

Réseaux sans fil

B. Tanguy KABORE

Doctorant IT

tanguykabore@yahoo.fr

Avertissement sur les Droits d'Auteur et Licence

- Ce cours est un projet open source publié sous la licence Creative Commons Attribution (CC BY).
- Certaines images et textes utilisés dans ce cours proviennent de sources diverses.
- Bien que nous ayons essayé de créditer les auteurs lorsque possible, il est possible que certaines attributions aient été omises.
- Si vous êtes l'auteur d'un contenu utilisé et que vous souhaitez que votre contribution soit correctement citée, veuillez nous contacter à tanguykabore@yahoo.fr
- Licence : Vous êtes libre de partager, modifier et redistribuer ce cours sous réserve de citer la source originale et de respecter les termes de la licence.
- Contact : Pour toute question ou correction, veuillez nous contacter à tanguykabore@yahoo.fr

Planning

- ☐ **Partie 1: WLAN**
- ☐ **Partie 2: WMAN**
- ☐ **Partie 3: Réseaux mobiles**
- ☐ **Partie 4: Réseaux de Capteurs Sans Fil**

Architecture des réseaux

B. Tanguy KABORE

Doctorant IT

tanguykabore@yahoo.fr

Partie 1: WLAN et IEEE 802.11

1.1. Origines des WLAN

- ❑ Nouveau besoin des utilisateurs : la mobilité
- ❑ Développement et commercialisation d'équipements portables munis de liaisons radio ou infrarouges
- ❑ WLAN (Wireless LAN, LAN sans fil) : Système local offrant un moyen de communication direct entre plusieurs ordinateurs portables par liaison radio.

1.2. Utilisation des WLAN

☐ **Mobilité** : augmente l'efficacité et la productivité

☐ Installation dans zones difficiles à câbler

- Immeubles anciens
- Halls, salles de réunion, cafés, lieux publics

☐ Temps d'installation réduits

☐ Facilité d'emploi pour les utilisateurs

☐ Maintenance facile, coût de câblages faibles

☐ Réseaux ad-hoc : réunions, interventions militaires et humanitaires

1.3. Protocole MACA (1/3)

❑ *Multiple Access with Collision Avoidance*

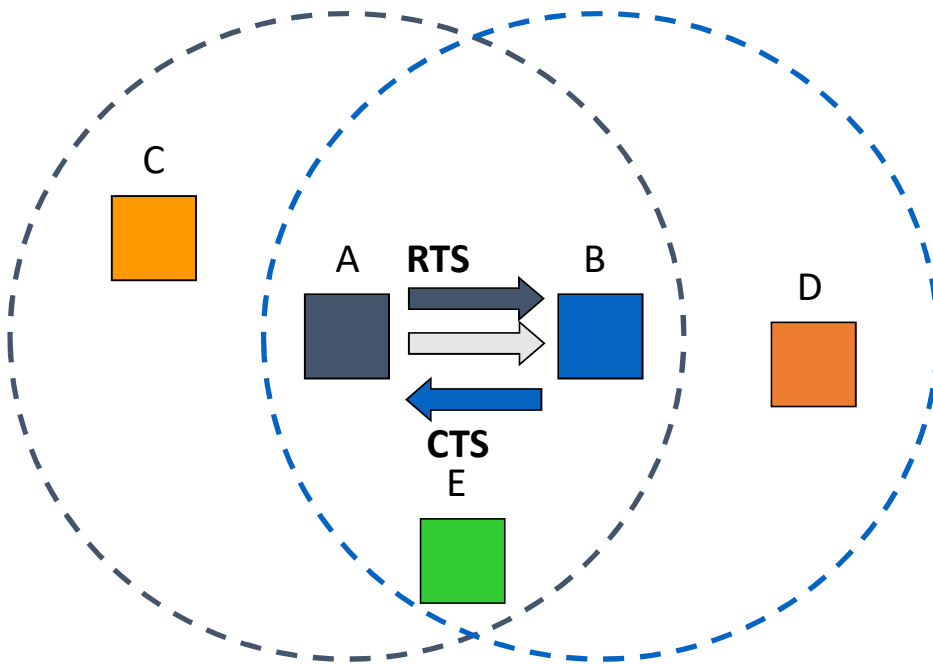
❑ Développé en 1990, il est à la base des travaux sur la norme 802.11

❑ Principe

- Avant de transmettre, l'émetteur émet une trame RTS (*Request To Send*).
- Les stations entendant le RTS s'interdisent de transmettre pendant le temps nécessaire à la transmission.
- Le récepteur signale qu'il accepte la transmission par une trame CTS (*Clear To Send*).

1.3. Protocole MACA (2/3)

❑ Exemple



- A émet un RTS contenant @A, @B et durée de la transaction

⇒ C et E se taisent jusqu'à la fin de la transaction

- B répond par un CTS contenant @A, @B et durée de la transaction

⇒ D et E se taisent jusqu'à la fin de la transaction

- A émet les données

1.3. Protocole MACA (3/3)

❑ Le risque de collision n'est pas nul : il existe lors de l'envoi de RTS

- RTS et CTS = trames courtes pour minimiser la probabilité de collision
- Si collision, elle est détectée par l'absence de CTS en retour : retransmission d'un RTS après un temps aléatoire

❑ Amélioration MACAW (1992)

- Introduit des ACK
- Ecoute de la porteuse avant émission des RTS
- Contrôle de congestion

1.4. Problèmes spécifiques aux transmissions sans fil

- ❑ **Interférences** : Les bandes de fréquences utilisées sont les mêmes que les fréquences de travail des fours micro-ondes, et d'autres normes (Bluetooth)
- ❑ **Sécurité** : Les informations transitent « dans l'air ». Sans précaution particulière, tout récepteur équipé d'une antenne peut : lire les données, les modifier, se connecter au réseau. 3 problèmes : **confidentialité**, **intégrité**, **authentification**.
- ❑ **Roaming** (*handover*): un **utilisateur mobile** peut quitter la portée d'un **point d'accès**.
- ❑ **Consommation de puissance** : Les équipements mobiles ont une **batterie de faible capacité**. L'énergie doit être économisée.
- ❑ **Réglementation des émissions** : on n'émet pas à n'importe quelle fréquence ni à n'importe quelle puissance !

1.5. Technologies



Acronyme de **W**irless **F**idelity ou **W**irless **P**HY, est plus précisément connu sous la norme IEEE 802.11.



"Dents bleues" a été développé en 1994 par le suédois ERICSSON. Remplace les liaisons filaires courtes de types périphériques, GSM, PDA et autres.



Infrared Data Association à l'identique du *Bluetooth*, il permet la connexion de périphériques et autres équipements portables, grâce à une liaison **optique infrarouge**.

1.6. Dimension des réseaux sans fil (1/2)

WPAN - Réseau Personnel sans Fils

Réseaux domestiques de faible portée.

Technologies applicables:

Bluetooth, IrDA

WLAN – Réseau Local sans Fils

Réseaux locaux d'entreprise nécessitant une portée supérieure aux réseaux domestiques.

Technologies applicables:

Wi-Fi, DECT pour la téléphonie, ...

1.6. Dimension des réseaux sans fil (2/2)

WMAN – Réseau Métropolitain sans Fils

Réseaux métropolitains de type *WirelessMAN* de forte portée.

Technologies applicables:

WiMAX, ...

WWAN - Réseau Étendu sans Fils

Réseaux étendus de très forte portée à usage principalement téléphonique.

Technologies applicables:

WiMAX, GSM, ...

1.7. Norme IEEE 802.11 ? WiFi?

❑ La norme **IEEE 802.11** (ISO/IEC 8802-11) est un **standard international** décrivant les caractéristiques d'un réseau local sans fil.

❑ **WiFi ou Wi-Fi** : contraction de *Wireless Fidelity*, correspond initialement au nom donné à la certification délivrée par la **Wi-Fi Alliance**, anciennement WECA (*Wireless Ethernet Compatibility Alliance*).

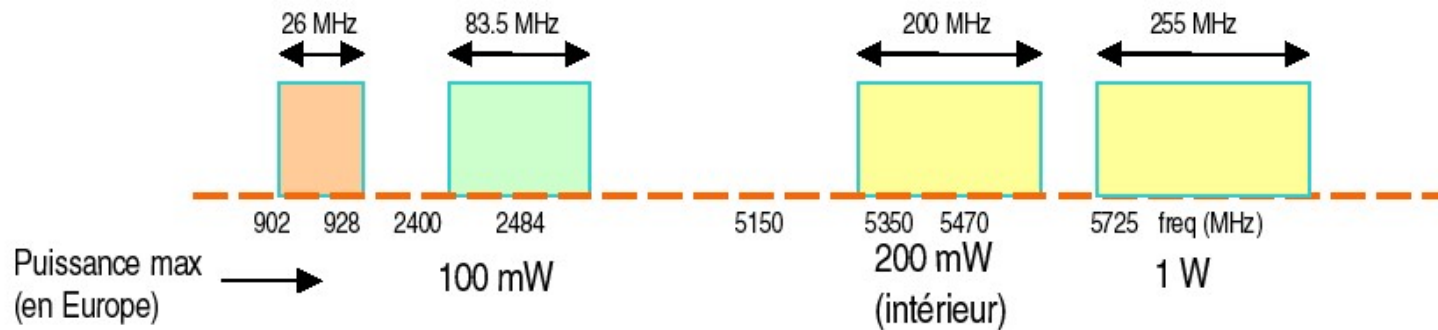
- La Wi-Fi Alliance est l'organisme chargé de maintenir **l'interopérabilité** entre les matériels répondant à la norme **802.11**.
- Le nom de la norme se confond aujourd'hui avec le nom de la certification.
- Matériels certifiés par la Wi-Fi Alliance identifiés par le logo



1.8. Norme IEEE 802.11

❑ Ces normes IEEE 802.11 utilisent les bandes ISM (*Industrial, Scientific and Medical*), allouées à travers le monde pour des opérations sans licences.

- La bande « des 2.4 GHz » : 83 MHz alloués aux WLAN
- La bande « des 5GHz » : 200 MHz alloués aux WLAN



La bande ISM

1.9. Bande de fréquence

Bande 2,4 GHz (métropole)

Norme 802.11b (Wifi et Bluetooth)

Limite des puissances PIRE en Wi-Fi:

Fréquences en MHz	Intérieur	Extérieur
2,400 GHz à 2,454 GHz	100 mW	100 mW
2,455 GHz à 2,4835 GHz		10 mW

1.10. Principales normes IEEE 802.11

802.11a (WiFi5)	1999	54 Mbit/s théoriques Bande des 5 GHz Incompatible avec 802.11b, g et n
802.11b (WiFi)	Septembre 1999	11 Mbit/s théoriques Bande des 2.4GHz
802.11g	Juin 2003	54 Mbit/s théoriques Bande des 2.4 GHz Compatibilité ascendante avec la norme 802.11b
802.11i	Juin 2004	Améliore la sécurité des transmissions S'appuie sur l'AES (Advanced Encryption Standard) Chiffrement des communications pour les transmissions utilisant les technologies 802.11a, 802.11b et 802.11g.
802.11n	Ratification prévue fin 2006 mais...!	Evolution rétrocompatible des normes 802.11b/g. Débits de 300 Mbit/s

1.11. Autres normes IEEE 802.11

802.11d	Pour une utilisation internationale des réseaux locaux 802.11, permet aux différents d'échanger des informations sur les plages de fréquence et les puissances autorisées dans le pays d'origine du matériel.
802.11c	Modification de la norme 802.1d afin de pouvoir établir un pont avec les trames 802.11 (niveau liaison de données).
802.11e	Introduction de qualité de service au niveau de la couche liaison de données.
802.11f	Recommandation à l'intention des vendeurs de point d'accès pour une meilleure interopérabilité des produits.
802.11h	Conformité avec la réglementation européenne en matière de fréquence et d'économie d'énergie

1.12. Normes concurrentes d'IEEE 802.11

- ❑ Bluetooth (IEEE 802.15) : Pas vraiment concurrente, car Bluetooth concerne les WPAN et non les WLAN.
- ❑ Hiperlan/2 (*High Performance Radio LAN*) : La concurrente européenne de la norme IEEE 802.11. Même couche physique que IEEE 802.11a. Pas d'applications commerciales.

1.13. Architecture physique : deux modes de configuration

❑ Mode infrastructure

- Les hôtes sans fil sont organisés en cellules autour d'un point d'accès
- Les points d'accès sont eux-mêmes connectés à un réseau local filaire.
- La communication entre deux hôtes de deux cellules distinctes passe via les point d'accès par le réseau filaire.

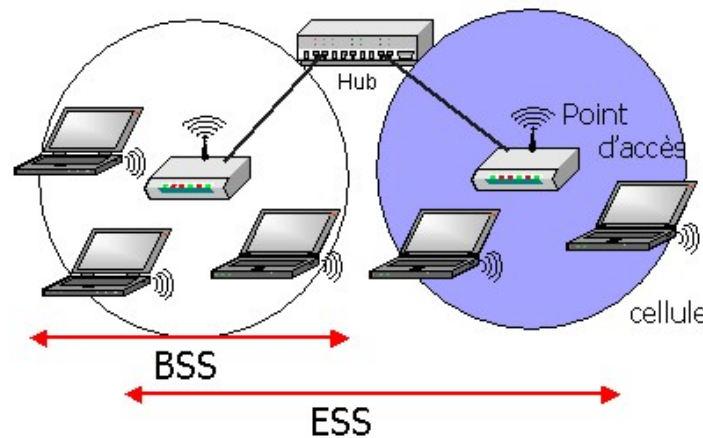
❑ Mode sans infrastructure (= mode ad hoc)

- Pas de point d'accès
- Chaque hôte sans fil fait office de routeur pour acheminer les communications

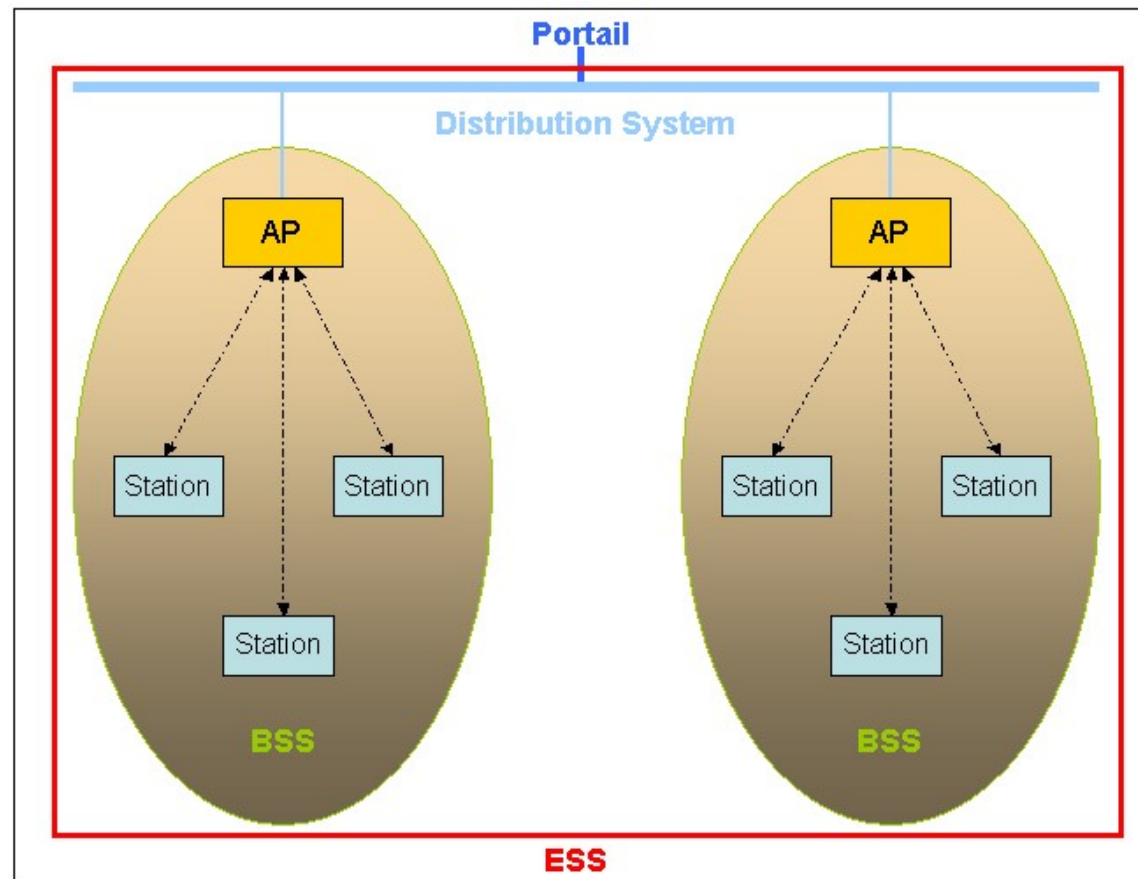
1.13.1. Mode infrastructure (1/2)

❑ Des points d'accès sont connectés au réseau local filaire. Chacun définit une cellule.

- Cellule = BSS (*Basic Service Set*)
- Les communications émises par toutes les stations passent par un point d'accès (AP *Access Point*) : il peut y avoir un ou plusieurs AP.
- Les AP sont interconnectés par le DS (*Distribution System*), par exemple Ethernet.
- Les BSS connectés en sous-réseau constituent l'ESS (*Extended Service Set*).

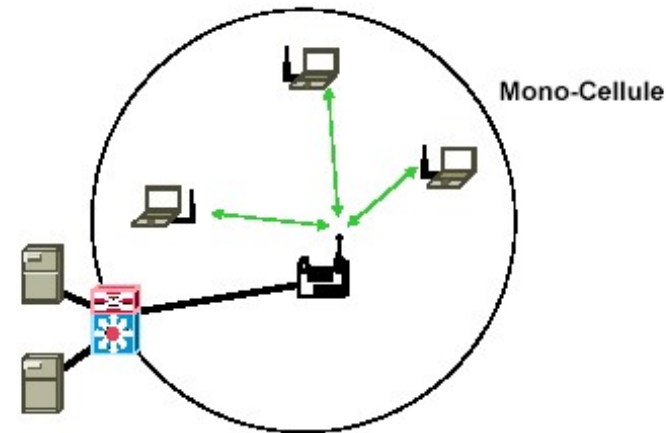


1.13.1. Mode infrastructure (2/2)

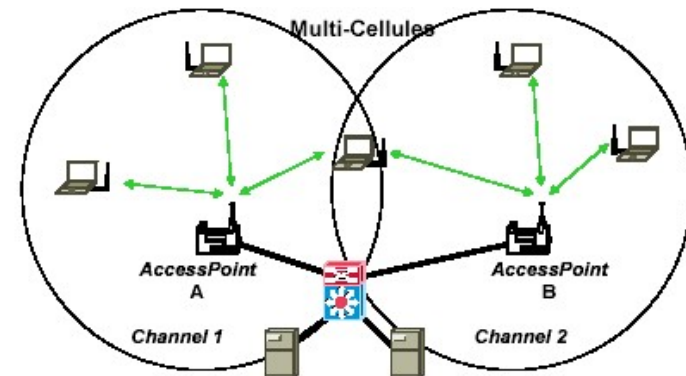


1.13.2. Exemples de configurations avec infrastructure

❑ La plus courante : **monocellule** interconnectée avec un réseau filaire



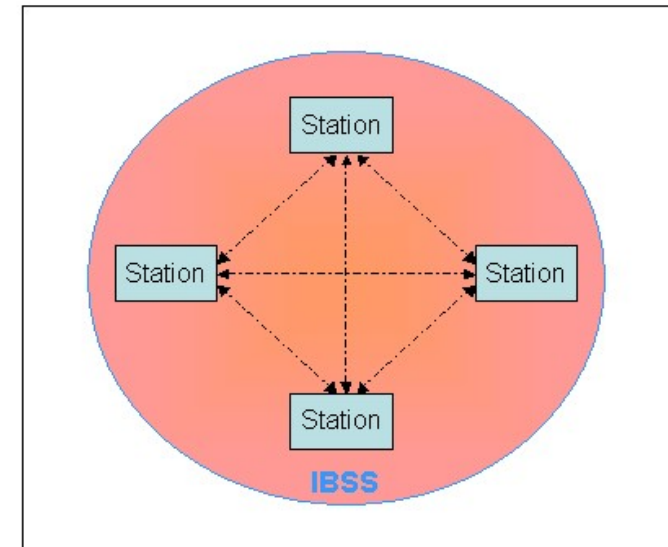
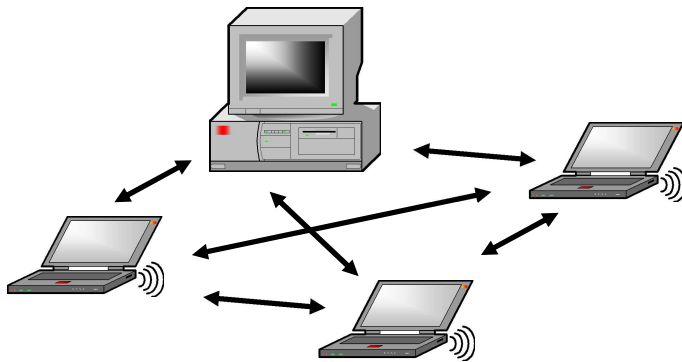
❑ **Multicellules** : plusieurs canaux, couverture étendue, mais problème du *handover*



1.13.3. Mode sans infrastructure (ad hoc)

❑ Mode ad hoc : Mode sans infrastructure.

- Réalise un réseau **poste à poste** (chaque poste peut communiquer avec chacun des autres postes).
- Un poste fait à la fois office d'hôte et de routeur.
- Également appelé **IBSS** (*Independent Basic Service Set*).

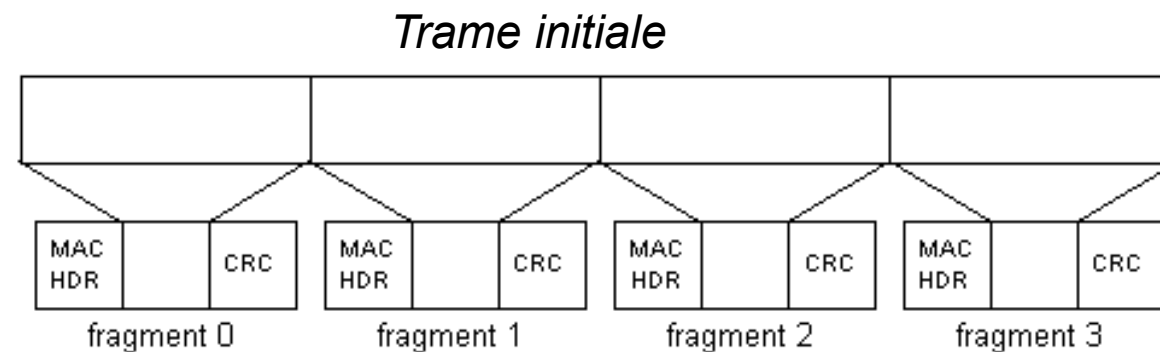


1.14. Virtual Carrier Sense

- Le **VCS** consiste à « réserver » le support avant émission.
- Avant de transmettre, si le support est libre
 - L'émetteur émet une trame **RTS** (@src, @dest, durée transaction = paquet+ACK)
 - Si le support est libre, le récepteur émet un **CTS**
 - Toute station entendant le RTS ou le CTS déclenche son **NAV** (*Network Allocation Vector*) et se tait pendant toute la durée de la communication.
- La probabilité de collision par une station cachée de l'émetteur est limitée à la courte durée du **RTS**.
- Si données courtes, pas de RTS ni CTS.

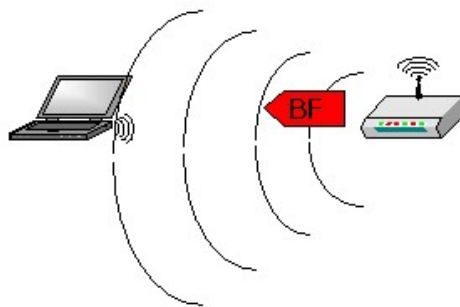
1.15. Fragmentation et réassemblage

- ❑ En sans fil, besoin de **petits paquets**
 - La **probabilité d'erreur augmente avec la taille du paquet**
 - Moins de **BP** gâchée par retransmission
 - Nécessaire si FHSS pour limiter le risque d'interruption de la transmission
- ❑ Fragmentation et réassemblage gérés au niveau de la **couche MAC**

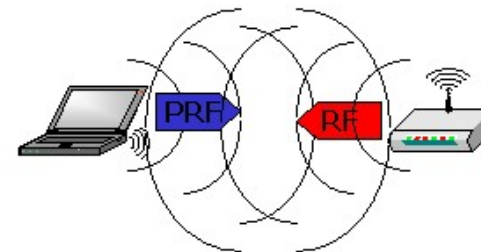


1.16. Entrée d'une station dans une cellule

- ❑ Après allumage, mode veille ou déplacement géographique, une station veut joindre un BSS
- ❑ **Synchronisation** sur l'AP (ou sur les autres stations dans le mode ad hoc)
 - Par **écoute passive** : écoute des trames balise (*beacon*) émises périodiquement par l'AP
 - Ou par **écoute active** : émission d'une requête *Probe Request Frame*, et attente de la réponse de l'AP
- ❑ **Authentication** : L'AP et la station se prouvent leur identité (par connaissance d'un mot de passe). Un « mode ouvert », sans authentication existe aussi.
- ❑ **Association** : échange d'information sur les stations de la cellule et leur capacité, enregistrement de la position des stations par l'AP



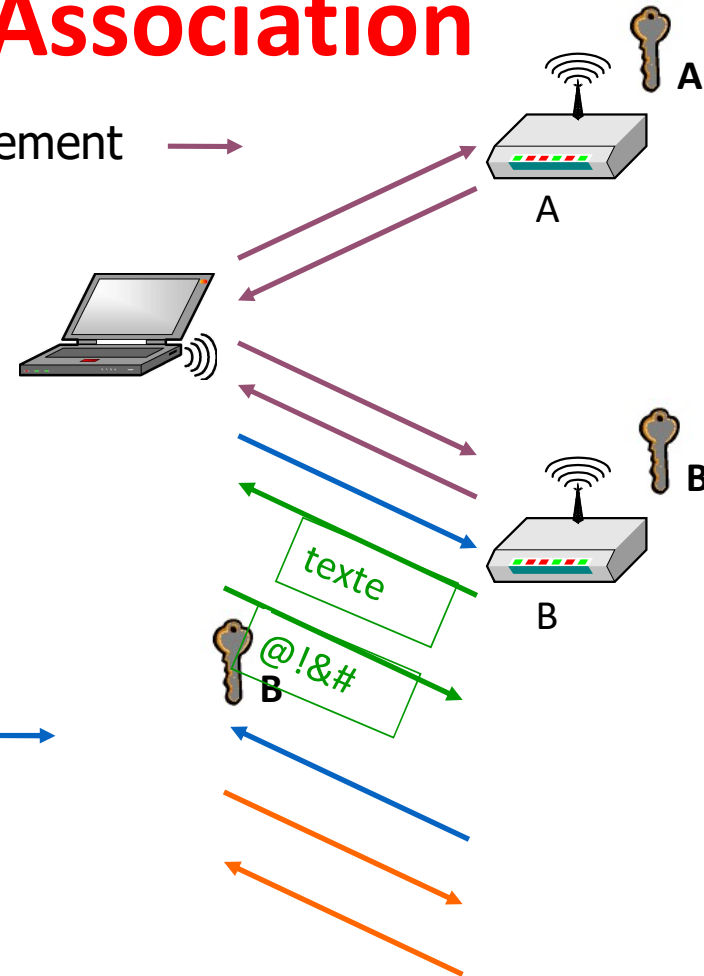
Ecoute passive



Ecoute active

1.17. Authentification et Association

- La station diffuse une demande d'enregistrement →
- Les points d'accès répondent →
 - La station évalue la réponse et sélectionne le meilleur point d'accès
- La station émet une trame « demande d'authentification » →
- Le PA envoie un texte →
- La station chiffre le texte avec la clé d'authentification de l'AP →
- Le PA confirme l'authentification du poste →
- La station envoie une demande d'association à l'AP →
- L'AP confirme l'association →



1.18. Handover

- ❑ Parfois appelé *roaming*.
- ❑ = Passage d'une station mobile d'une cellule à une autre
- ❑ N'est effectué qu'entre deux transmissions de paquets
- ❑ Peut affecter les performances à cause des retransmissions engendrées par les possibles déconnexions
- ❑ La norme ne définit pas la manière d'effectuer le *roaming* mais donne juste des principes à respecter

1.19. Attaques sur les réseaux sans fil

☐ Trois attaques essentiellement

- L'**écoute** (*eavesdropping*) : espionnage
- Le **brouillage** (*jamming*) : déni de service
- Ajout ou modification de données

1.20. Sécurité dans la norme IEEE 802.11 initiale

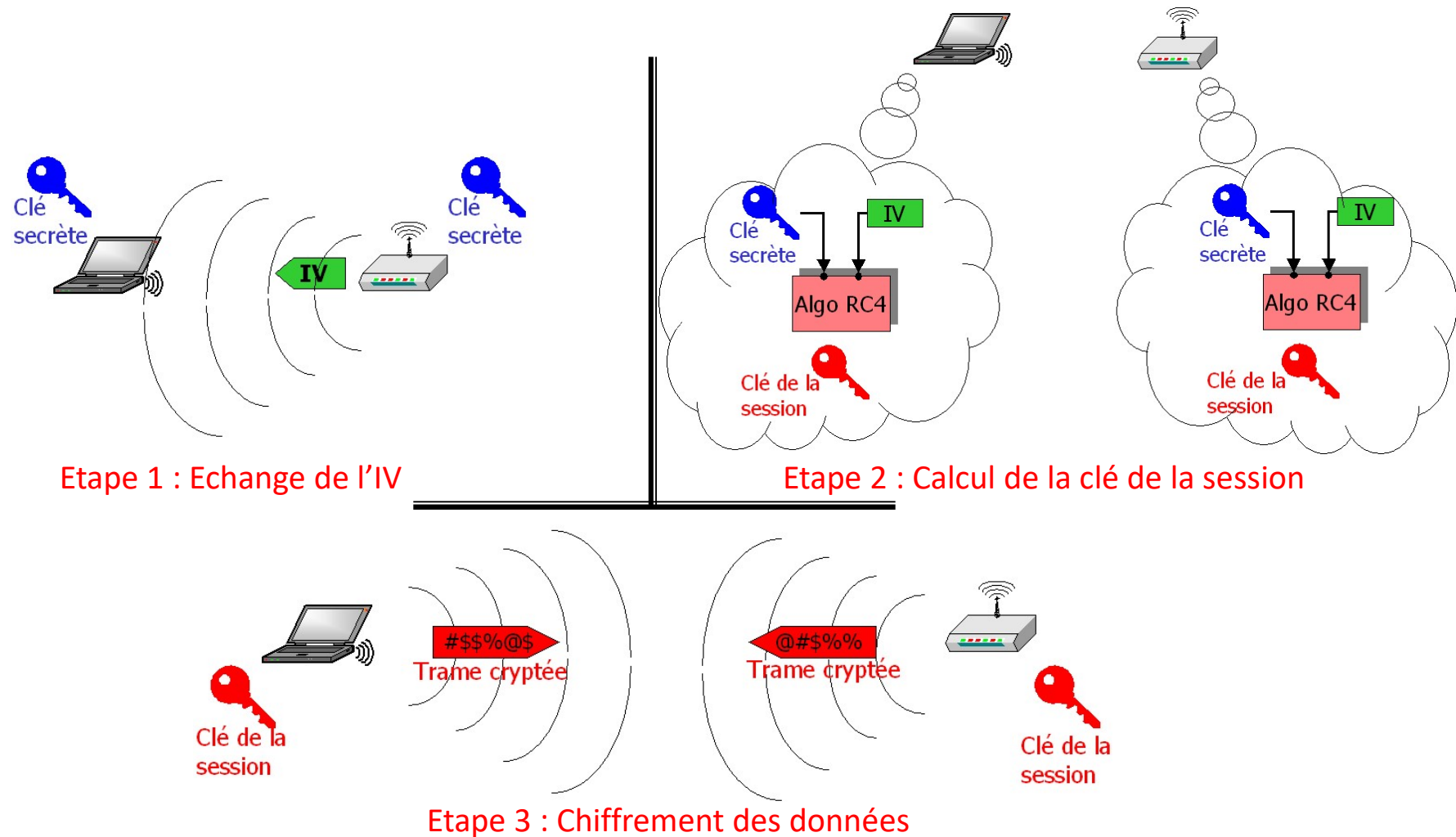
❑ Enjeux

- Empêcher un intrus de se connecter au réseau
- Empêcher l'écoute clandestine des données échangées

❑ « Solution » de la norme initiale: WEP (*Wired Equivalent Privacy*)

- Une clé secrète (40 bits) est partagée entre l'AP et les stations (échangée par voie sure).
- L'AP transmet en clair un mot initial IV (*Initial Vector*)
- La clé combinée à l'IV est utilisée pour générer une clé de 40 bits pseudo-aléatoire via un algorithme
- Les données sont chiffrées à partir de cette clé et ainsi émises
- Clé de 64 ou 128 bits

1.21. Fonctionnement du protocole WEP



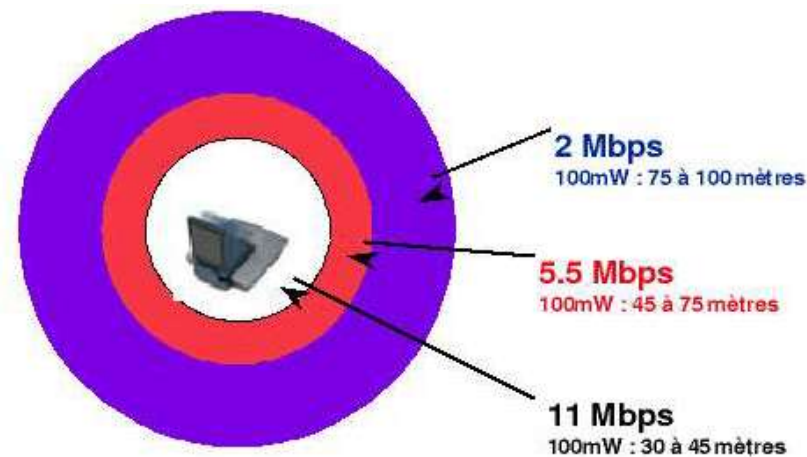
1.22. Failles du protocole WEP

- ❑ Possibilité de déchiffrer la clé dès que l'on connaît un couple « texte en clair, texte chiffré » de même IV
- ❑ Possibilité de trouver la clé WEP par une formule mathématique basée sur des IV « faibles »
- ❑ L'extension **IEEE 802.11i** apporte des **solutions** à ces failles de sécurité.

1.23. Norme IEEE 802.11b

❑ Le débit se dégrade avec la distance.

- Selon Cisco :



❑ En pratique, portée et débit dépendent beaucoup de l'environnement :

- Type de construction (cloisons, murs)
- Implantation des antennes
- Interférences (Bluetooth, fours micro-ondes, autres réseaux Wi-Fi).

1.24. Norme IEEE 802.11i

- ❑ Aussi appelée **norme WPA2**
- ❑ Vise à améliorer la sécurité des normes IEEE 802.11b et 8092.11g du point de vue du chiffrement et de l'authentification
- ❑ Chiffrement : failles du protocole WEP
 - Possibilité de casser la clé par écoute des communications
 - Solution : **changer la clé régulièrement** ⇒ **maintenance lourde** !
 - Tous les utilisateurs utilisent la même clé : possibilité d'écouter les communications des autres utilisateurs du réseau

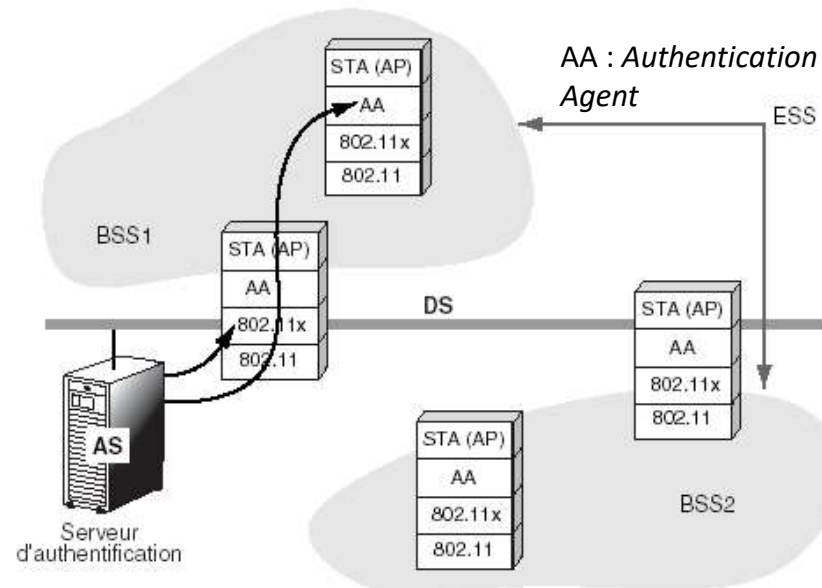
1.25. Norme IEEE 802.11i

- ❑ Solution pour le chiffrement : IEEE 802.11i repose sur le standard WPA (*Wi-Fi Protected Access*)
 - Le protocole TKIP (*Temporal Key Integrity Protocol*) réalise un changement automatique des clés (1 clé par paquet, calculée à partir de la clé de la session, l'IV et l'adresse MAC) et ajoute à chaque trame un code d'intégrité MIC (*Message Integrity Code*) sur l'entête et les données
 - L'algorithme de chiffrement AES (*Advanced Encryption Standard*) est implémenté. Plus robuste que WEP.

1.26. Norme IEEE 802.11i

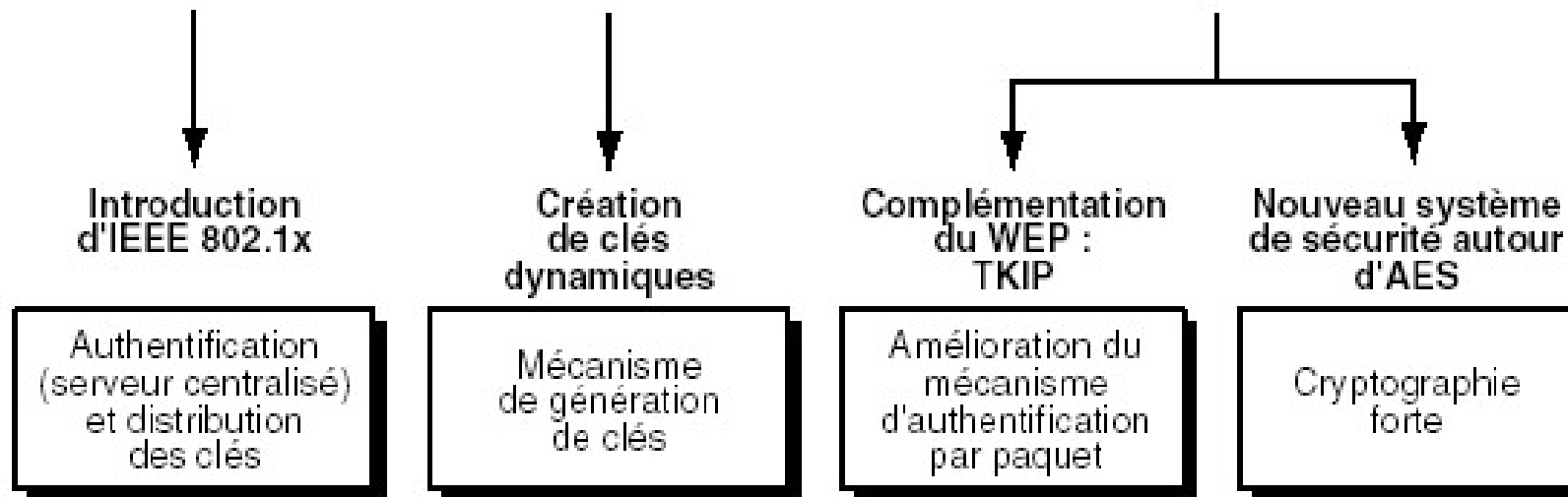
- ❑ Problèmes de l'authentification dans IEEE 802.11 : basée sur une clé WEP, méthode peu robuste.
- ❑ Intégration de la norme IEEE 802.11x, qui permet la mise en place de procédures d'authentification dans un réseau avec ou sans fil.
 - Un **serveur d'authentification** identifie les stations souhaitant se raccorder au réseau. Il peut de plus assurer la **distribution de clés dynamiques**.

La station envoie les informations d'authentification au point d'accès, qui les relaie par le système de distribution vers le serveur d'authentification AS. Ce dernier authentifie la station IEEE 802.11.



1.27. Norme IEEE 802.11i

❑Résumé :



❑ Cependant, peu de recul sur ces algorithmes. On conseille l'utilisation d'**IPSEC** pour garantir la confidentialité des échanges.



Réseaux sans fil

B. Tanguy KABORE

Doctorant IT

tanguykabore@yahoo.fr

Partie 2: WiMAX

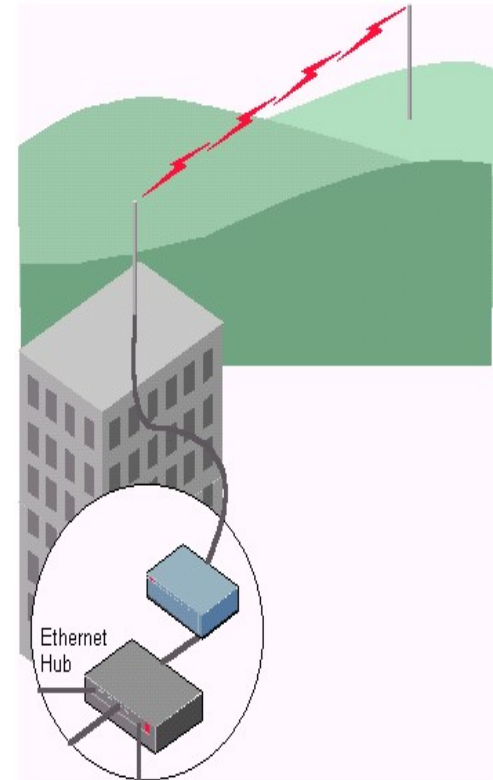
1.1. WMAN

❑ Définition

- Réseau **métropolitain** (Wireless Metropolitan Area Network)
- Plus connu sous le nom de **Boucle Local Radio (BLR)**
- Permet à un particulier ou une entreprise d'être relié à son opérateur (téléphonie fixe, Internet, télévision...) via les **ondes radio**.
- Basé sur la norme **802.16**

❑ Technologies

- Local Multipoint Distribution Service (**LMDS**)
- Multi Channel Multipoint Distribution Service (**MMDS**)
- Worldwide Interoperability for Microwave Access (**WiMAX**)



1.2. Worldwide Interoperability for Microwave Access

- ❑ Un standard de communication sans fil;
- ❑ Un mode de transmission et d'accès à Internet haut débit, portant sur une zone géographique étendue;
- ❑ **WiMAX** est le label commercial délivré par le *WiMAX Forum*;
- ❑ Se présente en deux versions: fixe et mobile.



1.3. Objectif

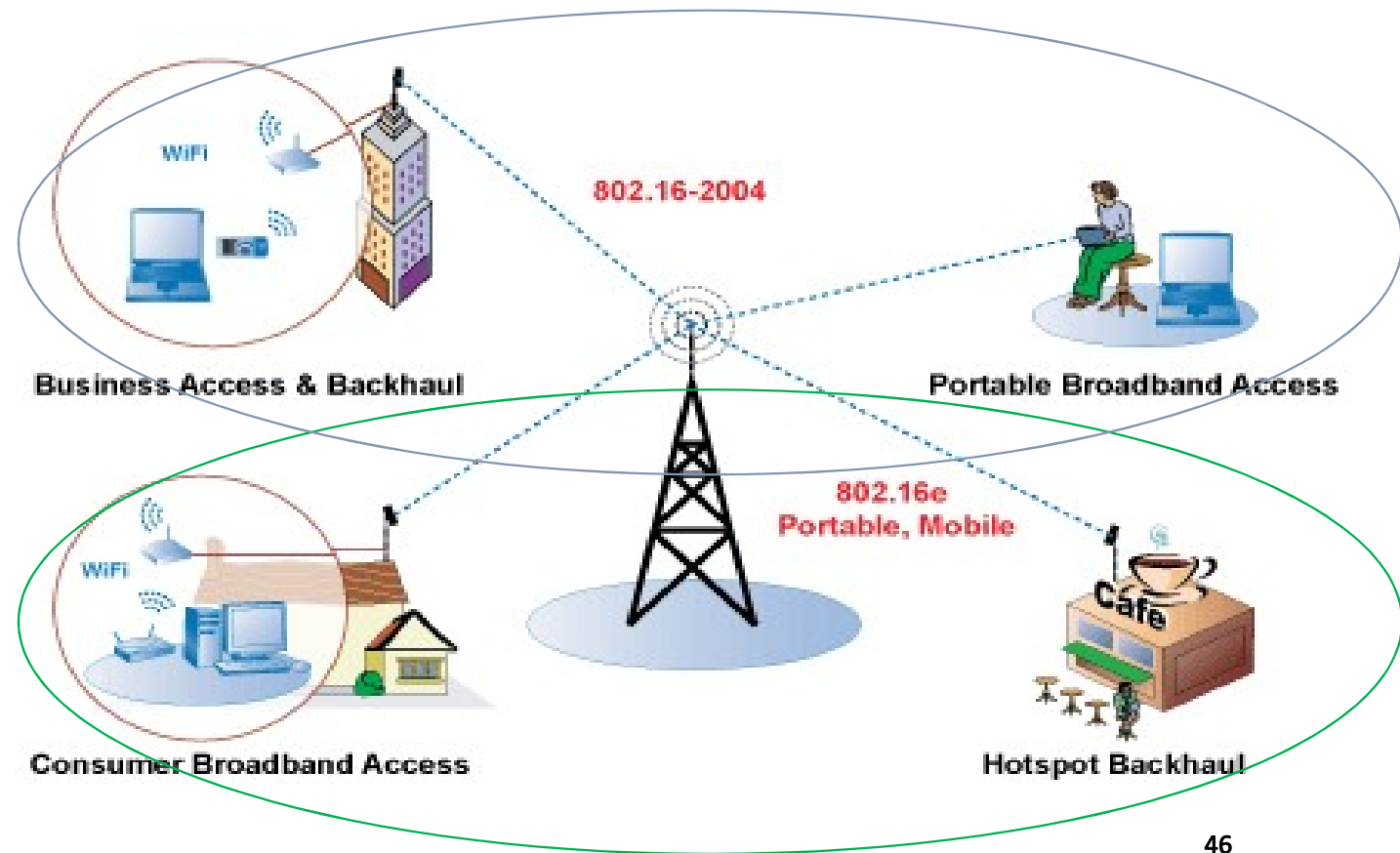
❑ Fournir une Technologie hertzienne pour la transmission de données :

- Téléphoner (VoIP);
- D'interconnecter des réseaux d'entreprises;
- Surfer sur Internet à haut débit, sur une zone de couverture de plusieurs kilomètres ;
 - En théorie : 74 Mbit/s avec une portée de 50 kilomètres.
 - En réalité : 12 Mbit/s avec une portée de 4,5 kilomètres.

1.4. VERSION DU WIMAX

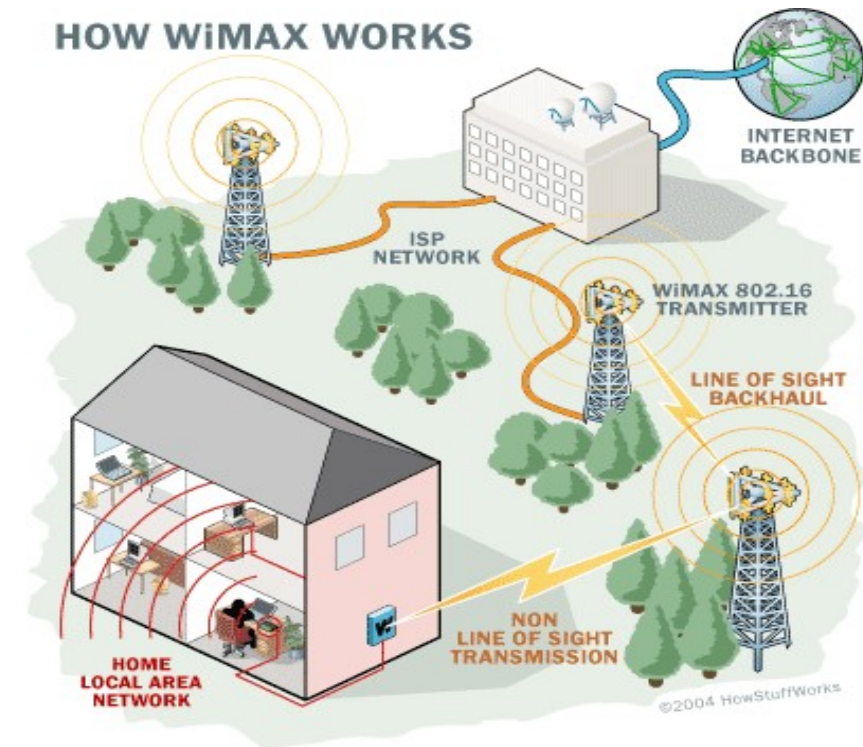
Le WiMax se présente sous deux versions:

- ❖ **Fixe**: remplacer l'ADSL dans les zones rurales.
- ❖ **Mobile**: permet d'avoir un modem ADSL dans sa poche et d'être toujours connecté.



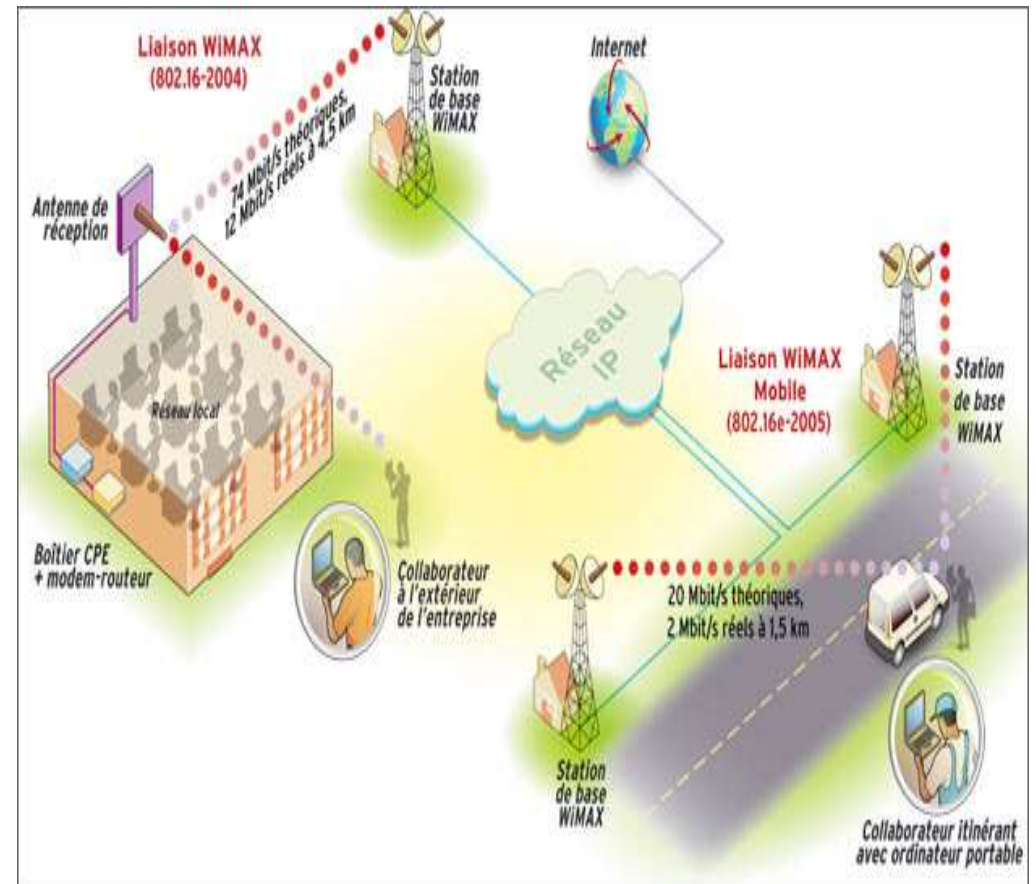
1.5. WIMAX FIXE-IEEE 802.16-2004

- ❑ Prévu pour un **usage fixe** ;
- ❑ Antenne semblable à l'antenne TV;
- ❑ Spectre de fréquence : entre **2.5 GHz** et **3.5 GHz** ;
- ❑ Débit théorique : **75 Mbps** ;
- ❑ Portée : **10 Km** ;



1.6. WIMAX MOBILE-802.16E-2005

- ❑ Prévoit la possibilité de connecter des **clients mobiles** à internet ;
- ❑ Permet le passage d'une antenne à une autre d'où la mobilité ;
- ❑ Permet une **connexion omniprésente** par l'intermédiaire d'un appareil mobile ;
- ❑ Permet la téléphonie IP Mobile ;
- ❑ plage de fréquence : **2 GHz à 6 GHz** ;
- ❑ un débit théorique maximal : **30 Mbps** ;
- ❑ Portée : **3.5 Km** .



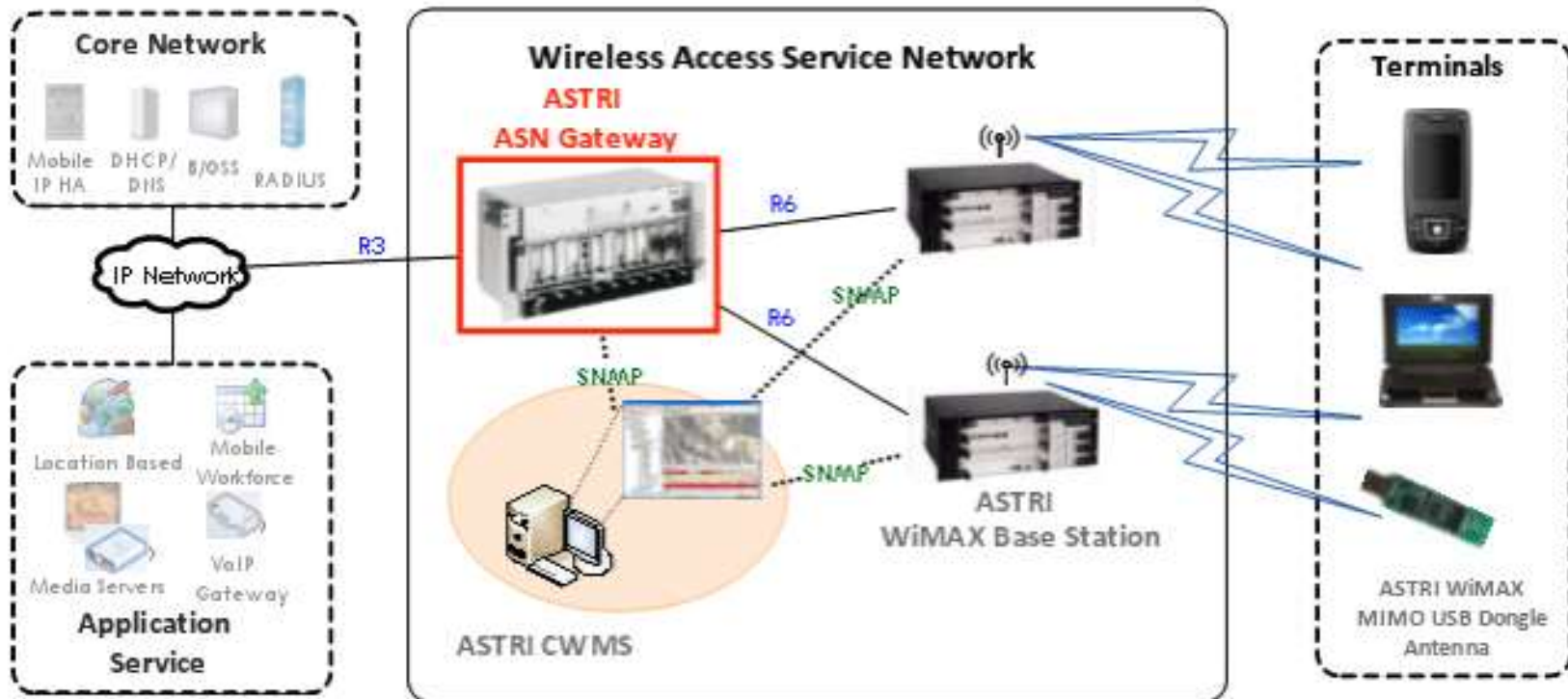
1.7. PRINCIPE DE FONCTIONNEMENT

- ❑ Le Wimax fonctionne avec un Principe de **station de base** et des **Stations d'abonnés** reliées par des antennes.
- ❑ Le réseau peut être subdivisé en deux sous réseaux :
 - Le **backhaul** :
 - Constitue le réseau formé par l'**ensemble des BS** interconnectées **point à point** entre elles,
 - nécessité d'une visibilité directe (**LOS**) entre deux BS.
 - Le **réseau d'accès** :
 - C'est une liaison **point à multipoint** entre une BS et plusieurs SS.
 - Une visibilité directe peut ne pas être nécessaire (**NLOS**).

1.8. ARCHITECTURE DU WIMAX

Un réseau WiMax comprend **trois parties**:

- ❖ la Radio;
- ❖ le cœur du réseau IP ;
- ❖ les équipements terminaux.



1.9. FAMILLE 802.16

Standard	Description	Publié	Statut
IEEE std 802.16-2001	définit des réseaux métropolitains sans fil utilisant des fréquences supérieures à 10 GHz (jusqu'à 66 GHz)	8 avril 2002	obsolètes
IEEE std 802.16c-2002	définit les options possibles pour les réseaux utilisant les fréquences entre 10 et 66 GHz.	15 janvier 2003	
IEEE std 802.16a-2003	amendement au standard 802.16 pour les fréquences entre 2 et 11 GHz.	1 ^{er} avril 2003	
IEEE std 802.16-2004 (également désigné 802.16d)	il s'agit de l'actualisation (la révision) des standards de base 802.16, 802.16a et 802.16c.	1 ^{er} octobre 2004	obsolète/actifs
IEEE 802.16e (également désigné IEEE std 802.16e-2005)	apporte les possibilités d'utilisation en situation mobile du standard, jusqu'à 122 km/h ¹ .	7 décembre 2005	actifs
IEEE 802.16f	Spécifie la MIB (Management Information Base), pour les couches MAC (Media Access Control) et PHY (Physical)	22 janvier 2006	
IEEE 802.16m	Débits en nomade ou stationnaire jusqu'à 1 Gbit/s et 100 Mbit/s en mobile grande vitesse. Convergence des technologies Wi MAX, Wi-Fi et 4G	2009 (IEEE 802.16-2009)	actifs

1.10. Applications

Le caractère de mobilité ainsi que les coûts d'installations réduits, ouvre la voie à de nombreuses applications pour le WiMax :


- ❑ Offres commerciales **grand public triple play** : données, voix, télévision ;
- ❑ Couvertures conventionnelles de **zones commerciales** (« hot zones ») : zones d'activité économique, parcs touristiques, centres hôteliers... ;
- ❑ **Déploiements temporaires** : chantiers, festivals, infrastructure de secours sur une catastrophe naturelle... ;
- ❑ Gestion de **réseaux de transports intelligents** ;
- ❑ **Zone hospitalière** étendue (lieu médicalisé) ;
- ❑ **Sécurité maritime** et **sécurité civile** ;
- ❑ **Systèmes d'information géographique** déportés
- ❑ **Métérologie** (télémessure, pilotage à distance, relevés géophysiques...)

1.11. Etablissement d'une connexion

la station cliente (SS) envoie une demande de connexion.




Si le client à les droits nécessaires, la BS autorise l'accès au réseau et envoie un acquittement crypté avec la clé publique du client.



Authentification de la BS devant le client.



Le client vérifie l'identité de la BS puis s'enregistre sur le réseau, il reçoit par la suite un acquittement crypté,



la connexion est maintenant établie et sécurisée.

1.12. WIMAX ET WI-FI

	Wi-Fi	WIMAX
Services offerts	Wireless LAN	<i>(Broad band Wireless Access) BWA</i>
zone de couverture	20m à 50	50Km(LOS) et 1 à 7Km(NLOS).
bande passante :	2.4 GHz ISN soit 25 Mhz par canal.	2 GHz à 11 GHz. 11 GHz à 66 GHz,



Réseaux sans fil

B. Tanguy KABORE

Doctorant IT

tanguykabore@yahoo.fr

Partie 3: Réseaux mobiles

1.1. Introduction aux Réseaux Mobiles

- ❑ Les réseaux mobiles permettent la communication **sans fil** entre **appareils mobiles** et l'infrastructure réseau.
- ❑ Les réseaux sont **organisés en cellules**, chaque cellule étant desservie par une **station de base**.
- ❑ Principales générations de réseaux mobiles :
 - **2G** : Appels et SMS
 - **3G** : Internet mobile et services multimédia
 - **4G** : Haut débit mobile
 - **5G** : Faible latence et connexion massive d'appareils

1.2. Générations des Réseaux Mobiles

❑ 2G (GSM) : Début des réseaux numériques, appels vocaux, SMS.

❑ 3G (UMTS, CDMA2000) : Introduction de l'Internet mobile, accès aux e-mails, vidéos et services de données.

❑ 4G (LTE) : Réseau IP tout-en-un, haut débit mobile, services de streaming vidéo HD.

❑ 5G : Vitesse ultra-rapide, très faible latence, prise en charge des objets connectés (IoT).









1.3. Architecture d'un Réseau Mobile

- ❑ Station de base (BTS) : Fournit la connectivité sans fil aux appareils dans une cellule.
- ❑ Contrôleur de réseau radio (RNC) : Gère les ressources radio et le handover entre cellules.
- ❑ Nœud central (Core Network) : Gère les appels, l'acheminement des données et la mobilité.
- ❑ Backhaul : Connexion entre les stations de base et le cœur du réseau.

1.4. Technologies Clés des Réseaux Mobiles

- ❑ **GSM** (Global System for Mobile Communications) : Standard pour les communications 2G.
- ❑ **UMTS** (Universal Mobile Telecommunications System) : Standard pour les réseaux 3G.
- ❑ **LTE** (Long Term Evolution) : Technologie de réseau 4G pour la transmission de données à haute vitesse.
- ❑ **5G NR** (New Radio) : Norme pour les réseaux 5G, supportant des vitesses de transfert élevées et une faible latence.

1.5. Comparaison des réseaux mobiles

 1G <i>1^{er} génération de réseau mobile</i> <ul style="list-style-type: none">• services vocaux de base• basé sur des protocoles analogiques  2.4 Kbps	 2G <i>2^{ème} génération de réseau mobile</i> <ul style="list-style-type: none">• conçu pour la transmission de voix• couverture et capacité améliorée• première norme numérique  64 Kbps	 3G <i>3^{ème} génération de réseau mobile</i> <ul style="list-style-type: none">• conçu pour la transmission de voix avec des données (média, internet...)• premier mobile avec haut débit  2 Mbps	 4G <i>4^{ème} génération de réseau mobile</i> <ul style="list-style-type: none">• conçu principalement pour les données• vrai haut débit mobile  100 Mbps
--	--	---	--



Réseaux sans fil

B. Tanguy KABORE

Doctorant IT

tanguykabore@yahoo.fr

Partie 4: Réseaux de capteurs sans fil

Confer TP Guidé

