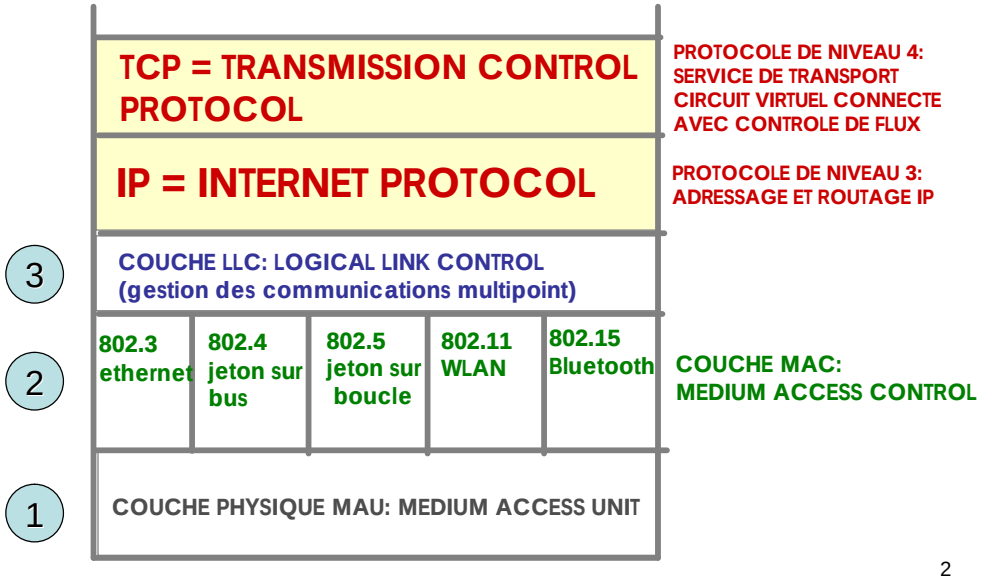
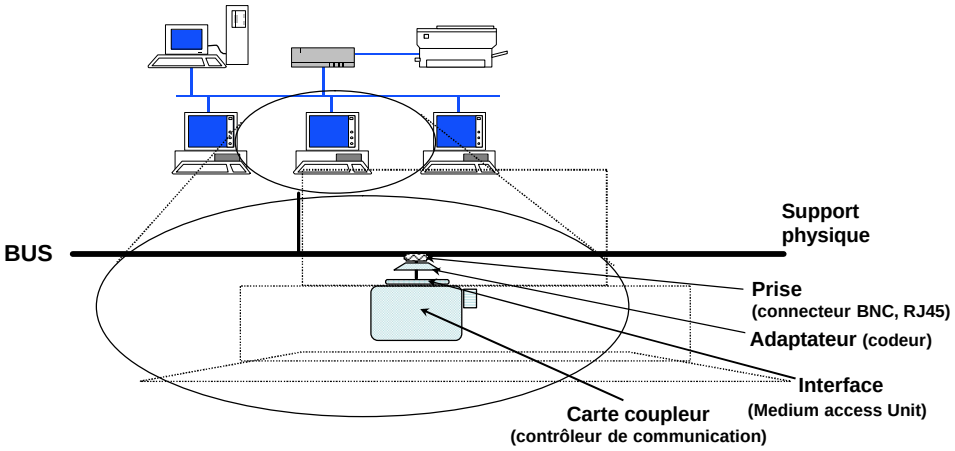
Sécurité des Réseaux Locaux Informatiques
VLAN et WLAN

ARCHITECTURE
IEEE 802 LAN et WLAN

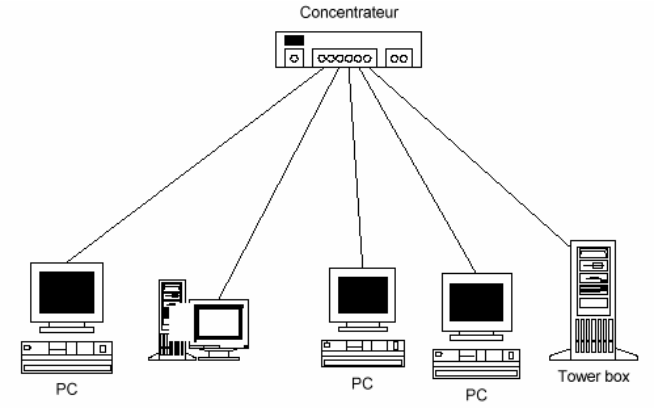


LES RESEAUX LOCAUX INFORMATIQUES
ETHERNET 10BASE5

- Utilisation d'un BUS
- Partage du support entre les stations au moyen d'un protocole de niveau 2 (Liaison) appelé MAC (Medium Access Control)

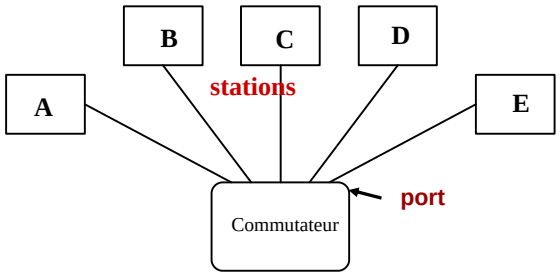


ETHERNET 802.3
10 base T (1990)



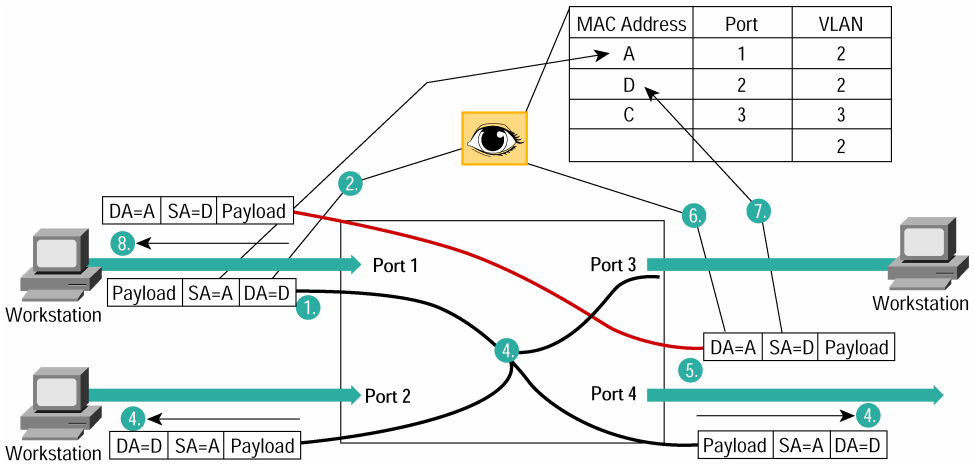
- **Utilisation d'une topologie en étoile autour d'un HUB (migration facile)**
- **Faciliter la gestion du parc de terminaux**
- **Ne supprime pas les collisions**
- **Les stations se partagent les 10 Mbps**

ETHERNET COMMUTE
PRINCIPES



- **Réduire les collisions pour accroitre les débits**
- **Utilisation d'une topologie en étoile (migration facile)**
- **Remplacer le nœud central passif (HUB) par un commutateur.**
- **chaque station possède 10 Mbps entre elle et le Commutateur**
- **Mettre à peu de frais des réseaux virtuels (utilisation de table dans les commutateurs)**

SWITCH COMMUTE - APPRENTISSAGE



REPEATER / HUB / SWITCH

Répéteur/adaptateur (UNICOM)

Switch multi Protocole (3com)

hubs 16/8 ports (HP)

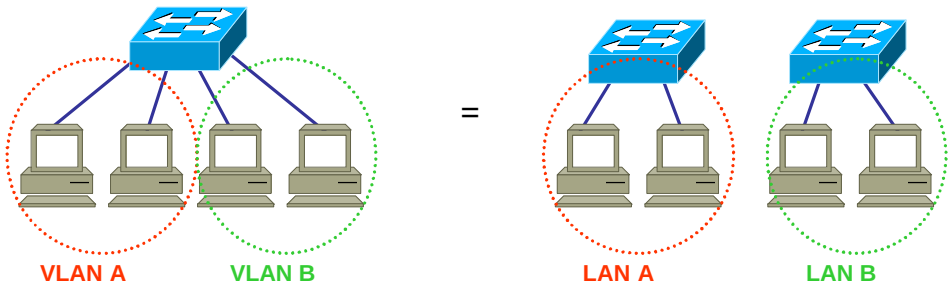
Commutateur/ Switch Netgear

Switch empilables

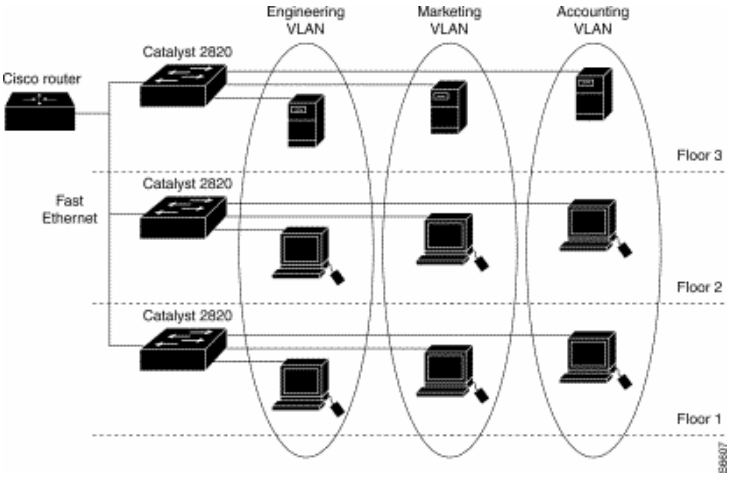
VLAN: Définition

Définition : **V**irtual **L**ocal **A**rea **N**etwork

Utilité : Plusieurs réseaux virtuels sur un même réseau physique



VLAN: Architecture



Typologie des VLAN

Plusieurs types de VLAN sont définis, selon le critère de commutation et le niveau auquel il s'effectue :

1. **Un VLAN de niveau 1 (aussi appelés VLAN par port, en anglais *Port-Based VLAN*) définit un réseau virtuel en fonction des ports de raccordement sur le commutateur ;**
2. **Un VLAN de niveau 2 (également appelé VLAN MAC ou en anglais *MAC Address-Based VLAN*) consiste à définir un réseau virtuel en fonction des adresses MAC des stations. Ce type de VLAN est beaucoup plus souple que le VLAN par port car le réseau est indépendant de la localisation de la station; le défaut est que chaque station doit être manuellement associée à un VLAN.**
3. **Un VLAN de niveau 3**

Typologie des VLAN (2)

3. Un VLAN de niveau 3 : on distingue plusieurs types de VLAN de niveau 3 :

- **Le VLAN par sous-réseau (en anglais *Network Address-Based VLAN*) associe des sous-réseaux selon l'adresse IP source des datagrammes. Solution souple car la configuration des commutateurs se modifient automatiquement en cas de déplacement d'une station. En contrepartie une légère dégradation de performances car les informations contenues dans les paquets doivent être analysées plus finement.**
- **Le VLAN par protocole (en anglais *Protocol-Based VLAN*) permet de créer un réseau virtuel par type de protocole (par exemple TCP/IP, IPX, AppleTalk, etc.), regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même réseau.**

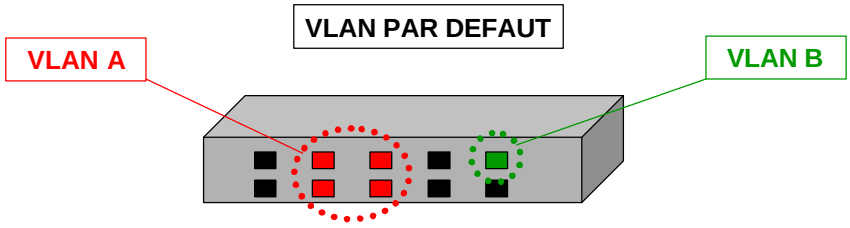
VLAN: de niveau 1

VLAN de niveau 1 ⇔ VLAN par port

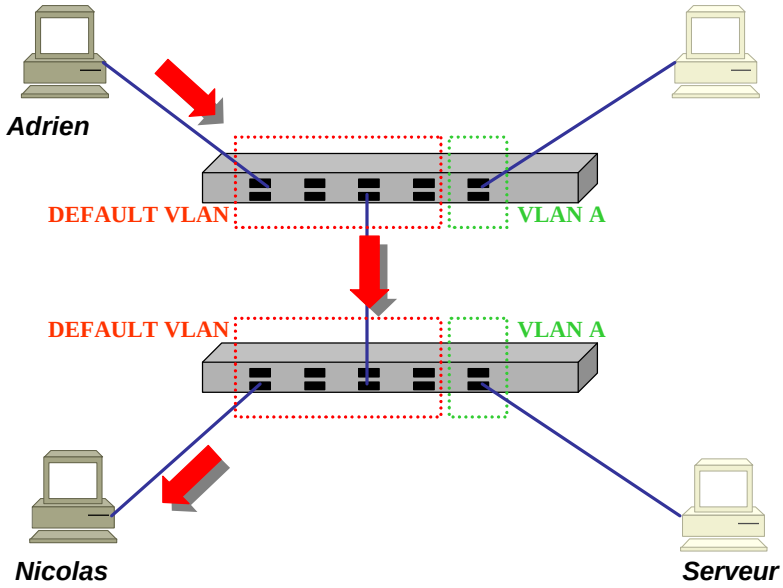
→ 1 port du switch dans 1 VLAN

→ configurable au niveau de l'équipement

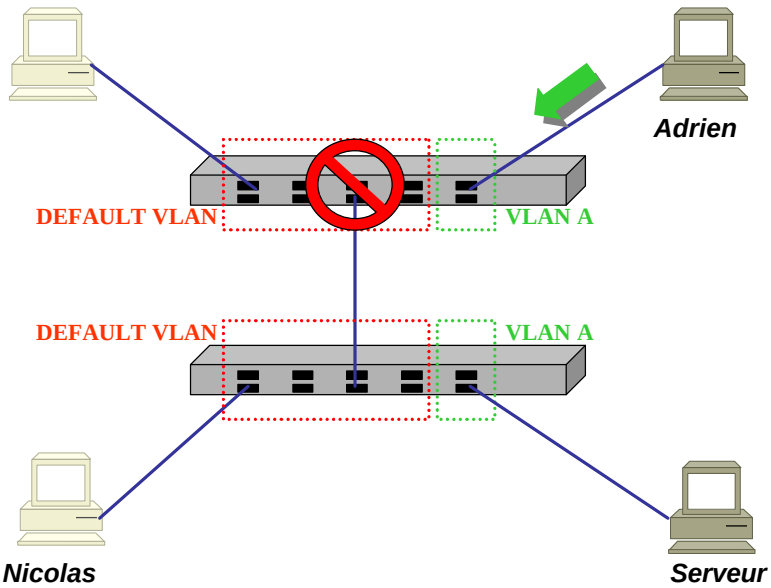
→ 90% des VLAN sont des VLAN par port



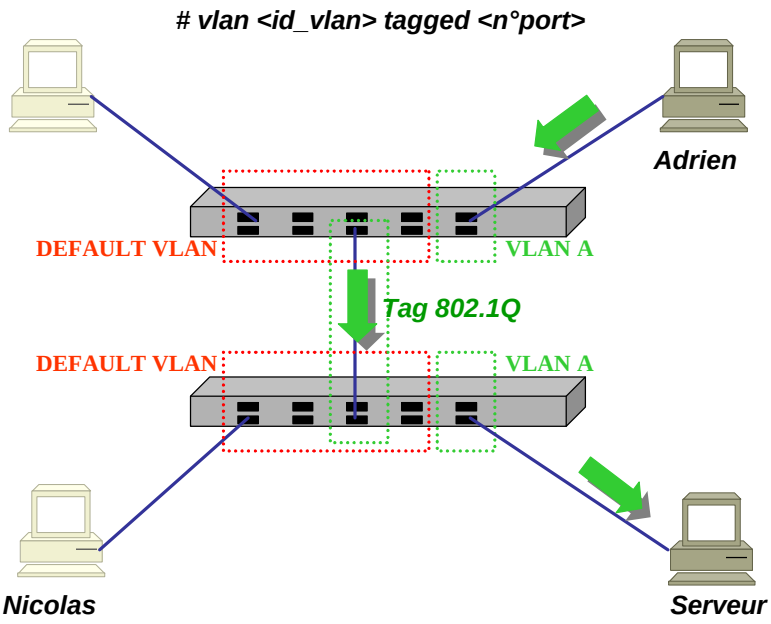
802.1Q – Démonstration 1



802.1Q – Démonstration 2



802.1Q – Démonstration 3



VLAN et QOS

- IEEE 802.1p et 802.1q -

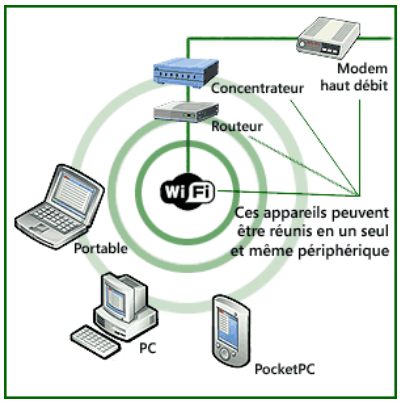
Tame Ethernet non 802.1p

Destination	Source	Type / Longueur

Tame Ethernet etendue 802.1p

Destination	Source	**Tag Control Info**		Type / Longueur
		Type de trame	**Priorite**	**Cano-nical**	**802.1q VLQN identifiant**
		2 bytes	3 bits	3 bits	12 bits

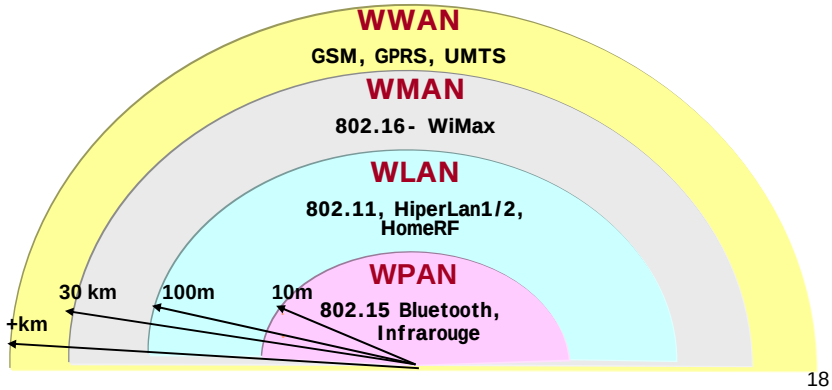
Sous champ de controle	Description
Type de frame marquée	Toujours a 8100h (type trame Ethernet)
Champ priorité (802.1p)	Valeur representant le niveau de priorite
« Canonical »	Toujours a 0
802.1q VLQN identifiant	Numero d'identification du VLAN



Sécurité WiFi

Les réseaux WLAN

- **Réseaux locaux sans fil (Wireless Local Area Networks)**
- **Faire communiquer des dispositifs sans fil dans une zone de couverture moyenne**



Les standards réseaux sans fils

- **WPAN :**
  - **IEEE 802.15 (WiMedia)**
    - **IEEE 802.15.1 : Bluetooth**
    - **IEEE 802.15.3 : UWB (Ultra Wide Band)**
    - **IEEE 802.15.4 : ZigBee**
  - **HomeRF**
- **WLAN :**
  - **IEEE 802.11 (Wifi)**
    - **IEEE 802.11b**
    - **IEEE 802.11a**
    - **IEEE 802.11g**
    - **IEEE 802.11n**
  - **HiperLAN 1/2**
- **WMAN**
  - **IEEE 802.16 (WiMax)**
    - **IEEE 802.16a**
    - **IEEE 802. 16b**
  - **IEEE 802.20 (MBWA)**

Les technologies WLAN

- **En 1985 les Etats-Unis ont libéré trois bandes de fréquence à destination de l'Industrie, de la Science et de la Médecine. Ces bandes de fréquence, baptisées ISM (Industrial, Scientific, and Medical), sont les bandes 902-928 MHz, 2.400-2.4835 GHz, 5.725-5.850 GHz.**

- **En Europe la bande s'étalant de 890 à 915 MHz est utilisée pour les communications mobiles (GSM), ainsi seules les bandes 2.400 à 2.4835 GHz et 5.725 à 5.850 GHz sont disponibles pour une utilisation radio-amateur.**

- **En 1990 : IEEE débute la spécification d'une technologie de LAN sans fil**
- **Juin 1997: finalisation du standard initial pour les WLAN IEEE 802.11**
- **Fin 1999 : publication des deux compléments 802.11b et 802.11a**

La famille des standards IEEE 802

802.11x – Amendements

- **802.11a** - Vitesse de 54 Mbits/s (bande 5 GHz)
- **802.11b** - Vitesse de 11 Mbits/s (bande ISM 2,4 GHz)
- **802.11g** - Vitesse de 54 Mbits/s (bande ISM)
- **802.11n** - Vitesse de 100 Mbits/s (bande ISM)
- **802.11e** - Qualité de service
- **802.11x** – Amélioration de la sécurité (court terme) : WEP
- **802.11i** - Amélioration de la sécurité (long terme) : AES
- **802.11f** – itinérance : Inter-Access point roaming protocol

Wi-Fi ou 802.11b

- Basé sur la technique de codage physique DSSS : étalement de spectre à séquence directe (Direct Sequence Spread Spectrum);
- Mécanisme de variation de débit selon la qualité de l'environnement radio : débits compris entre 1 et 11 Mbits/s

Zone de couverture

Vitesses (Mbits/s)	Portée (Mètres)
11	50
5	75
2	100
1	150

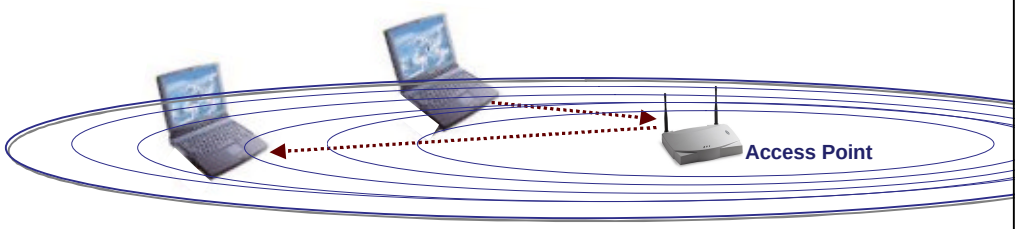
À l'interieur des batiments

Vitesses (Mbits/s)	Portée (Mètres)
11	200
5	300
2	400
1	500

À l'extérieur des batiments

Topologies IEEE 802.11 -1-

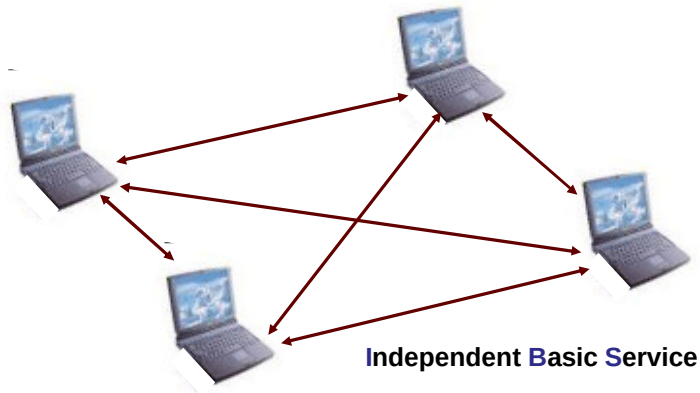
- Architecture basée infrastructure
  - architecture cellulaire
  - architecture BSS (Basic Service Set)
  - chaque cellule (BSS) est contrôlée par une station de base appelée Point d'accès : AP (Access Point)



Basic Service Set

Topologies IEEE 802.11 -2-

- Architecture ad hoc
  - aucune infrastructure
  - architecture IBSS (Independent Basic Service Set)



Independent Basic Service Set

Au cœur de la couche MAC 802.11

- **fonctions sous-couche MAC**
  - **accès au réseau**
  - **sécurité (authentification, confidentialité)**
  - **économie d'énergie**
  - **accès au médium**
  - **fragmentation des longues trames**
  - **Qualité de Services**

Sécurité dans le standard IEEE 802.11

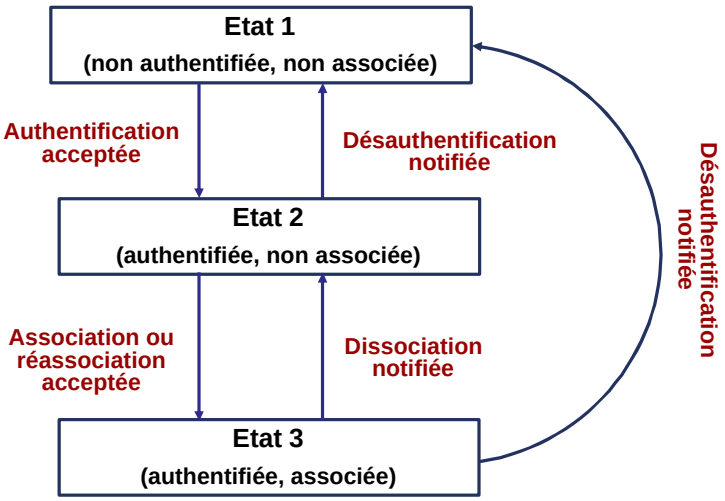
Les risques liés à la mauvaise protection d'un réseau sans fil sont multiples :

1. **L'interception de données consistant à écouter les transmissions des différents utilisateurs du réseau sans fil**
2. **Le détournement de connexion dont le but est d'obtenir l'accès à un réseau local ou à internet**
3. **Le brouillage des transmissions consistant à émettre des signaux radio de telle manière à produire des interférences**
4. **Les dénis de service rendant le réseau inutilisable en envoyant des commandes factices**

Initialisation : Accès au Réseau

- **Allumer station : phase de découverte**
  - **Découvrir l'AP et/ou les autres stations**
  - **La station attend de recevoir une trame de balise (Beacon) émise toute les 0,1 sec.**
  - **A la réception de « Beacon » prendre les paramètres (SSID & autres)**
  - **SSID Service Set Identifier : nom du réseau (chaîne de 32 caractères max.)**
- **Présence détectée : rejoindre le réseau**
  - **Service Set Id (SSID) : nom du réseau de connexion**
  - **Synchronisation**
  - **Récupération des paramètres de la couche PHY**
- **Négocier la connexion**
  - **Authentification & Association**

Diagramme d'états d'une station



Sécurité dans le standard IEEE 802.11

6 mesures de base à appliquer :

- MAC “authentication”
- SSID “hiding”
- Disabling DHCP (use static addressing)
- Antenna placement and signal suppression
- Switch to 802.11a Wireless LANs
- _____
- Encryption WEP : Wired Equivalent Privacy

Wired Equivalent Privacy

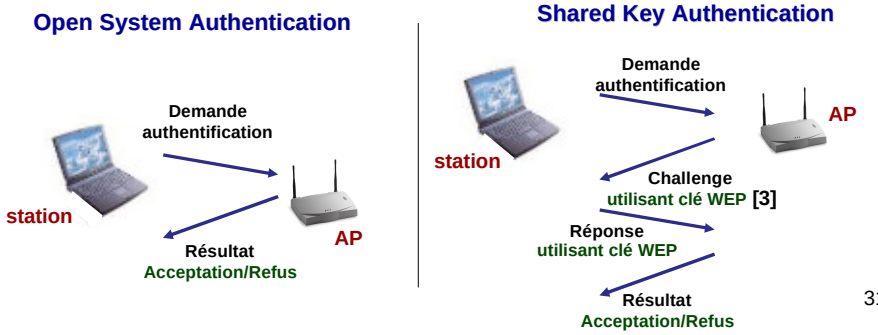
WEP repose sur l’utilisation d’une clé (de 40 ou 104 bits)

Cette clé est utilisée pour offrir 2 services de sécurité:

- une authentification du terminal par clé partagée
  - selon le mode « challenge-response »
- et le chiffrement des données
  - avec algorithme de chiffrement symétrique: RC4 (Rivest Cipher)

WEP : Authentification des stations

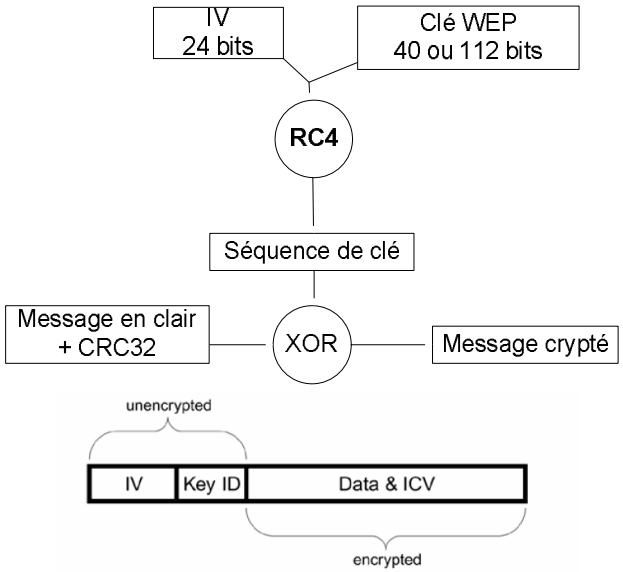
- Envoi d'une requête d'authentification par la station vers l'AP
- l'AP envoi un « challenge » à la station mobile
- Le mobile chiffre le challenge avec l'algo. WEP et la clé secrète et transmet le résultat (la réponse) au AP
- Le point d'accès déchiffre la réponse à l'aide de la clé secrète et l'algo. WEP et compare la valeur obtenue.
  - Si valeur identique alors mobile authentifié.



WEP: Confidentialité des échanges

- La procédure de chiffrement WEP utilise 3 éléments en entrée :
  - ➔ Un vecteur d'initialisation (IV) de 24 bits (nombre pseudo aléatoire)
  - ➔ une clé secrète partagée (K) de 40 bits ou 104 bits
  - ➔ Le texte en clair (P) à chiffrer
- Etape 1 : le vecteur d'initialisation est concaténé a la clé pour former une sous-clé (seed) de 64 bits ou 128 bits.
- Etape 2 : La sous-clé est utilisée par l'algo. RC4 pour générer une séquence de clé de chiffrement
- Etape 3 : une valeur d'intégrité (ICV) de 32 bits est calculée sur le texte en clair (P) en utilisant l'algorithme CRC-32.
- Etape 4 : ICV est concaténé à P
- Etape 5 : (P+ICV) est XORé avec la clé
- Etape 6 : message chiffré + IV en clair sont envoyés

WEP: Confidentialité des échanges (2)



Tools of the wireless LAN hacker

Overview

- Software
  - BackTrack Linux LiveCD (Auditor LiveCD + Traxx)
  - Kismet
  - Void11, Aircrack (Aireplay, Airedump, and Aircrack)
  - airodump: 802.11 programme de capture de paquets
  - aireplay: 802.11 programme d'injection de paquets
  - aircrack: crackeur de clef wep statiques et WPA-PSK
  - airdecap: decrypte les fichiers WEP/WPA capturés
- Hardware
  - Cheap and compatible cardbus adapters
  - Omni directional high-gain antennas
  - Off the shelf Laptop computer

Sniffing des échanges WLAN

Works with WIRESHARK

- **Possible sous Linux / BSD**
- **Restreint sous windows**
  - **Wireshark 0.10.6 ou supérieure**
  - **interface centrino (Intel)**
  - **désactiver le mode « promiscuous off »**
  - **Sinon utiliser AIRPCap (www.cacetech.com/)**

Tools of the wireless LAN hacker

BackTrack LiveCD

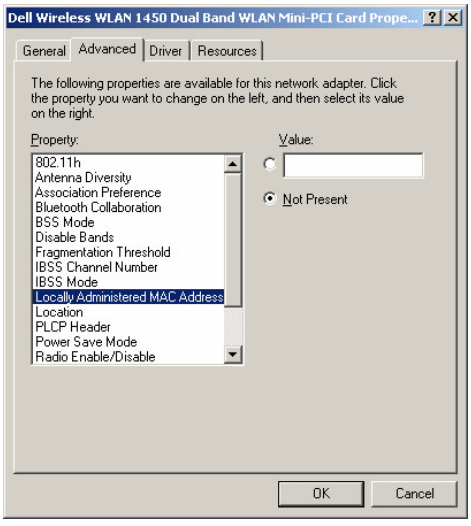
- www.remote-exploit.org
- Bootable Linux CD with every security auditing tool under the sun
- Everything needed to penetrate most wireless LAN and more
- Mentioned as a favorite of the FBI
- Relatively easy to use
- FR-Tutorial : http://www.tuto-fr.com/tutoriaux/tutorial-crack-wep-aircrack.php

Sécurité dans le standard IEEE 802.11

Tous ces mécanismes de sécurité initiaux peuvent être déjoués aux moyens d'outils du domaine public:

- Identification des AP:
  - SSID, channel, adresse MAC AP : Kismet
- MAC :
  - Identifier l'adresse MAC d'un client : Kismet
  - Spoofing ARP
    - ifconfig eth0 hw ether aaaaaa000002
- WEP :
  - Cracker la clé : AirSnort ou WEPCrack ou AirCrack
    - Il faut capturer 50 000 (clé de 64 bits) à 200 000 (clé 128 bits) trames contenant un vecteur d'Initialisation (IV) différents -> plusieurs heures
    - forcer la ré-authentification des clients: void11
    - Générer du trafic : Ping –t l 50000 @MAC_AP
    - Utiliser l'outil Aireplay (Linux) pour faire du rejeux et ne pas être identifié par l'AP
    - 5 mns pour cracker une clé de 64 bits
    - 10 mns pour une clé de 128 bits

MAC spoofing



SSID “hiding”

- All that’s happening is Access Point beacon suppression
- Four other SSID broadcasts not suppressed
  - Probe requests
  - Probe responses
  - Association requests
  - Re-association requests
- SSIDs **must** be transmitted in clear text or else 802.11 cannot function

Sécurité dans le standard IEEE 802.11

Tous les mécanismes de sécurité initiaux peuvent être déjoués : avec les Outils « AirSnort » or « WEPcrack »

- **Passé**
  1. **Wired Equivalent Privacy (WEP) étendue**
     - **clé de cryptage passe de 64 à 128 bits**
     - **Défaut : une seule et même clé pour toutes les stations**
- **Présent**
  2. **Wifi Protected Access (WPA)**
     - **Double authentification du terminal sur la base du port physique (802.1x) puis par mot de passe ou carte à puce via un serveur d’authentification RADIUS (EAP-TLS).**
     - **TKIP : Temporal Key Integrity Protocol (TKIP) : clé différente par station et par paquet avec renouvellement périodique;**
- **Demain**
  3. **WPA2 (IEEE 802.11i) avec:**
     1. **Authentification via certificat (EAP-TLS)**
     2. **TKIP**
     3. **Chiffrement robuste AES (Advanced Encryption Standard)**

The best ways to secure the WLAN

WPA and WPA2 standards

- WPA used a trimmed down version of 802.11i
- WPA2 uses the ratified 802.11i standard
- WPA and WPA2 certified EAP types
  - EAP-TLS (first certified EAP type)
  - EAP-TTLS
  - PEAPv0/EAP-MSCHAPv2 (Commonly known as PEAP)
  - PEAPv1/EAP-GTC
  - EAP-SIM
- WPA requires TKIP capability with AES optional
- WPA2 requires both TKIP and AES capability

Details on EAP types at: http://blogs.zdnet.com/Ou/?p=67