Université
De Boumerdes

Université
De Limoges

Département de physique/Infotronique
IT/S5

Réseaux locaux wifi

Réalisé par : Dr RIAHLA
Docteur de l'université de Limoges (France)
Maitre de conférences à l'université de Boumerdes

2008/2009

Plan

- Concepts des LAN sans fil
- Déploiement de LAN sans fil
- Sécurité des LAN sans fil

Concepts des LAN sans fil

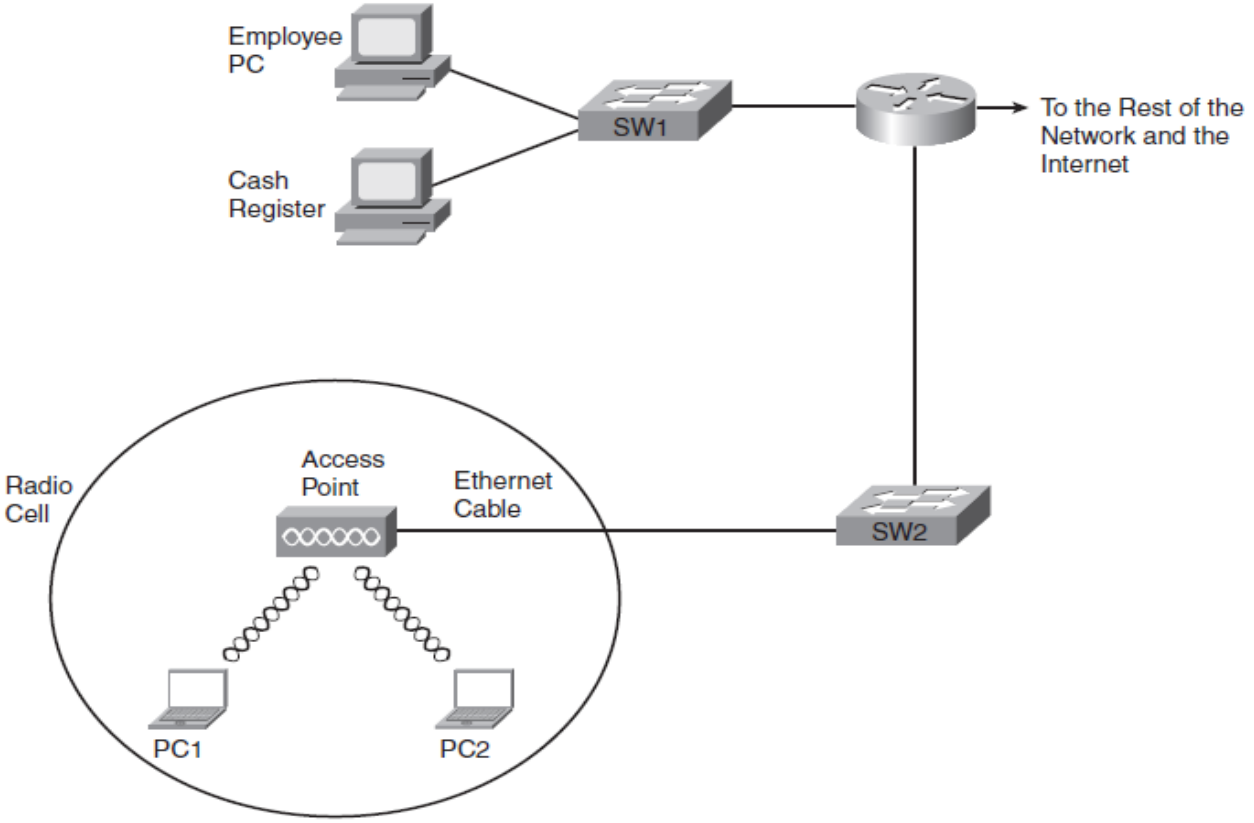
Concepts des LAN sans fil

- L'utilisation des Ordinateurs portables pour avoir des travailleurs mobiles

- La migration vers un modèle d'activité qui peut nécessiter de travailler n'import ou et d'etre connecté à internet en permanence.

stimule le développement des LANs sans fil.

Exemple
LAN sans fil dans une librairie



Le client utilise ses propres équipements

Concepts des LAN sans fil

- Les Pc équipés de fonctionnalités sans fil communiquent avec un point d'accès(AP, Acces point)

- AP permet d'échanger des trames avec les clients du LAN sans fil

Université
De Boumerdes

Université
De Limoges

LAN sans fil VS LAN Ethernet

2008/2009

LAN sans fil VS LAN Ethernet
Points communs

- Ils autorisent les communications entre les équipements

- Les deux définissent un format de trame avec un en-tète et un en-queue.

- L'en- tète contient un champ d'adresse MAC source et un champ d'adresse MAC destination de six octets chacun

- Elles définissent des règles sur la manière dont les équipements déterminent quand envoyer ou non des trames

LAN sans fil VS LAN Ethernet Différence

- **LAN sans fil** utilisent des ondes radio qui traversent l'espace.
- **LAN Ethernet** emploie des signaux électroniques (ou des signaux lumineux).

- La famille IEEE 802.3 Pour les LANs Ethernet
- La famille IEEE 802.11 Pour les LANs sans fils

LAN sans fil VS LAN Ethernet
Différence

- **Ethernet** peut prendre en charge les communication full-duplex (avec les commutateurs) donc pas de CSMA/CD.

- Si plusieurs équipements sans fils envoi simultanément des ondes radio dans le même espace sur la même fréquence, il faut avoir recours au half-duplex.
- WLAN utilisent CSMA/CA pour appliquer le HDX et éviter les collisions

Organismes qui influencent les normes des WLAN

Organization	Standardization Role
ITU-R	Worldwide standardization of communications that use radiated energy, particularly managing the assignment of frequencies
IEEE	Standardization of wireless LANs (802.11)
Wi-Fi Alliance	An industry consortium that encourages interoperability of products that implement WLAN standards through their Wi-Fi certified program
Federal Communications Commission (FCC)	The U.S. government agency with that regulates the usage of various communications frequencies in the U.S.

Normes de WLAN

IEEE

- 802.11
- 802.11a
- 802.11b
- 802.11g
- 802.11n (pas encore ratifiée!!!?)

Normes de WLAN

Feature	802.11a	802.11b	802.11g
Year ratified	1999	1999	2003
Maximum speed using DSSS	—	11 Mbps	11 Mbps
Maximum speed using OFDM	54 Mbps	—	54 Mbps
Frequency band	5 GHz	2.4 GHz	2.4 GHz
Channels (nonoverlapped)*	23 (12)	11 (3)	11 (3)
Speeds required by standard (Mbps)	6, 12, 24	1, 2, 5.5, 11	6, 12, 24

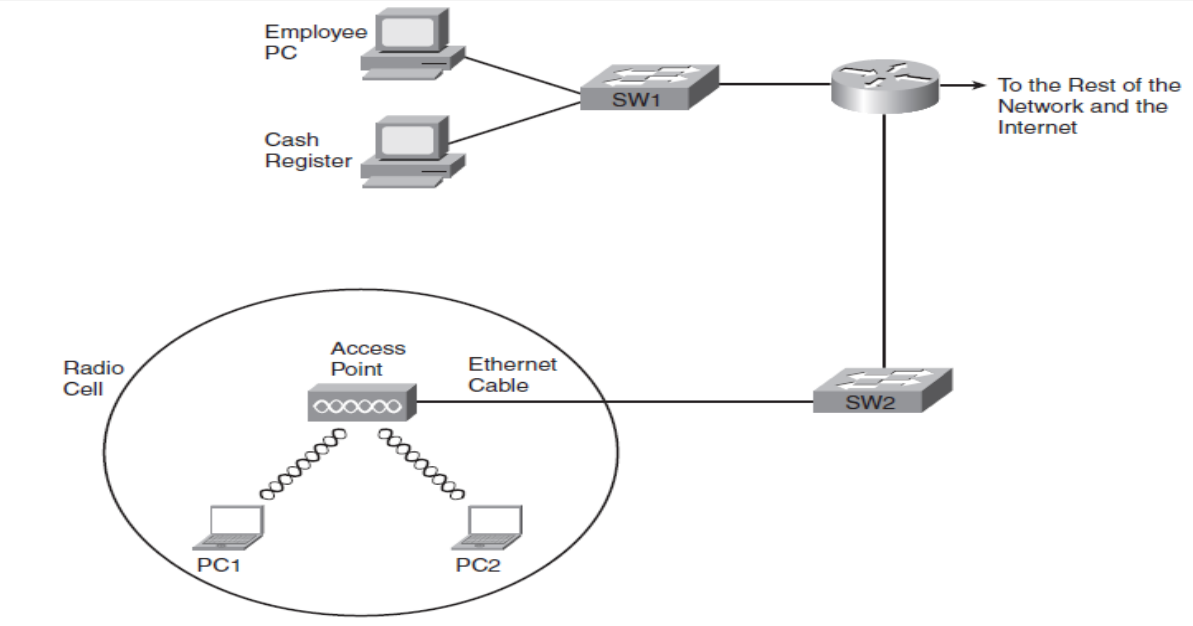
Modes des WLAN

Mode Ad hoc

- Un équipement sans fil communique directement avec un ou un nombre réduit d'autres équipements pendant une courte durée
- => **Echange de trames direct**

Mode infrastructure

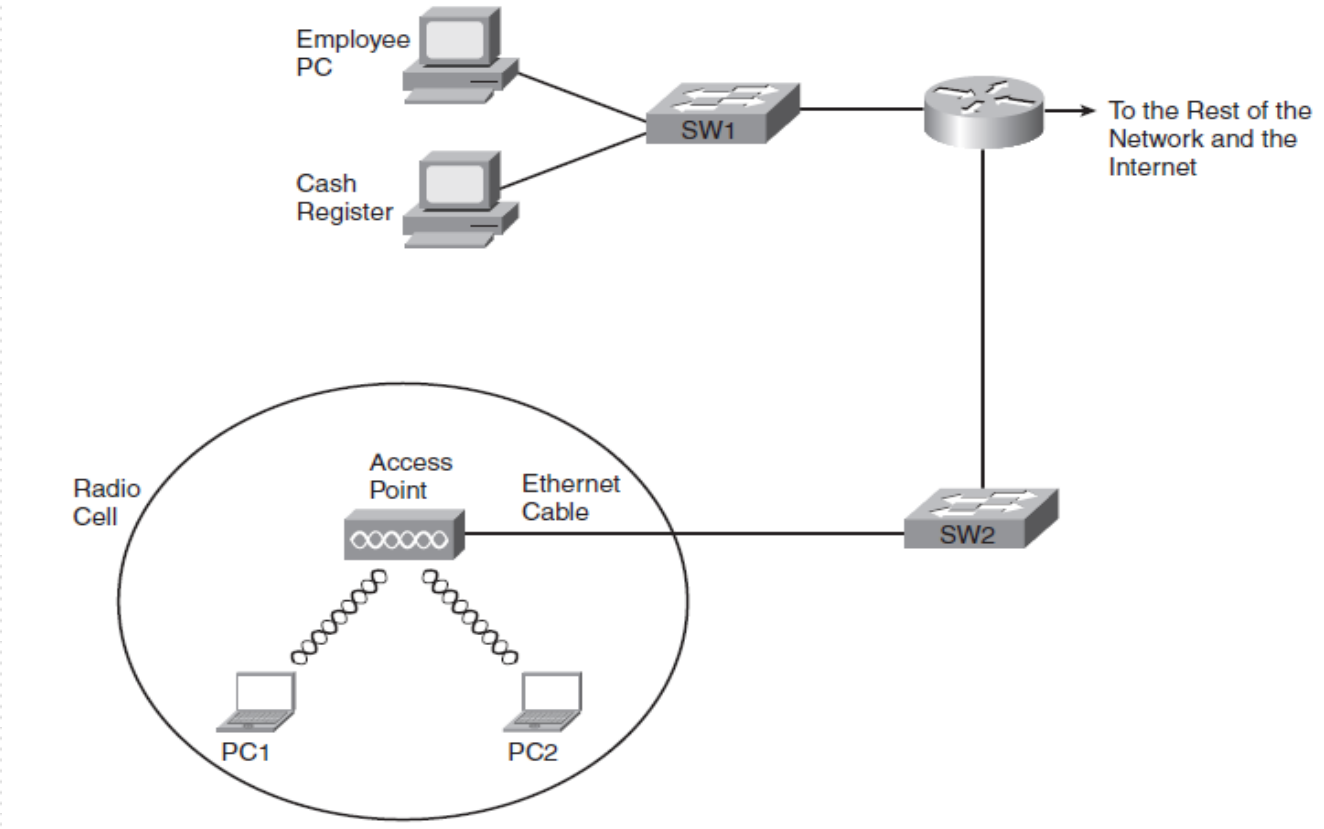
In infrastructure mode, each device communicates with an AP, with the AP connecting via wired Ethernet to the rest of the network infrastructure. Infrastructure mode allows the WLAN devices to communicate with servers and the Internet in an existing wired network,



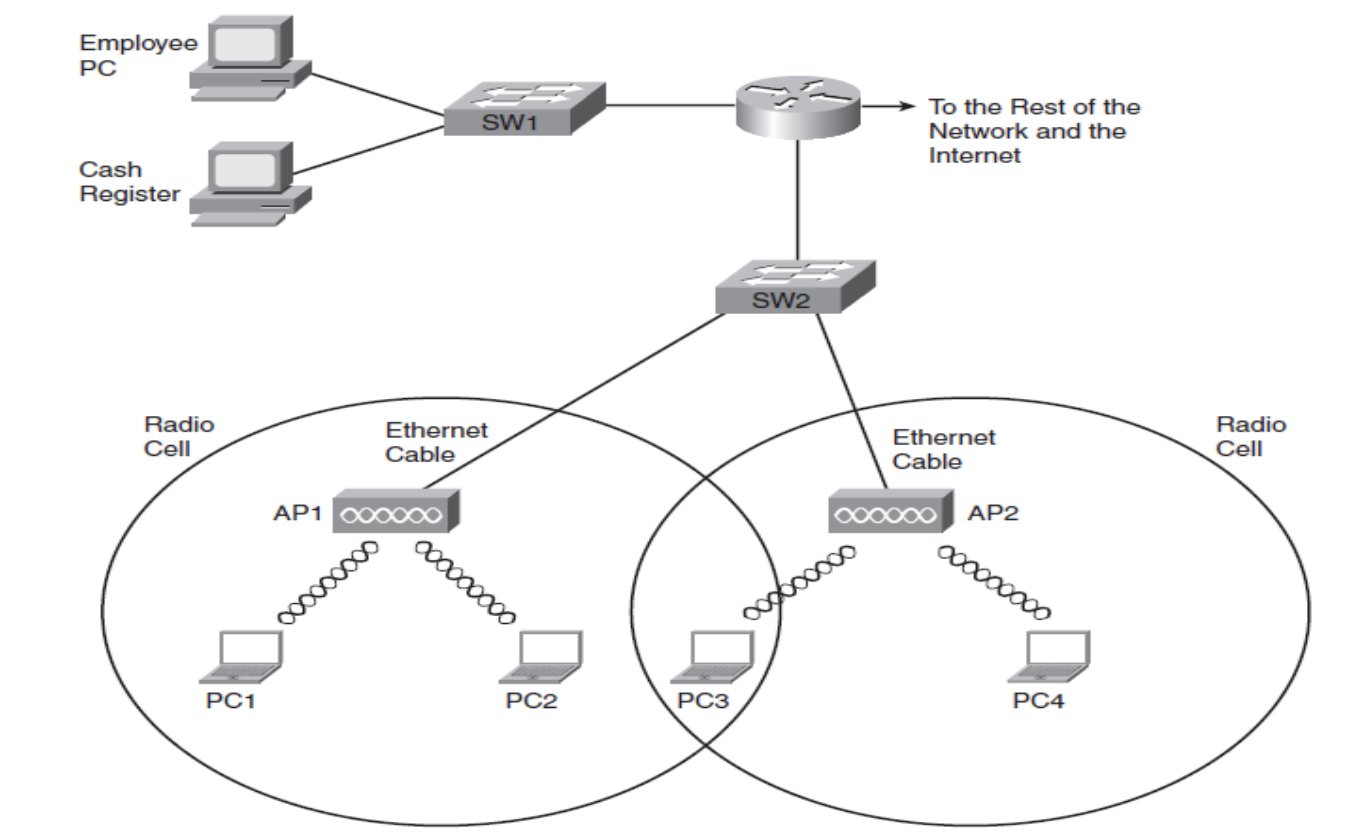
Mode infrastructure

- Prend en charge deux ensembles de services:

Mode infrastructure
BSS



Mode infrastructure
ESS



Des cellules qui se recouvrent➔ zone plus etendue

Mode infrastructure
ESS

- Les utilisateurs peuvent se déplacer dans la zone de couverture tout en restant connectés au même WLAN➔ pas de changement d'adresse IP

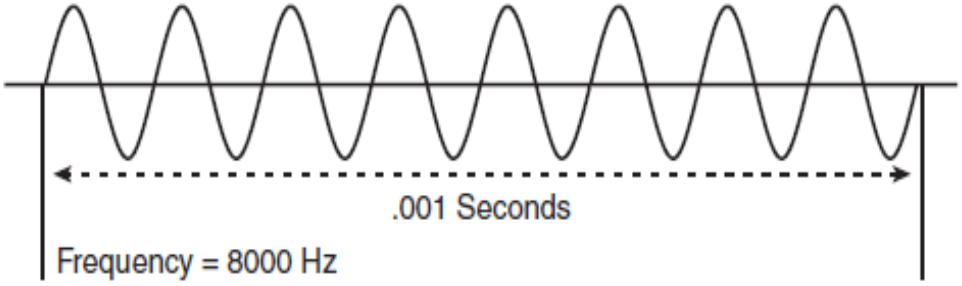
- Sentir les signaux faibles et forts

Modes des WLAN

Mode	Service Set Name	Description
Ad hoc	Independent Basic Service Set (IBSS)	Allows two devices to communicate directly. No AP is needed.
Infrastructure (one AP)	Basic Service Set (BSS)	A single wireless LAN created with an AP and all devices that associate with that AP.
Infrastructure (more than one AP)	Extended Service Set (ESS)	Multiple APs create one wireless LAN, allowing roaming and a larger coverage area.

Transmission sans fil (Couche 1)

- Electricité qui circule sur des fils de cuivres
- Lumière qui passe sur des câbles optiques
- Les ondes radio possèdent un signal qui se répète dans la durée



Transmission sans fil (Couche 1)

- Emission/réception ondes radio
- Les NIC et AP emploient des radio et des antennes pour envoyer, recevoir et modifier les radio pour encoder les données

- Pour éviter interférence entre les équipements, les administrations régulent et supervisent les plages de fréquences en usage dans chaque pays (ex: FCC en USA)
- AM et FM gérer par FCC

Transmission sans fil (Couche 1)

- Plage de fréquence=bande de fréquence
- Une station FM à besoin d'une fréquence d'environ 200KHZ, la FCC lui attribut une fréquence de base avec une marge de band passante de 100KHZ de part et d'autre

- Ex: FM émet sur la fréquence 96,5

Signal de base: 96,5MHZ
L'amplificateur radio utilise la bande de fréquence entre 96,4 et 96,6MHZ➔?
Plus band de fréquence grande=> plus d'informations envoyées (tèl requiert 4,5MHz)

Transmission sans fil (Couche 1)

- FCC et autres tiennent sous licences certaines bandes de fréquences, mais certaines sont libres.
- **Sous licences:**
  - AM
  - FM
  - Communications polices
  - Téléphones mobiles
- **Sans licence:**
- Les fours à micro-ondes rayonnent de l'énergie dans la bande sans licence de 2,4 GHZ, cette même bande est utilisée par certaines normes de WLAN et par de nombreux téléphones sans fil

Transmission sans fil (Couche 1)

Il arrive que vous ne puissiez pas entendre votre interlocuteur ou surfer sur le Net avec une liaison sans fil parce qu'une personne est en train de réchauffer son diner!!!

Bande de fréquence sans licence FCC

Frequency Range	Name	Sample Devices
900 KHz	Industrial, Scientific, Mechanical (ISM)	Older cordless telephones
2.4 GHz	ISM	Newer cordless phones and 802.11, 802.11b, 802.11g WLANs
5 GHz	Unlicensed National Information Infrastructure (U-NII)	Newer cordless phones and 802.11a, 802.11n WLANs

À Voir

- **Encodage?**
  - **DSSS,**
  - **FHSS,**
  - **OFDM**

Name of Encoding Class	What It Is Used By
Frequency Hopping Spread Spectrum (FHSS)	802.11
Direct Sequence Spread Spectrum (DSSS)	802.11b
Orthogonal Frequency Division Multiplexing (OFDM)	802.11a, 802.11g

- **Canaux non recouvrant?**

interférences

- Les ondes radio traversent l'espace et tout ce qui se trouve dans la zone de couverture:
  - Les mures
  - Les planchers
  - Les plafonds

- En traversant la matière, le signal est partiellement absorbé=> réduire sa force et la taille de la zone de couverture (surtout si la quantité de métal est importante).
- Ainsi les communications sans fil sont impactée par d'autres zones radio dans la même bande de fréquence.

interférences

- Mesuré l'Interférence => signal/bruit

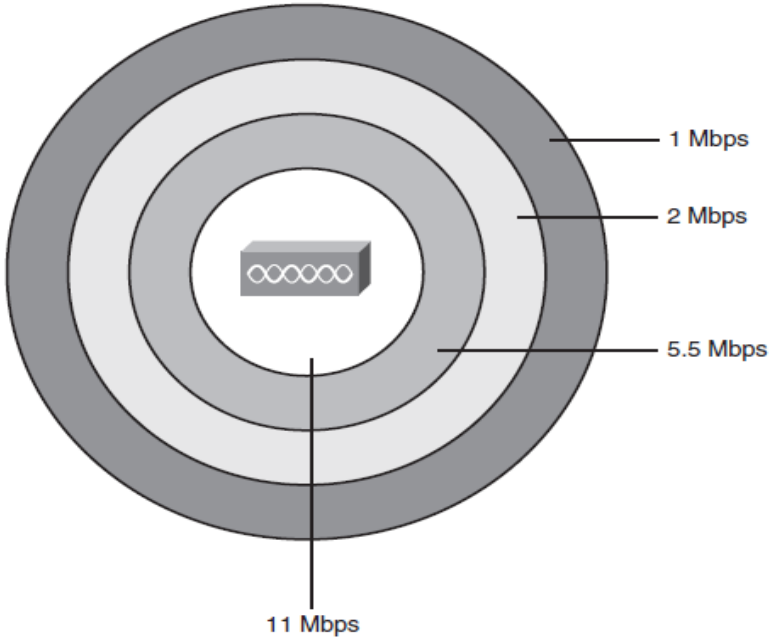
Zone de couverture, débit et capacité

- Zone de couverture?
- Une construction en béton armé réduit la zone de couverture. => les PA peuvent utiliser divers types d'antennes qui modifient la forme de la zone de couverture(antennes à gain?)
- Les signaux sans fil faibles ne peuvent pas transmettre des données à des vitesses élevées=> les normes de WLAN intègrent la notion de **vitesses multiples.**
- Equipement à proximité d'un PA => signal fort =>envoyer/recevoir à des vitesses élevées

Zone de couverture, débit et capacité

- Equipement situé au bord de la zone de couverture => signal faible=>envoyer/recevoir à des vitesses moins rapides

Réseau BSS
Norme IEEE 802.11b



Comment accroitre la taille de la zone de couverture?

- Utiliser des antennes spécialisées et augmenter la puissance du signal

- Comment? (à voir)

Transmission sans fil (Couche 2)

- CSMA/CD ETHERNET CLASSIQUE
- Si plusieurs équipements sans fils envoi simultanément des ondes radio dans le même espace sur la même fréquence, il faut avoir recours au half-duplex.
- Sinon=> aucun des signaux émis ne sera compris par les équipements récepteurs.

- L'équipement qui émet ne peut écouter en même temps
- Collision=> les émetteurs n'en ont pas directement connaissance

Transmission sans fil (Couche 2)

- Solution=> CSMA/CA
- Réduire le risque statistique de collisions
- CSMA/CA ne les évite pas réellement donc il faut intégré un processus pour les gérer lorsqu'elles se produisent.
- Utiliser des acquittements (sinon il renvoi)

Step 1	Listen to ensure that the medium (space) is not busy (no radio waves currently are being received at the frequencies to be used).
Step 2	Set a random wait timer before sending a frame to statistically reduce the chance of devices all trying to send at the same time.
Step 3	When the random timer has passed, listen again to ensure that the medium is not busy. If it isn't, send the frame.
Step 4	After the entire frame has been sent, wait for an acknowledgment.
Step 5	If no acknowledgment is received, resend the frame, using CSMA/CA logic to wait for the appropriate time to send again.

Déploiement de LAN sans fil

Déploiement de LAN sans fil

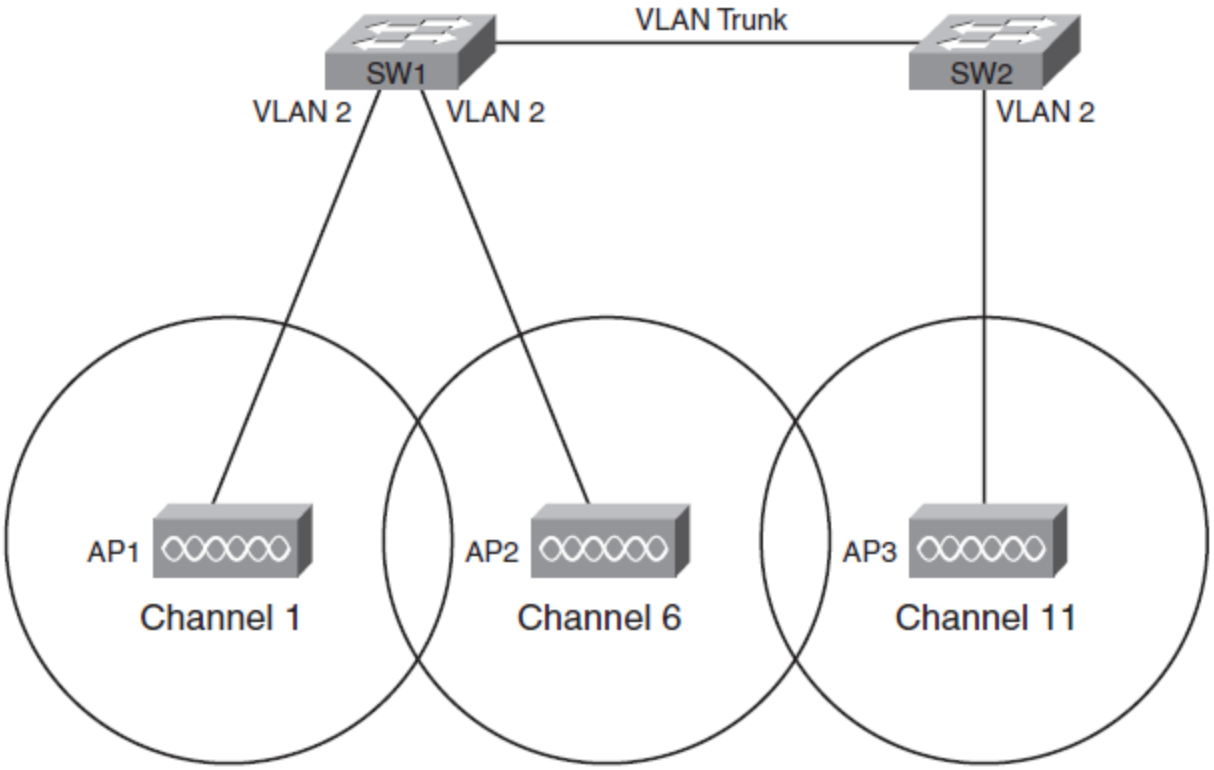
- Un bon déploiement pour une sécurité forte
- Mais d'abord, il faut installer:

1. Vérifié que le réseau filaire existant fonctionne (VLAN, Connexion Internet, DHCP,…etc.).
2. Installer le PA et configurer sa connectivité au réseau filaire(adresse IP, masque, Passerelle par défaut).
3. Configurer et vérifier les paramétrages du PA (dont le SSID).
4. Configurer et installer un client sans fil.
5. Vérifier que le LAN fonctionne depuis le client WLAN

Déploiement de LAN sans fil

6. Configurer la sécurité sans fil sur le client et le PA
7. Vérifier de nouveau que le LAN sans fil fonctionne en présence des fonctionnalités de sécurité

Etape 1: Vérifié que le réseau filaire existant fonctionne (voir cours licence)



Etape 1: Vérifié que le réseau filaire existant fonctionne

- **ESS**: tous les ports du commutateur auquel les points d'accès sont reliés doivent se trouver dans le même VLAN.

- Testez d'abord le port du PA par une carte Ethernet d'un ordinateur et voir si le DHCP vous donne IP, Masque,…etc.

Etape 2: Installer et configurer les aspects IP et filaires du PA

- Un PA fonctionne au niveau de la couche 2, mais le commutateur a besoin de lui affecter une adresse IP (voir configuration de l'adresse IP d'un commutateur c'est la même chose.).

- Un PA a besoin de :
  - Adresse IP
  - Masque
  - Passerelle par défaut
  - Ip d'un serveur DNS

- Connecté au commutateur par un câble droit

Etape 3: Configurer les aspects sans fil du point d'accès

- Par défaut? C'est possible
- Il existe une multitude de paramètre pour les PA:
  - Norme IEEE(a, b, g ou **plusieurs**(PB))
  - Canal sans fil
  - SSID (identifiant du LAN sans fil sur 32 caractères ASCII)
  - Puissance d'émission

- Configurer un réseau ESS=> chaque PA doit être configuré avec le même SSID

- PA mixte (802.11b/g)+ PA 802.11g dans la même zone de couverture= meilleurs performances

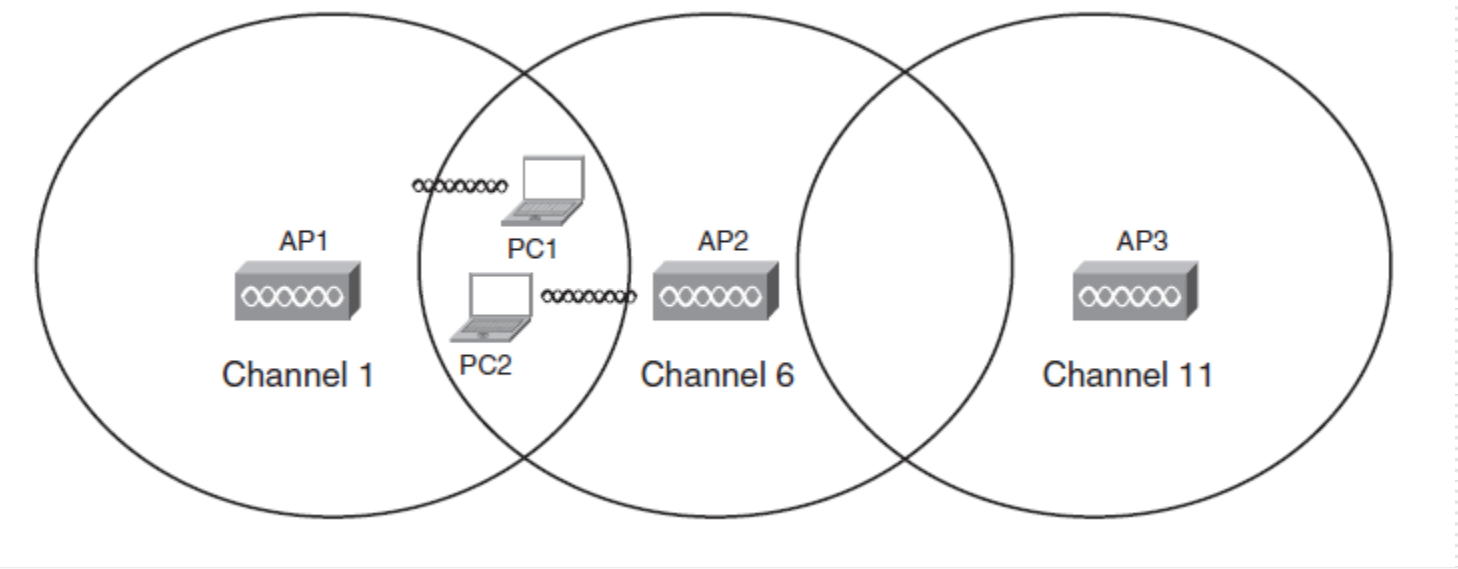
Etape 4: Installer et configurer un client sans fil

- Carte réseau même normes que le PA.
- Contient une radio (pour régler sur les fréquences utilisée)et une antenne.
- Aucune sécurité n'est activée sur le client.
- Au début un client tente de détecté tous les PA en écoutant sur les canaux de toutes le normes qu'il prend en charge par défaut.

- CCX (Cisco Compatible Extensions)???
- ZCF (tout est auto) de Microsoft???

Etape 4: Installer et configurer un client sans fil

- Exemple:



- Le client découvre les 3 PA.
- Il choisit celui dont le signal est plus fort.
- Il apprend le SSID du PA.

Etape 5: Vérifier que le WLAN fonctionne depuis le client

- Ping Serveur sur le réseau filaire.
- Problème???
  - Le PA est-il situé au centre de la zone ou se trouve le client?
  - Le PA ou le client est-il situé à proximité d'une importante quantité de métal?
  - Le PA ou le client est-il proche d'une source d'interférence, comme un four à micro-ondes ou un téléphone sans fil?
  - La zone de couverture du PA est-elle suffisamment étendue pour atteindre le client?

Etape 5: Vérifier que le WLAN fonctionne depuis le client

- Prenez votre Laptop et cherchez.
- La carte réseau activée? (bouton d'économie d'énergie)
- Les radios des PA activées?
- Le PA possède le dernier microprogramme (SE PA)?
- Vérifier la configuration du PA (surtout celle du canal pour s'assurer qu'il n 'utilise pas un canal qui recouvre d'autres PA situés au même endroit)

MPDU / MSDU

- MSDU : Mac Service Data Unit
  - paquet de données envoyé par l'applicatif à la couche MAC
- MPDU : Mac Protocol Data Unit
  - paquet de données envoyé par la couche MAC à l'antenne
- Point important : Un MSDU peut être fragmenté en plusieurs MPDU
- Cette distinction a son importance pour TKIP (WPA) et CCMP (WPA2)
  - Pour TKIP, le MIC est calculé sur le MSDU
  - Pour CCMP, le MIC est calculé sur chaque MPDU

La sécurité des LAN sans fil

- Les LAN ont des exigences particulières

- **Les hackers:**
  - Voler des informations en accédant aux hotes at a la partie filaire du réseau
  - DOS

- **Employé** bien intentionné mais mal informé:
  - Installer un Point d'accès sans l'accord du service informatique
    - Sans mesure de sécurité

Menaces

- **Wardriving**

L'attaquant souhaite accéder gratuitement a internet

- **Hackers**

Trouver des informations ou lancé des attaques Dos
Pirater des hotes de l'entreprises sans passer par les parefeu

Employés

Acheté un point d'acces
Installer le PA par des parametre par defaut
L4attaquant