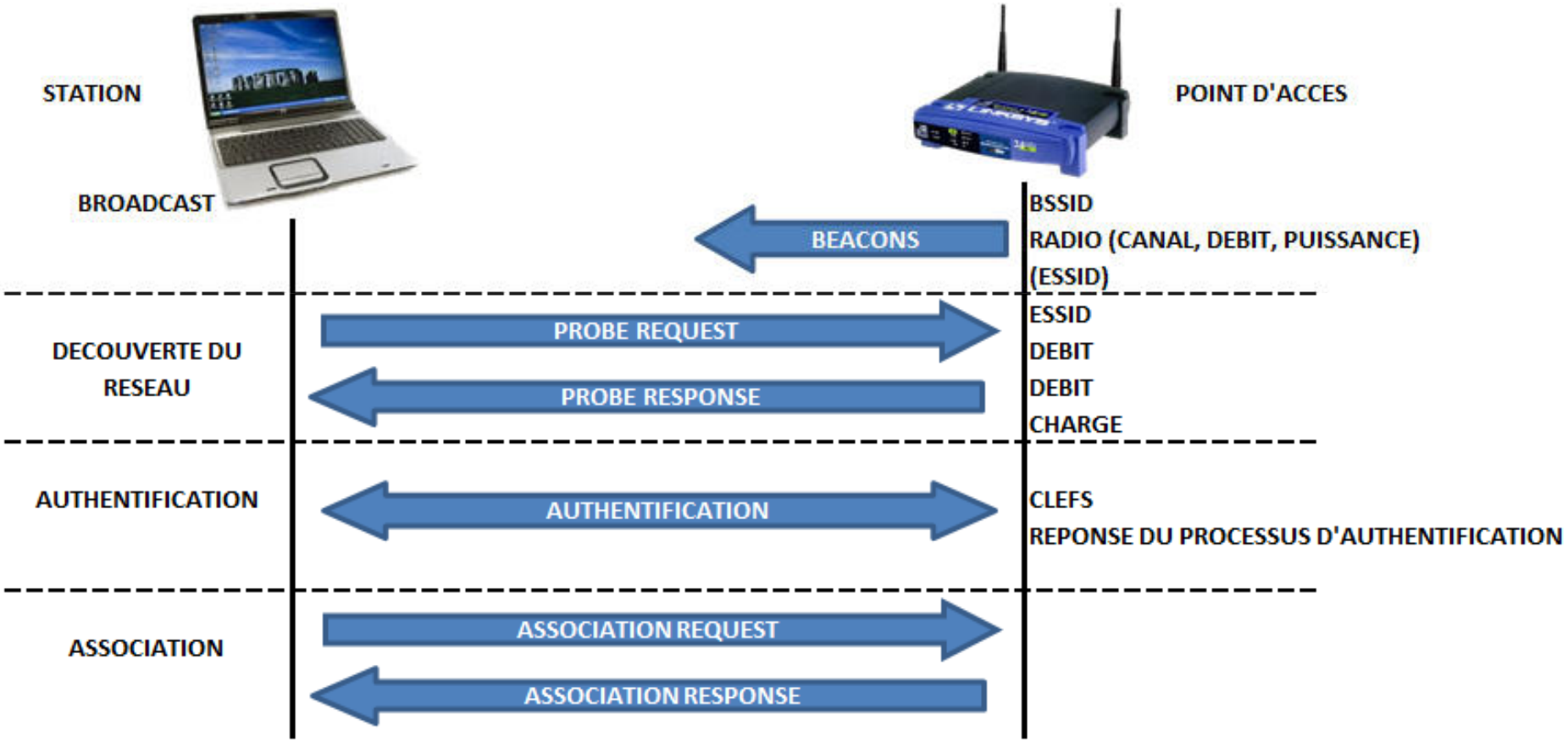
- Topologie infrastructure étendue
  - Plusieurs point d'accès reliés par un service de distribution ou DS (Distribution Service)
  - Permet d'obtenir un ensemble de services étendu ou ESS (Extended Service Set)
    - Un ESS est identifié par un ESSID
      - Identifiant à 32 caractères au format ASCII nécessaire pour s'y associer
    - Tous les Access Point du réseau doivent utiliser le même ESSID
    - Les cellules de l'ESS peuvent être séparées ou se recouvrir pour offrir un service de mobilité
      - Concept du "roaming" (norme 802.11f)
  - Le service de distribution est la dorsale (ou backbone) du réseau
    - Réseau Ethernet
    - Pont Wifi



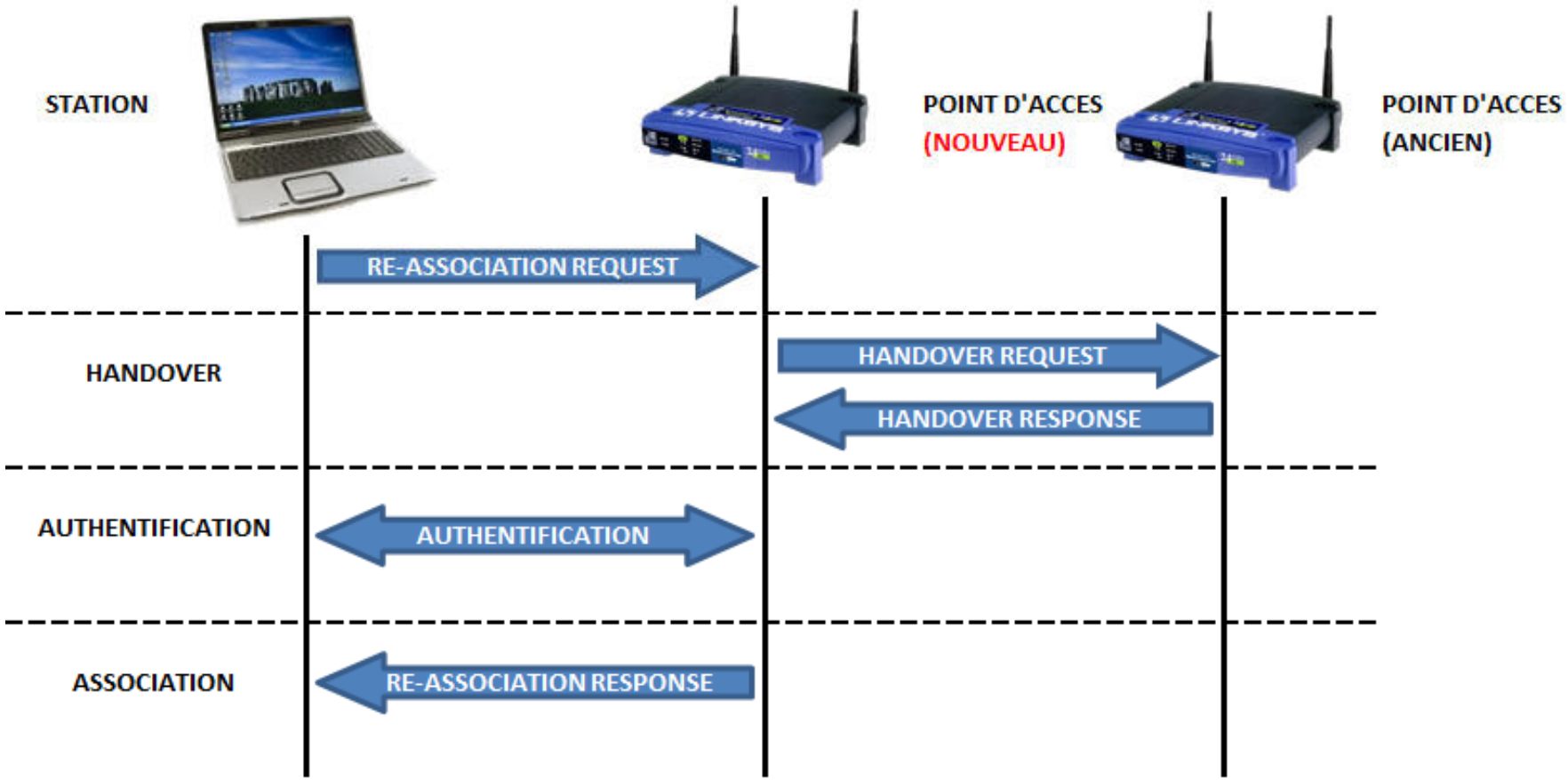
- Notion de Roaming (ou Handover)
  - Mécanisme de mobilité permettant d'offrir un service continu en mobilité
    - Fonctionnant sur le principe de l'organisation spatiale des canaux
    - Norme 802.11f / Protocole Inter Access Point Protocol (IAPP)
    - Notions de Roaming et Handover différentes en GSM mais identiques pour le Wifi
  - Configuration
    - Nécessité de vigilance liée au recouvrement des canaux
  - Contraintes
    - Nécessité de compatibilité entre les équipements
    - Débit pouvant être réduit

- Mécanisme d'association
  - Toutes les 0,1s
    - Le point d'accès diffuse une trame balise (Beacon) contenant
      - Son BSSID (exemple : 00:16:39:8A:FC:88)
      - Ses caractéristiques radio (exemple : canal 2 / 54 Mbit/s / ENC)
      - En option, son ESSID en clair (exemple : UHA-AMPHI-NORD)
  - Lors de la détection de son entrée dans une cellule
    - L'adaptateur client diffuse une requête de sondage (Probe Request) contenant
      - L'ESSID sur lequel(s) il est configuré (ex : UHA-AMPHI-NORD, BATIMENT-A-GEII, …)
        - Si aucun ESSID n'est configuré il écoute le réseau à la recherche d'un ESSID en clair
      - Ses caractéristiques radio (exemple : 300 Mb/s)
  - Lors de la réception d'une requête de sondage (Probe Request)
    - Le point d'accès vérifie le ESSID et les caractéristiques radio proposées
      - En cas de compatibilité, il envoie une réponse avec les informations sur sa charge et des données de synchronisation (puissance / débit)
  - A la réception de la réponse, l'adaptateur client
    - Evalue la qualité du signal émis et la distance du point d'accès
    - Choisit le point d'accès avec le meilleur débit et la plus faible charge en cas de choix multiples
    - Envoie une demande d'association au point d'accès choisi

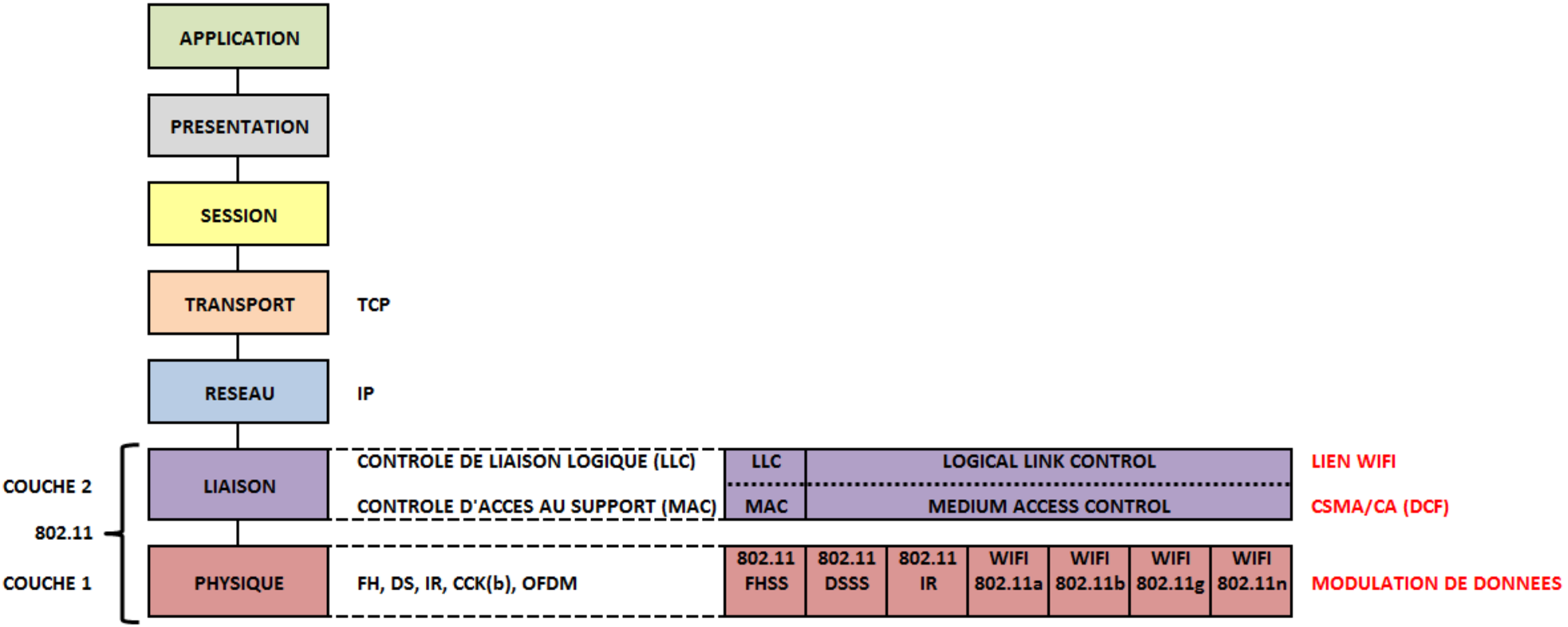
- Mécanisme d'association



- Mécanisme de Roaming (ou Handover)

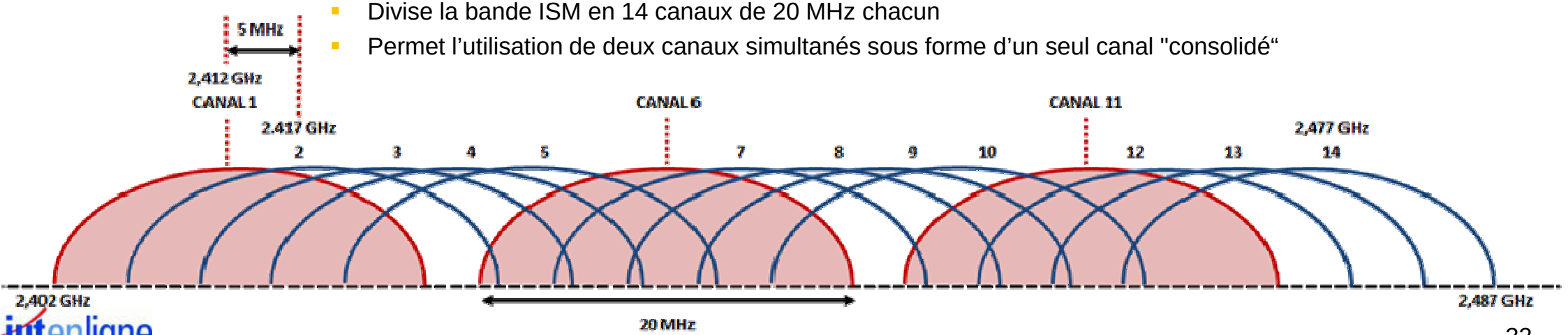


- Wifi et modèle OSI
  - Situé sur les deux couches inférieures du modèle OSI
    - La couche physique et la couche liaison de données
      - Comme tous les protocoles IEEE 802
      - TCP/IP et autres protocoles de couches supérieures peuvent fonctionner aussi bien sous 802.11 (Wifi) que sur 802.3 (Ethernet)



- Wifi et modèle OSI
  - Couche physique
    - 802.11 utilise la bande des 2,4 GHz (de 2,402 GHz à 2,487 GHz)
      - Bande de fréquences ISM (Industrial, Scientific and Medical)
    - La couche physique est en réalité la radio mais l'utilisation du Wifi ne nécessite pas de licence
      - Au niveau radio, la méthode utilisée est l'étalonnement du spectre
    - Composée de deux sous-couches
      - Physical Medium Dependent (PMD)
        - Gérant l'encodage des données et la modulation
      - Physical Layer Convergence Protocole (PLCP)
        - Gérant l'écoute du support et signalant à la couche MAC que le support est libre
        - Signalement à la couche MAC réalisé par un Clear Channel Assessment (CCA)
    - Canal de transmission
      - Bande de fréquence étroite utilisable pour une communication
      - La largeur du canal (Bande Passante) est en général proportionnelle au débit de communication
      - Des canaux peuvent se recouvrir en partie, générant une dégradation de la qualité du signal et du débit

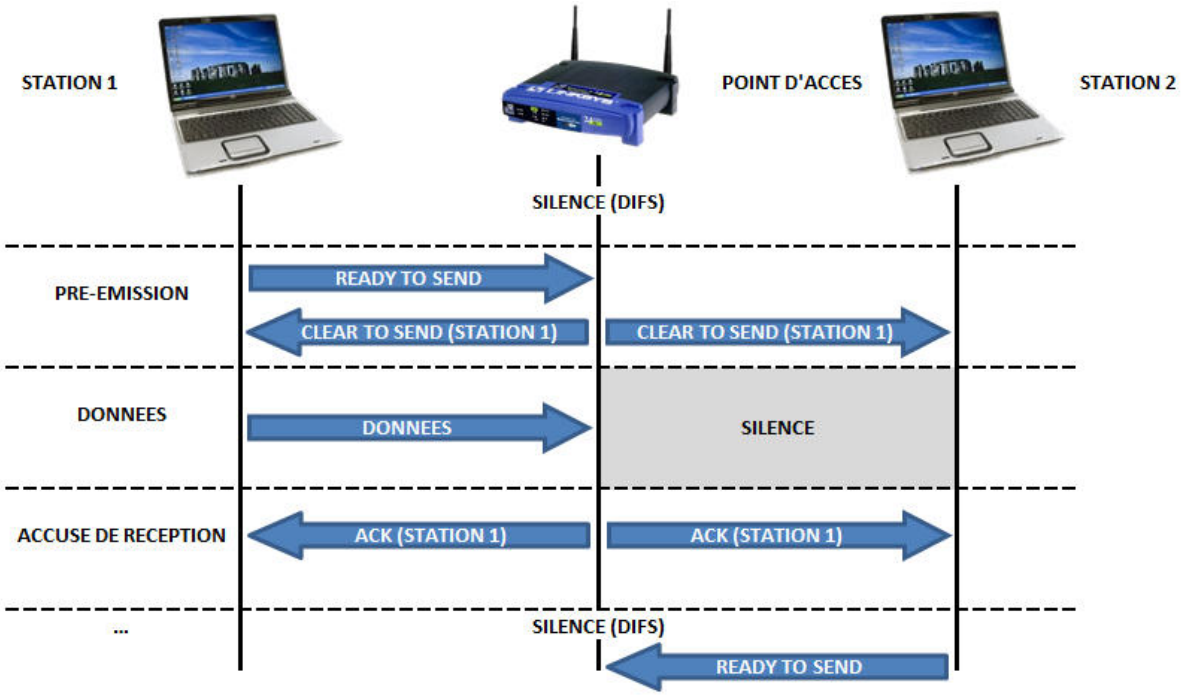
- Wifi et modèle OSI
  - Couche physique
    - Méthode d'étalement Direct Sequence Spead Spectrum (DSSS)
      - Technique d'étalement de spectre basée sur la séquence directe utilisée par 802.11b et 802.11g
        - Consiste à transmettre pour chaque bit une séquence Barker également appelée bruit pseudo-aléatoire
        - Chaque bit valant 1 est remplacé par une séquence de bits et chaque bit valant 0 par son complément.
      - Divise la bande ISM en 14 canaux de 22MHz chacun
      - La largeur de bande ISM de 85MHz permet de placer 14 canaux de 22 MHz adjacents
        - Nécessité de recouvrement partiel des canaux
        - Les fréquences centrales de chaque sous-canal sont espacées de 5 MHz
        - Les canaux bas sont plus stables
        - Seul trois canaux sont utilisables simultanément et à proximité : 1,6 et 11
        - La transmission ne se fait que sur un canal fixé lors de la configuration
    - Méthode d'étalement Orthogonal Frequency-Division Multiplexing (OFDM)
      - Technique d'étalement de spectre basée sur la séquence directe utilisée par 802.11n
      - Divise la bande ISM en 14 canaux de 20 MHz chacun
      - Permet l'utilisation de deux canaux simultanés sous forme d'un seul canal "consolidé"



- Wifi et modèle OSI
  - Couche physique
    - Multiple In, Multiple Out (MIMO)
      - Multiples entrées, multiples sorties
      - Multiplie le nombre de canaux de transmission effectifs dans un même canal radio
      - Les émetteurs et les récepteurs utilisent plusieurs antennes (de 2 à 8)
      - Chaque antenne est utilisée comme un émetteur différent
      - Un algorithme exploite les interférences liées à la réflexion des ondes pour distinguer les différents flux reçus
      - Utilisable uniquement en intérieur
    - Impact de la technologie MIMO
      - A même puissance et à distance égale
        - Permet de doubler le débit de 802.11G, sans rendre le réseau plus stable
      - A même puissance et à débit égal
        - Permet d'augmenter la portée des équipements, tout en garantissant une qualité de réception
    - Evolution
      - Alliée à d'autres technologies, MIMO peut devenir la future référence en terme de communication mobile
      - Les constructeurs de matériels réseau (Netgear, Linksys/Cisco, D-Link, ...) proposent des solutions MIMO sans garantir les débits théoriques indiqués par la norme

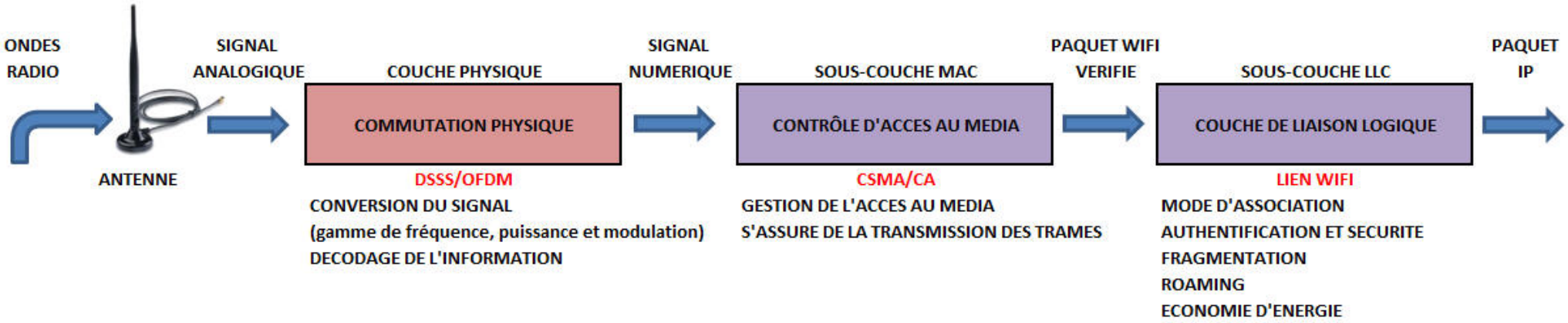
- Wifi et modèle OSI
  - Couche liaison de données
    - Au niveau de la couche MAC (Media Access Control)
      - Protocole CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) :
        - En Ethernet, CSMA/CD (Collision Detection) permet de détecter une collision à l'émission car les stations ont la possibilité d'écouter les transmissions en cours
        - En Wifi, ceci n'étant pas le cas, un mécanisme d'esquive de collision appelé CSMA/CA (Collision Avoidance) est nécessaire
      - CSMA/CA tente d'éviter les collisions en imposant un accusé de réception systématique des paquets (ACK)
        - Pour chaque paquet de données arrivé intact, un paquet ACK est émis par la station réceptrice
    - Fonctionnement de CSMA/CA
      - Une station souhaitant émettre explore les ondes
        - Si aucune activité n'est détectée, elle attend un temps aléatoire avant de transmettre, si le support est toujours libre
        - Si le paquet est intact à la réception la station réceptrice émet une trame ACK
        - Une fois la trame ACK reçue par l'émetteur, un terme est mis au processus
        - Si la trame ACK n'est pas détectée par la station émettrice (le paquet original ou le paquet ACK n'a pas été reçu intact) une collision est supposée
        - Le paquet de données est retransmis après attente d'un autre temps aléatoire

- Wifi et modèle OSI
  - Couche liaison de données
    - Fonctionnement de CSMA/CA
      - Une station souhaitant émettre écoute le réseau, si celui-ci est encombré, la transmission est différée
      - Si le média est libre pendant le temps Distributed Inter Frame Space (DIFS) la station peut émettre
      - La station émettrice transmet un message Ready To Send (RTS) contenant des informations sur le volume des données qu'elle souhaite émettre et sa vitesse de transmission
      - Le récepteur répond un Clear To Send (CTS) permettant à la station de commencer l'émission des données
      - Toutes les stations avoisinantes patientent pendant un temps calculé à partir du Clear To Send
      - À réception de toutes les données émises par la station, le récepteur envoie un accusé de réception (ACK)



- Wifi et modèle OSI
  - Couche liaison de données
    - Au niveau de la couche LLC (Logical Link Control)
      - Multiplexage des protocoles fonctionnant au-dessus de la couche de liaison de données
      - Gestion du contrôle de flux
      - Gestion de l'accusé réception
      - Gestion de la correction d'erreur
      - Gestion de l'adressage et du contrôle de la liaison de données
      - Spécification des mécanismes devant être utilisés pour adresser des stations sur le support de transmission
        - Mode d'association
      - Spécification des mécanismes devant être utilisés pour le contrôle de l'échange des données entre l'expéditeur et le destinataire
        - Authentification
        - Sécurité
        - Fragmentation
        - Roaming
        - Economie d'énergie

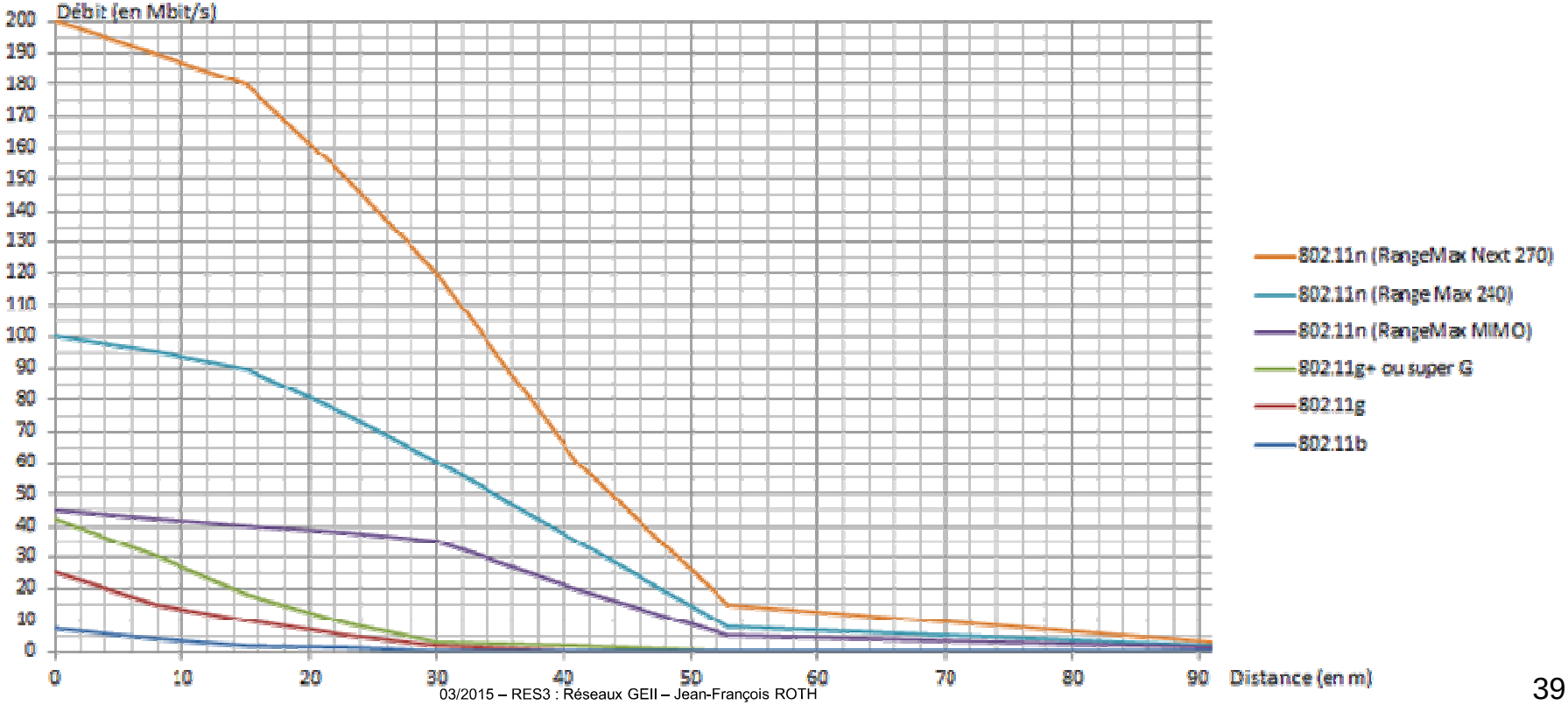
- Wifi et modèle OSI
  - Services successifs
    - La couche Wifi 802.11 est indépendante de la couche réseau Internet Protocol (IP)
      - Elle est préalable à son fonctionnement dans la communication réseau
    - Lors de la configuration du réseau
      - Deux aspects nécessaires à la communication entre les équipements sont traités séparément
        - Les paramètres radio (802.11)
        - Les paramètres réseau (IP)
    - En mode infrastructure, la transmission des données ne remonte pas jusqu'à la couche IP
      - l'Access Point peut avoir une IP LAN qui n'est pas dans le sous-réseau



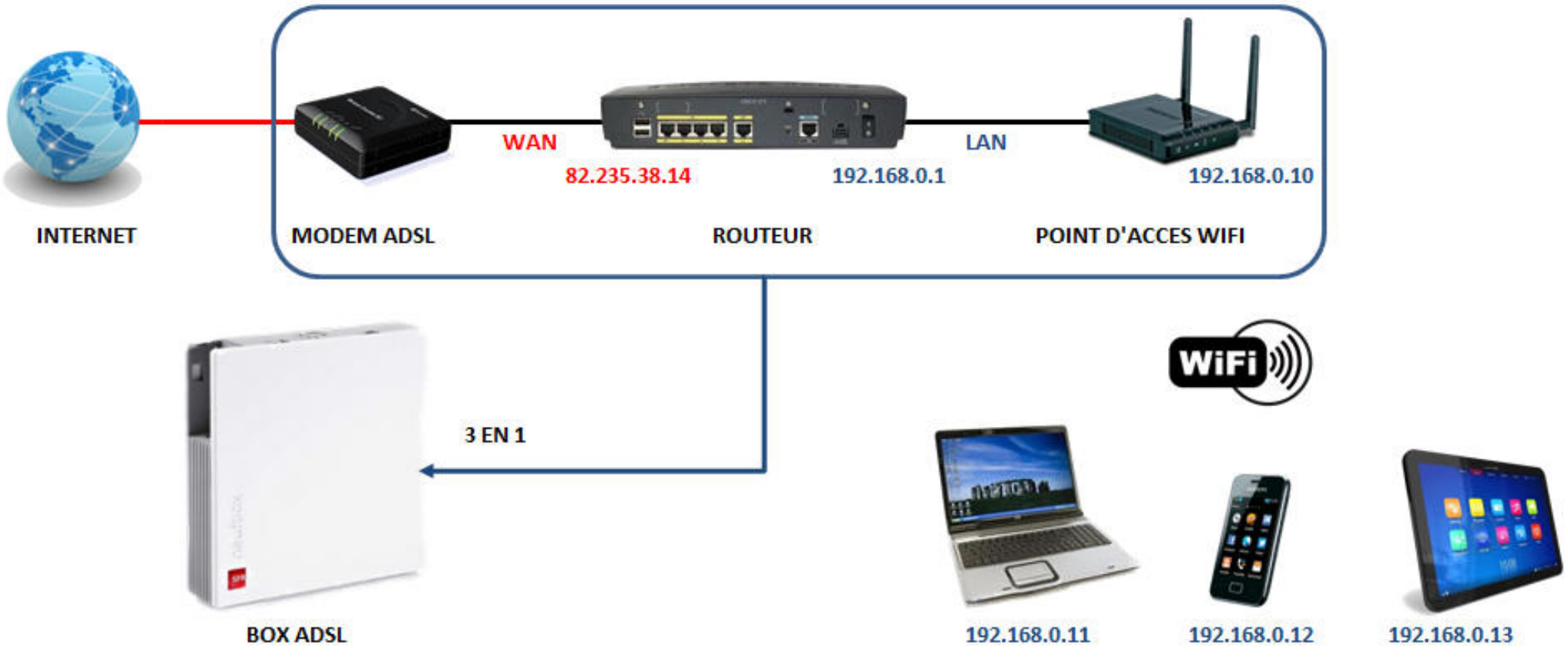
- Caractéristiques du Wifi
  - Portées et débits
    - Normes 802.11a, 802.11b, 802.11g et 802.11n
      - Appelées "normes physiques" correspondant à des révisions du standard 802.11
      - Permettent d'obtenir différents débits en fonction de la portée
      - Les équipements 802.11a ne sont pas compatibles avec les équipements 802.11b, g et n
      - Des matériels "Dual Band" intègrent des puces 802.11a et 802.11b, g ou n
    - Les débits varient en fonction de l'environnement
      - Intérieur, extérieur, obstacles, matériaux rencontrés, …
    - Les débits varient en fonction du type de données transmises
      - Taille de trame, niveau de sécurité, …

Protocole	Date de normalisation	Fréquence	Débit (Théorique)	Débit (Typique)	Portée intérieur	Portée extérieur
802.11a	1999	5 GHz	54 Mbit/s	25 Mbit/s	environ 25 m	environ 75 m
802.11b	1999	2.4 Ghz	11 Mbit/s	6.5 Mbit/s	environ 35 m	environ 100 m
802.11g	2003	2.4 Ghz	54 Mbit/s	25 Mbit/s	environ 40 m	environ 100 m
802.11n	2009	2.4 ou 5 Ghz	300 Mbit/s	100 Mbit/s	environ 80 m	environ 150 m

- Caractéristiques du Wifi
  - Portées et débits
    - Norme physique actuelle : 802.11n
      - Débit théorique de 270-300Mbit/s et débit réel plus proche de 75-100Mbit/s en réalité (RangeMax 240)
      - Portée théorique identique (MIMO) deux fois supérieure à celle de 802.11g
      - Optimisé par l'utilisation du codage Orthogonal Frequency-Division Multiplexing (OFDM)
      - La combinaison MIMO-OFDM sur la bande ISM optimise les performances de transmission
      - Norme compatible avec les matériels 802.11b et 802.11g (sauf pour certains anciens matériels)



- Caractéristiques du Wifi
  - Infrastructure



- Wifi et sécurité
  - La sécurité est le principal problème des réseaux sans-fil
    - Un réseau sans fil non sécurisé permet à des personnes non autorisées d'écouter et d'y accéder
      - Un réseau sans-fil est équivalent à des câbles RJ45 qui pendent par les fenêtres…
      - Nécessité de sécuriser les réseaux sans fil dès leur installation
      - En fonction de l'importance du réseau, il est possible de le sécuriser de façon plus ou moins forte
      - Le soucis de sécurité sans-fil est présent un peu partout au sein du réseau
  - Nécessité d'appliquer les mêmes procédures que pour les réseaux filaires
    - Informer les utilisateurs
      - La sécurité d'un réseau passe par la prévention, la sensibilisation et la formation des utilisateurs
    - Auditer son réseau
      - Audit physique
        - Permet de s'assurer que le réseau sans-fil ne diffuse pas d'informations dans des zones non désirées
        - Permet de s'assurer qu'il n'existe pas de réseau sans fil non désiré dans le périmètre à sécuriser
      - Audit informatique
        - Permet de s'assurer que le degré de sécurité obtenu est bien égal à celui désiré
    - Surveiller son réseau
      - Surveillance au niveau réseau (IP) avec un système de détection d'intrusions classique : prelude, snort, ...
      - Surveillance au niveau physique (sans fil) avec des outils dédiés : PrismDump, AirTraf, AirIDS, ...

- Wifi et sécurité
  - Attaques possibles
    - L'écoute des données
      - Solution efficace : le chiffrement (ou cryptage) de données
    - L'intrusion et le détournement de connexion
      - Solution efficace : restreindre l'accès radio et l'accès au réseau, authentifier la personne
      - Nécessite : une bonne configuration radio (SSID, …) et réseau (@IP, passerelle, DNS …)
    - L'occupation de la Bande Passante
      - Provenance : échange de fichiers lourds bloquant la bande passante de l'utilisateur principal
      - Nécessite : une configuration radio (SSID, …), et réseau (@IP, passerelle, DNS …)
    - Le brouillage des transmissions
      - Provenance : téléphones DECT, fours à micro-ondes, …
      - Solution efficace : Couper la source ou s'en éloigner
    - Le dénis de service
      - Provenance : utilisation de connaissances du protocole CSMA/CA pour occuper l'Access Point ou lui envoyer des paquets chiffrés pour le mettre hors-service
      - Solution efficace : WPA

- Wifi et sécurité
  - Sécurité des points d'accès
    - Produits les plus sensibles du réseau sans fil
      - Suppression de la configuration d'usine (mot de passe, …) avant mise en place
      - Identification du réseau sans-fil pour que les différentes stations puissent être reconnues
        - Suivant le type du matériel, le SSID par défaut a une valeur différente (ex: 111 pour 3Com)
        - Il est déconseillé de cacher son SSID, ceci pouvant poser des problèmes de connexion
      - Sécurisation du réseau par une clef d'encryptage WPA ou WPA2
      - Possibilité d'administrer la puissance d'émission de l'antenne
        - En la réglant au minimum, les risques d'écoute sont minimisés, sans être supprimés
      - Possibilité de filtrer les adresses MAC ayant le droit de communiquer avec le Point d'Accès
        - Dans un réseau disposant de plusieurs Points d'Accès, ce filtrage devra être reproduite sur chacun d'eux pour garder toute la mobilité du réseau
      - Il reste possible à un utilisateur mal intentionné de récupérer le trafic échangé entre des équipements voire de simuler une adresse MAC interceptée

- Wifi et sécurité
  - Sécurité des équipements
    - WEP (Wired Equivalent Privacy)
      - Protocole de chiffrement utilisant une clef secrète statique de 64 ou 128 bits et l'algorithme de chiffrement RC4
      - WEP 64 bits utilise une clé de chiffrement de 40 bits à laquelle est concaténé un vecteur d'initialisation (initialization vector ou IV) de 24 bits
      - WEP 128 bits utilise une clé de chiffrement de 104 bits à laquelle est concaténé un vecteur d'initialisation de 24 bits
      - WEP 128 bits est saisie comme une suite de 13 caractères ASCII ou 26 caractères hexadécimaux de A à F et de 0 à 9
        - Exemple : BB8854D96DEC24A153A2F239A9
      - Nécessite d'être configuré sur le Point d'Accès (AP) et toutes les stations
      - Fiabilité
        - Une attaque de type "force brute" permet de casser une clef de 64 bits
        - Une capture d'environ 1M de paquets permet de casser une clef de 64 ou 128 bits (faille algorithmique)
        - WEP présente un grand nombre de failles le rendant vulnérable et obsolète

- Wifi et sécurité
  - Sécurité des équipements
    - WPA (Wifi Protected Access)
      - Norme 802.11i allégée permettant deux modes d'authentification
        - Mode entreprise : EAP (Extensible Authentication Protocol) nécessitant un serveur central qui répertorie les utilisateurs et distribue les différentes clefs (ex: serveur RADIUS)
        - Mode personnel : PSK (Pre-Shared Key) méthode simplifiée d'authentification des utilisateurs, sans serveur central, utilisant un mot de passe alphanumérique "passphrase"
      - Protocole reposant sur l'algorithme de cryptage TKIP (Temporary Key Integrity Protocol) et de chiffrement MIC (Message Integrity Code)
        - TKIP permet la génération aléatoire de clefs et offre la possibilité de modifier la clef de chiffrement plusieurs fois par secondes, pour plus de sécurité
        - MIC authentifie l'émetteur et le récepteur et réalise un hachage cryptographique
      - Protocole de chiffrement utilisant quatre clefs de 128 bits générées à l'authentification (PSK ou EAP)
        - Clé de chiffrement des données (128 bits) et clé d'intégrité (128 bits) pour protéger les données
        - Clé de chiffrement EAPOL (128 bits) et clé d'intégrité EAPOL (128 bits) pour protéger la "poignée de main" initiale

- Wifi et sécurité
  - Sécurité des équipements
    - WPA-PSK (Wifi Protected Access-Pre Shared Key)
      - Mode personnel adapté aux particuliers et PME ne nécessitant pas de serveur d'authentification
        - Solution moins chère à mettre en œuvre, mais moins sécurisée
      - L'utilisateur doit saisir une phrase secrète "Passphrase" pour accéder au réseau
        - La "Passphrase" contient de 8 à 63 caractères ASCII ou 64 symboles hexadécimaux de A à F et de 0 à 9 (256 bits)
        - La solution ASCII est préférable à condition d'utiliser une phrase secrète complexe
      - Fonctionnement
        - La "Passphrase" est convertie vers une clé 256 bits nommée Pairwise Master Key (PMK)
        - Les 4 clefs temporelles sont générées par TKIP à partir de cette Pairwise Master Key
        - TKIP génère une clé de paquets (per-packet key) et mélange les paquets du message
        - TKIP remet les paquets dans l'ordre pour retrouver l'intégrité du message grâce à un mécanisme de triage (re-keying)

- Wifi et sécurité
  - Sécurité des équipements
    - WPA2-PSK (Wifi Protected Access 2-Pre Shared Key)
      - Norme 802.11i évolution des protocoles WPA-PSK et WPA-EAP
      - Permet de sécuriser aussi bien la topologie infrastructure que la topologie Ad'hoc
      - Protocole reposant sur l'algorithme de cryptage AES (Advanced Encryption Standard)
        - L'algorithme prend en entrée un bloc de 128 bits (16 octets), la clé fait 128, 192 ou 256 bits
        - Les 16 octets en entrée sont permutés selon une table définie au préalable
        - Ces octets sont ensuite placés dans une matrice de 4x4 éléments
        - Les lignes de cette matrice subissent une rotation vers la droite (incrément de rotation variant selon le numéro de ligne)
        - Une transformation linéaire est appliquée sur la matrice
        - Consiste en la multiplication binaire de chaque élément de la matrice avec des polynômes issus d'une matrice auxiliaire
        - Cette multiplication est soumise à des règles spéciales selon GF(2^8) (groupe de Galois ou corps fini)
        - La transformation linéaire assure une meilleure diffusion (propagation des bits dans la structure) sur plusieurs tours
        - Finalement, un XOR entre la matrice et une autre matrice, permettant d'obtenir une matrice intermédiaire
        - Ces différentes opérations sont répétées plusieurs fois et définissent un "tour"
        - Une clé de 128, 192 ou 256 bits AES nécessitant respectivement 10, 12 ou 14 tours

- Wifi et sécurité
  - Sécurité des équipements
    - Pour les particuliers (et PME)
      - WPA-PSK est le premier protocole grand public sérieux
      - WPA2-PSK est le protocole le plus sécurisé à ce jour
      - Il est préférable d'utiliser le cryptage AES plutôt que le cryptage TKIP
      - Pour rendre ces solutions fiables il est nécessaire de choisir une "Passphrase" complexe, d'au moins 8 caractères, n'appartenant pas au dictionnaire et contenant des caractères alphanumériques
    - Pour les entreprises
      - Pour augmenter la sécurité, il est nécessaire de mettre en place, en parallèle, des moyens supplémentaires permettant d'identifier l'utilisateur sur le réseau
      - La solution la plus sécurisée est la mise en place d'un réseau privé virtuel (Virtual Private Network VPN)
    - Alternative pour la sécurité en entreprise : la norme 802.1X
      - Amélioration du chiffrement :
        - Les clefs peuvent être de 128 bits et différentes pour chaque nouvelle session
      - Amélioration de l'authentification :
        - Utilisation de protocoles d'authentification comme EAP (Extensible Authentification Protocol) ou RADIUS (Remote Authentification Dial-In User Service) pour l'authentification mutuelle
        - Utilisation du protocole LEAP (Light Extensible Authentification Protocol), protocole d'authentification s'appuyant sur le protocole EAP pour l'authentification entre le client et l'Access Point sur les réseaux sans fil

- Wifi et sécurité
  - Aspects juridiques
    - Loi contre le terrorisme (LCT) du 29 octobre 2005
      - Impose à tous ceux qui proposent un accès à Internet au public (particuliers, cybercafés ou des fournisseurs d'accès à Internet) de conserver les données de connexion pendant 3 ans et à les communiquer si nécessaire aux services de police
        - En pratique, le log des adresses MAC connectées suffit
        - Certains points d'accès embarquent des solutions d'enregistrement des logs
    - Aspect important
      - En cas d'utilisation de votre réseau à votre insu vous êtes responsable de ce qui est fait depuis votre connexion
        - Problématique accentuée par la loi HADOPI du 12 Juin 2009
  - Conclusion
    - La couche liaison de 802.11 offre une sécurité limitée
      - De nouveaux protocoles et de nouvelles normes peuvent encore faire leur apparition
      - Toute personne se trouvant dans le rayon d'émission, voire même au-delà grâce à des dispositifs amplifiants, peut être susceptible de communiquer sur le réseau en tant qu'utilisateur valide
      - La sécurité nécessite une attention quotidienne
    - L'évolution du sans fil est constante
      - Lorsque ses inconvénients auront été résolus, le réseau sans fil sera à son apogée et pourrait, éventuellement, mettre un terme aux réseaux filaires

Wifi vs Bluetooth

- Comparatif entre Wifi et Bluetooth

	BLUETOOTH	802.11b	802.11g	802.11n
TRANSPORT DE LA VOIX	TROIS CANAUX PRIORITAIRES	VOIX SUR IP UNIQUEMENT	VOIX SUR IP UNIQUEMENT	VOIX SUR IP UNIQUEMENT
TYPE DE TERMINAUX	ORDINATEUR, TÉLÉPHONE PORTABLE, CAPTEUR, VÉHICULE, LECTEUR DE CODE BARRE, …	ORDINATEUR ET TÉLÉPHONE PORTABLE	ORDINATEUR ET TÉLÉPHONE PORTABLE	ORDINATEUR ET TÉLÉPHONE PORTABLE
CONSOMMATION ÉLÉCTRIQUE	TRÈS FAIBLE	IMPORTANTE	IMPORTANTE	IMPORTANTE
COÛT D'INTÉGRATION	FAIBLE	MOYEN	MOYEN	MOYEN
DÉBIT THÉORIQUE (EFFECTIF)	VERSION 1.0 : 1 MB/S VERSION 2.0 : 10 MB/S	11 MB/S (7 MB/S EFFECTIF)	54 MB/S (30 MB/S EFFECTIF)	300 MB/S (100 MB/S EFFECTIF)
TAUX DE TRANSFERT THÉORIQUE	VERSION 1.0 : 0,125 MO/S VERSION 2.0 : 1,25 MO/S	1,4 MO/S	6,75 MO/S	37,5 MO/S
PORTÉE MAXIMALE EN INTÉRIEUR	*CLASSE 1 : 100 M* CLASSE 2 : 10 À 20M *CLASSE 3 : QUELQUES MÈTRES*	DE 1 À 35M	DE 1 À 40M	DE 1 À 50M (À L'ORIGINE) DE L'ORDRE DE 1 À 100M (VOIRE 200M POUR LES VERSIONS ÉVOLUÉES)
RÉSISTANCE AUX INTERFÉRENCES	FORTE	MOYENNE	MOYENNE	MOYENNE
SÉCURITÉ	FORTE	PERFECTIBLE	PERFECTIBLE	PERFECTIBLE
UTILISATIONS	INTERCONNEXION DE PROXIMITÉ (LECTEUR CODE BARRE), INTERCONNEXION D'OUTILS NOMADES (PC PORTABLE ET TÉLÉPHONE GPRS/UMTS) ET PARTAGE D'ACCÈS INTERNET RAPIDE	RÉSEAUX INFORMATIQUE ET PARTAGE D'ACCÈS INTERNET RAPIDE	RÉSEAUX INFORMATIQUE ET PARTAGE D'ACCÈS INTERNET RAPIDE	RÉSEAUX INFORMATIQUE ET PARTAGE D'ACCÈS INTERNET RAPIDE

Planning

- *CM 1 : Généralités Réseaux*
- *CM 2 : Topologie et supports de transmission*
  - *TD 1 : Débit et technologie ADSL*
- *CM 3 : Codage des informations et contrôle d'intégrité*
  - *TD 2 : Codage des informations et contrôle d'intégrité CRC*
- *CM 4 : Modèle OSI / Ethernet*
- *CM 5 : Couches transport et réseau (TCP/IP)*
  - *TD 3 : Analyse de trames Ethernet / Adresse IP et masque de sous-réseaux*
  - *TD 4 : Adressage IP / Routage IP*
- *CM 6 : Réseaux WLAN et sécurité*
  - **TD 5 : Réseaux Wifi et sécurité**
- CM 7 : Réseaux et bus de terrain
  - TD 6 : Réseaux et bus de terrain
    - TP 1 : Technologie ADSL
    - TP 2 : Analyse de trames et Encapsulation Ethernet
    - TP 3 : Configuration d'un réseau IP / Routage IP / Wifi
    - TP 4 : Réseaux et bus de terrain
    - TP 5 : TP Test
- CM 8 : Contrôle de connaissances

- Exercice 1 (15 minutes)
  - Pour quelle raison la portée de Bluetooth n'est-elle que de quelques mètres ?
    - Justifiez votre réponse
      - La puissance d'émission du Bluetooth est très faible, beaucoup plus faible que dans les technologies sans-fil Wi-Fi et GSM
  - Pour quelle(s) raison(s) le débit effectif d'un réseau Wi-Fi est-il loin du débit théorique ?
    - Justifiez votre réponse
      - Les stations s'adaptent à l'environnement et émettent à la vitesse maximale compte tenu des contraintes environnementales (distances, matériaux traversés, interférences, …)
      - Les mécanismes destinés à éviter les collisions ralentissent la transmission des données
      - Un niveau de sécurité élevé réduit le débit utile et ralentit la transmission des données

- Exercice 2 (25 minutes)
  - Soit un réseau 802.11n proposant un débit théorique de 300 Mbit/s.
    - Si 20 utilisateurs se partagent les ressources d'une cellule, quel sera le débit théorique moyen de chaque station ? Pour quelle raison ?
      - Le débit disponible étant mutualisé, le débit théorique moyen sera divisé entre les stations actives dans la portée du réseau.
      - Avec 20 stations actives, le débit théorique moyen par station sera de 300/20 = 15 Mbit/s
  - Quelles sont les conséquences négatives de l'augmentation de la portée des réseaux sans-fil ?
    - Proposez une solution pour y remédier.
      - Le débit disponible étant divisé par le nombre de stations actives dans un réseau sans-fil, une augmentation de portée risque d'entrainer une augmentation du nombre de station active
      - Afin d'obtenir un débit suffisant, il convient d'augmenter le nombre de cellules
  - La puissance d'émission nécessaire croit comme le carré de la portée.
    - Quelles seront les contraintes induites par la solution proposée à la question précédente pour une station nomade (Smartphone, PC portable, …) ?
      - Avantage : lorsque la portée d'une cellule est diminuée, la puissance nécessaire à l'émission est plus faible, la durée des batteries des stations nomades dans la cellule seront préservées.
      - Inconvénient : L'augmentation du nombre de cellules impose l'utilisation de plusieurs fréquences distinctes. L'affectation des fréquences peut s'avérer compliquée à gérer pour éviter les interférences au sein d'une même cellule ou entre cellules voisines.

- Exercice 3 (30 minutes)
  - Votre entreprise souhaite installer un réseau informatique sans-fil, compatible avec le réseau Ethernet existant, entre deux bâtiments proches l'un de l'autre
    - Quel réseau sans-fil conviendrait le mieux pour réaliser cette opération ? Justifiez.
      - La technologie 802.11n avec un débit théorique de 300 Mbit/s et une portée théorique de 80m en intérieur
    - Quel type de matériel convient-il d'installer dans le premier bâtiment ?
      - Des points d'accès wifi 802.11n (bases) permettant la roaming (norme 802.11f)
    - Quelles précautions doivent être prises pour relier les différentes bases ?
      - Les différentes bornes d'un WLAN étendu doivent se situer dans le même domaine de collision et appartenir au même sous-réseau IP, afin que vos utilisateurs se déplacent dans le bâtiment sans perdre la connexion au réseau (nécessité de matériels compatibles supportant 802.11f)
      - Les bornes doivent être placées de sorte à ce que leurs zones de couverture se chevauchent.
      - Le nombre de bases doit être suffisant pour assurer l'absence de zones d'ombre (sans couverture)
      - Vérifier que la puissance du signal reçu est suffisante dans toutes les zones
    - Quelles sont les conséquences de l'installation du réseau sans-fil dans le second bâtiment ?
      - La mise en cascade de certaines bornes en mode répéteur divisera le débit utile par deux, les bornes se partageant le même canal pour communiquer entre elles et avec les stations (la borne faisant office de répéteur et transmettant les trames à l'autre borne avec la même fréquence).
    - Quelles sont les étapes à respecter pour configurer le WLAN ?
      - Paramétrage du nom du WLAN (ESSID), du type de réseau (infrastructure), du débit (le plus élevé possible), les canaux de communication, la taille maximale d'une trame et la puissance d'émission
      - Les différents champs doivent être remplis en veillant à ce que tous les paramètres soient identiques dans tous les composants du WLAN.

- Exercice 4 (20 minutes)
  - Un étudiant dispose d'un ordinateur portable récent équipé d'une carte réseau Wifi 802.11n (RangeMax 240)
  - Il dispose également d'un accès à internet par un opérateur "câble" proposant une connexion en FTTLA dans son logement étudiant de Mulhouse
    - Son ordinateur actuel est-il adapté à son offre internet ? Justifiez votre réponse de manière détaillée.
      - Débit théorique de la norme 802.11n : 270 Mbit/s
      - Débit pratique de la norme 802.11n à une distance proche du points d'accès : 100 Mbit/s
      - Débit théorique d'un accès à internet avec une connexion FTTLA à Mulhouse : 100 Mbit/s
        - FTTLA (Fiber To The Last Amplifier) : Fibre optique jusqu'au dernier amplificateur puis câble coaxial entre l'amplificateur de rue (ou d'immeuble) et le logement de l'abonné
      - Le FTTLA utilisant la fibre sur une longue distance et un câble coaxial sur une distance beaucoup plus courte permet de réduire les pertes (en considérant un câble coaxial en bon état)
      - Le débit réel de l'accès à internet dans ce cas sera proche du débit théorique : de 90 à 60 Mbit/s en fonction de la distance entre l'abonné et l'amplificateur de rue (ou d'immeuble)
      - Sa connexion réseau à 100 Mbit/s ne bridera donc en aucun cas sa connexion internet (de 90 à 60 Mbit/s)

- Exercice 5 (25 minutes)
  - Un étudiant dispose d'un vieil ordinateur portable équipé d'une carte réseau Wifi 802.11b
    - Remarque : cet ordinateur ne dispose que de ports USB 1.0 (débit 1,5 Mbit/s)
  - Celui-ci est contacté par son Fournisseur d'Accès Internet (FAI) lui indiquant qu'à partir du mois prochain, celui-ci disposera, au même tarif, de la technologie ADSL2+ à son logement étudiant de Mulhouse
    - Pour profiter au mieux de cette nouvelle offre, est-il préférable pour lui de changer son ordinateur au plus vite et le remplacer par un ordinateur récent (équipé d'une carte réseau Wifi 802.11n) ou peut-il conserver son ordinateur actuel ? Justifiez votre réponse de manière détaillée.
      - Débit théorique de la norme 802.11b : 11 Mbit/s
      - Débit pratique de la norme 802.11b à une distance proche du points d'accès : 7 Mbit/s
      - Débit théorique d'un accès à internet avec une connexion ADSL 2+ : 22 Mbit/s IP
      - La technologie ADSL 2+, extension de l'ADSL, utilise la paire torsadée sur une distance maximale de 2,5 km
        - L'ADSL 2+ n'a de réel intérêt que pour les abonnés situés à moins de 1500 m du répartiteur contenant le DSLAM
        - A partir d'une distance de 2500 m le gain n'est plus significatif par rapport à une connexion ADSL standard
      - Si l'étudiant se trouve à moins de 1500 m du répartiteur contenant le DSLAM, sa connexion réseau (7 Mbit/s) bridera sa connexion internet (débit supérieur à 7 Mbit/s), il pourrait changer d'ordinateur
      - Si l'étudiant se trouve à plus de 2500 m du répartiteur contenant le DSLAM, sa connexion réseau (7 Mbit/s) n'aura aucun impact sur sa connexion internet (débit inférieur à 6,4 Mbit/s), il n'a aucun intérêt à investir dans un nouvel ordinateur
        - Remarque : son ordinateur ne disposant que de ports USB 1.0 à 1,5 Mbit/s il ne pourra pas « tricher » en ajoutant un point d'accès Wifi 802.11n USB à son PC portable
      - Il est recommandé à l'étudiant d'utiliser un site comme www.degrouptest.com (étudié en TP) pour estimer son débit ADSL théorique

Planning

- *CM 1 : Généralités Réseaux*
- *CM 2 : Topologie et supports de transmission*
  - *TD 1 : Débit et technologie ADSL*
- *CM 3 : Codage des informations et contrôle d'intégrité*
  - *TD 2 : Codage des informations et contrôle d'intégrité CRC*
- *CM 4 : Modèle OSI / Ethernet*
- *CM 5 : Couches transport et réseau (TCP/IP)*
  - *TD 3 : Analyse de trames Ethernet / Adresse IP et masque de sous-réseaux*
  - *TD 4 : Adressage IP / Routage IP*
- *CM 6 : Réseaux WLAN et sécurité*
  - *TD 5 : Réseaux Wifi et sécurité*
- CM 7 : Réseaux et bus de terrain
  - TD 6 : Réseaux et bus de terrain
    - TP 1 : Technologie ADSL
    - TP 2 : Analyse de trames et Encapsulation Ethernet
    - TP 3 : Configuration d'un réseau IP / Routage IP / Wifi
    - TP 4 : Réseaux et bus de terrain
    - TP 5 : TP Test
- CM 8 : Contrôle de connaissances