#### Pan [Mécanismes de sécurité aux réseaux wLAN]

- Introduction
- Pourquoi on a besoin des Wlan
- 802.11 présentation et architecture
- Protocoles
- Sécurité dans 802.11b
- Failles de sécurité
- Outils d'attaques
- Solutions
- Conclusion
- Bibliographie



#### Introduction

-Les réseaux sans fils prennent une grande importance durant les déplacements. Beaucoup d'utilisateurs ont des machines (ordinateurs, imprimantes et d'autres appareils) connectés à un Réseau Local [LAN] ou un Réseaux étendus [Wan], puisqu'il est impossible d'avoir une connexion filaire dans un avion, un bateau ou une voiture donc les réseaux sans fil sont du plus grand intérêt.

-Les réseaux locaux sans fil sont en plein développement du fait de la flexibilité de leur interface, qui permet à un utilisateur de changer de place dans l'entreprise tout en restant connecté. Plusieurs produits sont actuellement commercialisés, mais ils sont souvent incompatibles entre eux en raison d'une normalisation relativement récente. Ces réseaux atteignent des débits de plusieurs mégabits par seconde, voire de plusieurs dizaines de mégabits par seconde.

-Et surtout nous allons étudier les problèmes de sécurité que peuvent poser l'utilisation des Réseaux locaux sans fil [*Wireless Wan*]



## Les Wlan pourquoi faire?

#### Avantages

- Mobilité
- Topologie dynamique
- Facilité d'installation
- Coût

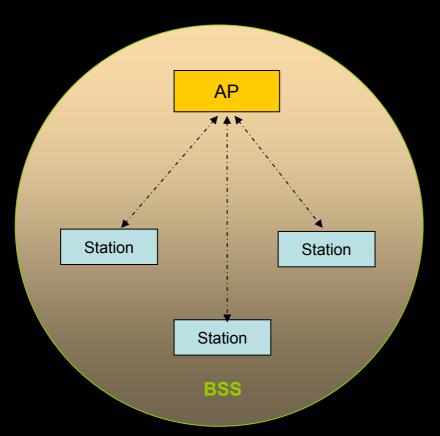
#### Usages

- salons, conférences, ...
- points d'accès haut débit dans les lieux publics (aéroports, gares, métros, ...)
- Hôtels , restaurants, hôpitaux..;



## 802.11b- Présentation et architecture(1)

#### **Basic Service Set (BSS)**



- Le réseau local 802.11b est fondé sur une architecture cellulaire ou chaque cellule appelée BSS (Basic Service Set) est contrôlée par un « AP » (Access Point)

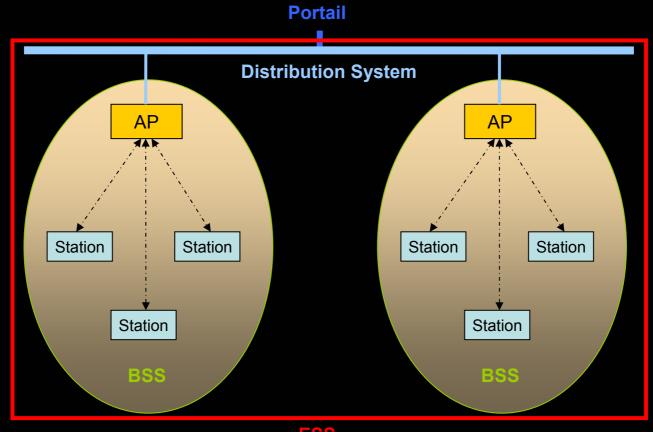


#### 802.11b- Présentation et architecture(2)

#### Réseau d'infrastructure

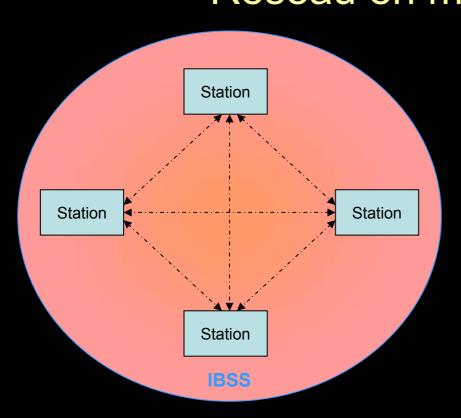
ESS (Extended Service Set). Ce mode de communication est appelé le mode « infrastructure ». Les ponts peuvent être reliés entre eux par des liaisons radios ou filaires et un terminal peut alors passer d'un pont à un autre en restant sur le même réseau (concept du « roaming »).

Chaque terminal sans fil reçoit donc tout le trafic circulant sur le réseau.





# 802.11b- Présentation et architecture(3) Réseau en mode ad hoc



Mode de communication « ad-hoc » : il s'agit d'un mode point à point entre des équipements sans fil qui utilise des protocoles de routage proactifs (échange périodique des tables de routage pour la détermination des routes) ou des protocoles de routage réactifs (les routes sont établies à la demande).



## Présentation de 802.11b

## Couche Physique

- **▶**Bande ISM
- Basé sur le DSSS
- ➤ Débits compris entre 1 et 11 Mbits/s
- Mécanisme de variation de débits selon la qualité de l'environnement

#### Couche de liaison de données LLC 802.2 et l'adressage sur 48 bits Couche MAC contrôle d'accès

- ➤ CSMA/CA (accusé de réception systématique des paquets )
- Un protocole optionnel de type RTS/CTS ("nœud caché", )
- Les sommes de contrôle CRC
- ➤ fragmentation des paquets

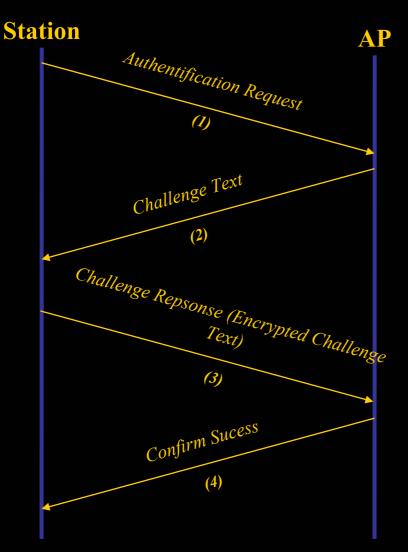


## Sécurité dans 802.11b

- Accès au réseau
  - Service Set ID (SSID)
  - Access Control List (ACL)
- Wired Encryption Privacy (WEP) : Mécanisme de chiffrement basé sur le RC4
- Authentification
  - Open System Authentication
  - Shared Key Authentication



## Shared Key Authentication

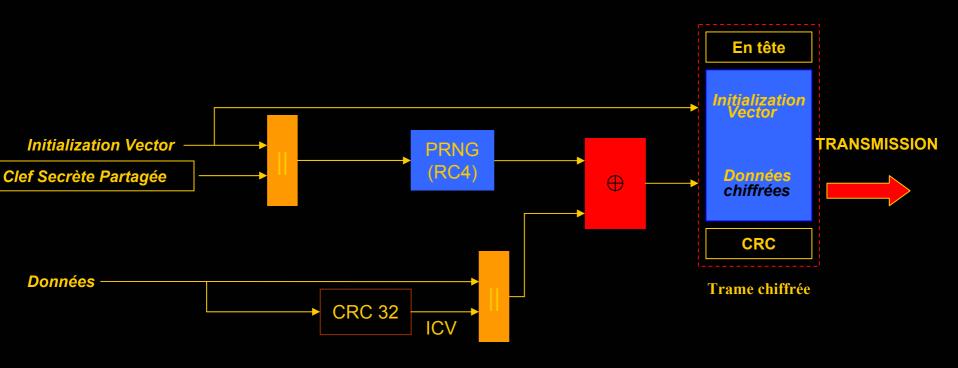


#### Association à un réseau:

- Découverte de l'AP par balayage de canaux
- Authentification (option Shared Key ou Open System)
- Association au cas de succès



## **WEP: Chiffrement**





#### Vulnérabilités de la norme 802.11b

- Les lacunes dans l'authentification
  - Pas de réels mécanismes d'authentification
  - Option open system
- Les faiblesses du WEP
  - attaque par dictionnaire-attaque par force brute analyse statistique.
  - Taille de la clé 40 bits(le cycle de longueur 2^24 implémenté)
  - 60 à 256 IV faibles pour retrouver la clé
- Absence de mécanisme de gestion des clés
  - cryptographie symétrique mais sans gestion de clé
- La faiblesse du vérificateur d'intégrité
  - code CRC de 32bits au lieu d'une fonction de hachage



## Quelques outils de compromission

#### • Découverte des réseaux

- Netstumbler: utilise des trames de gestion pour avoir des infos( activation du WEP, adresse MAC de l'AP, le ESSID..)
- Kismet idem mais détecte des matériels propriétaires.

#### Capture du trafic

- Ethereal 0.9: Toutes les trames sont capturées et les en-têtes conservés- dechiffrement ultérieur
- Mognet 1.14

#### Cassage de l'algorithme du WEP

- Wepcrack: simule le trafic d'un AP, collecte et retrouve la clé de 40 ou 128 bits
- Airsnort: capable de retrouver les clés en temps réel



## Solutions

#### 802.1x

- L'algorithme RC4 utilise des clés de 128 bits, plutôt que les 40 bits.
- Gestion des clés
- Utilisation des protocoles comme EAP (Extensible Authentication Protocol), RADIUS (Remote Authentication Dial-In User Service) et TLS (Transport Layer Security).

#### **Authentification**

**EAP** [Extended Authentification Protocol]

#### 1. Protocoles de protection:

#### SSH - Secure SHell

SSH est un protocole destiné à permettre aux utilisateurs d'ouvrir, depuis une machine cliente, des sessions interactives à distance sur des serveurs et de transférer des fichiers entre les deux. La connexion entre le client et le serveur est encryptée. Les données transitant sur cette connexion ne peuvent pas être lues par un éventuel pirate. L'utilisation de clés publiques garantit l'authentification du client et du serveur. La connexion ne peut donc pas être

pirate. L'utilisation de clés publiques garantit l'authentification du client et du serveur. La connexion ne peut donc pas être déviée vers un autre serveur contrôlé par le pirate.

#### SSL – Secure Socket Layer

SSL est un outil d'authentification et de chiffrement. Dans le cadre d'échanges WEB, il permet d'assurer une sécurité des protocoles http entre navigateurs et serveurs. Les fonctionnalités de base de SSL sont l'authentification du serveur WEB par le navigateur, la confidentialité des échanges par chiffrement et l'intégrité des échanges.

#### 2. Protection de type VPN



#### Conclusion

- Les réseaux 802.11b offrent de nombreux domaines d'applications
- Les réseaux 802.11b sont vulnérables aux attaques
- La sécurité ne peut pas reposer sur le WEP
- L'importance de l'utilisation des protocoles de sécurité supplémentaires tel que IPSec, SSL ou SSH.
- 802.1x la solution?



## Bibliographie

- [1] G. PUJOLLE, Guy Les Réseaux Edition 2003 Juillet, 2002, Eyrolles
- [2] IEEE IEEE Std 802.11b -1999 (Supplement to ANSI/IEEE Std 802.11, 1999 Edition)
- [3] Cisco Systems Extensible Authentication Protocol Transport Layer Security Deployment Guide for Wireless LAN Networks.
- [4] J. S. Silva, Adailton As Tecnologias de Redes Wireless Mai, 1998, Rede Nacional de Pesquisa – RNP, [http://www.rnp.br/newsgen/9805/wireless.shtml]
- [5] Site http://www.wi-fi.org/
- [6] Site d'IEEE http://www.ieee.org/
- [7] Site de l'Autorité de Régulation des Télécommunications <a href="http://www.art-telecom.fr/">http://www.art-telecom.fr/</a>
- [8] Scott Fluhrer, Itsik Mantin. et Adi Shamir Weakness in the key scheduling algorithm of RC4, Août 2001

