

Sécurité Wireless : 802.11(a|b...)

Introduction, sécurité et attaques.



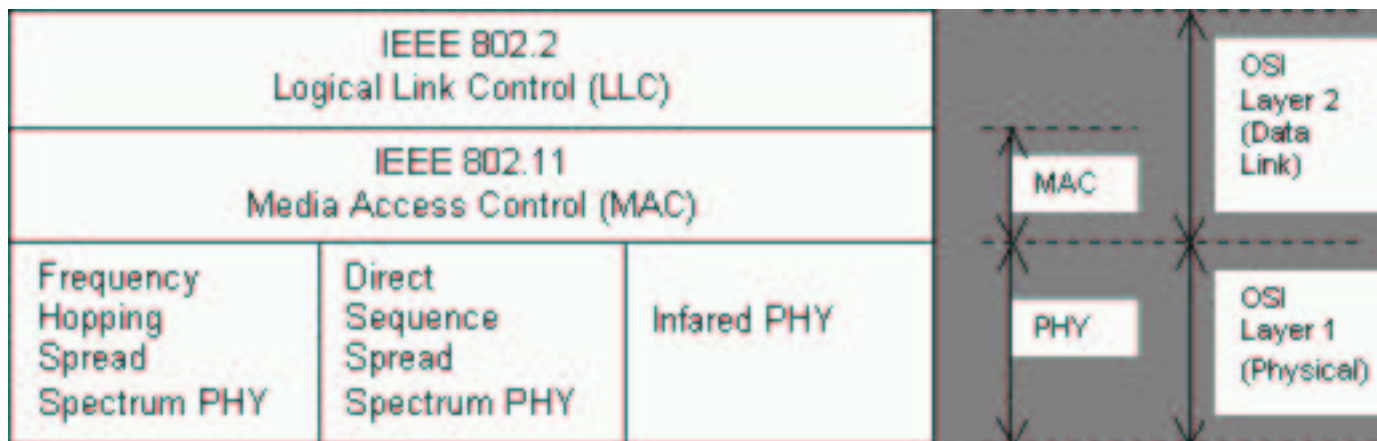
Alexandre Dulaunoy - adulau@conostix.com / adulau@foo.be

Plan

- 802.11 Introduction
- 802.11 Avantages
- 802.11 IBSS (ad-hoc)
- 802.11 IBSS (infrastructure mode)
- 802.11 ESS
- 802.11 Authentication & WEP
- Attaques 'physiques'
- WEP (IV)
- Sécurité
- Sécurité - Bonnes pratiques
- Sécurité - Auditing
- Luxembourg
- Technologies mobiles et sécurité

Wireless 802.11b

- ISM : 13 canaux de 5 MHz à 2.4 GHz en Europe libre d'accès.
- Standard IEEE-802.11-1997 (WLAN)
- Comparable à 802.3 (Ethernet) en terme de fonctions
 - Operation wireless de plusieurs réseaux (overlapping...)
 - Plusieurs interfaces physiques (FHSS, DSSS, IRA,...)
 - Contrôle de la couche physique
 - Contrôle de la sécurité



- 802.11a (12 canaux de 20 MHz à 5.180 GHz-5.320 GHz/5.745 GHz-5.805 GHz)
- QEDM à la place de DSSS

Wireless 802.11 avantages

■ Rapidité d'installation

- Demandes limitées
- Infrastructure & cabling

■ Coût moindre

- Infrastructure (vs standard system)

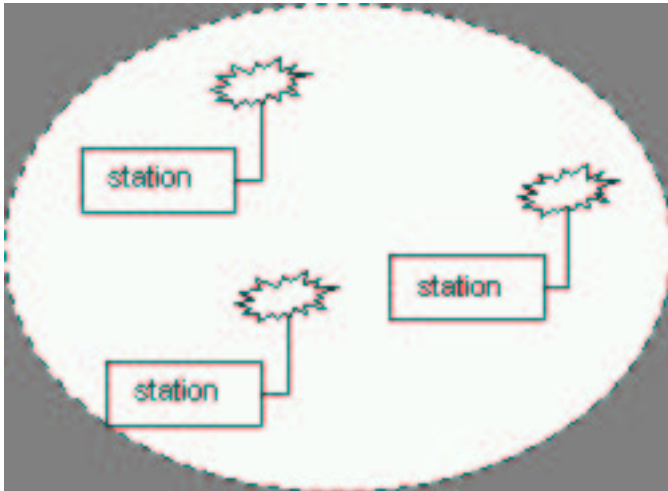
■ Mobilité

- Réseaux temporaires

■ Obstacles moins importants

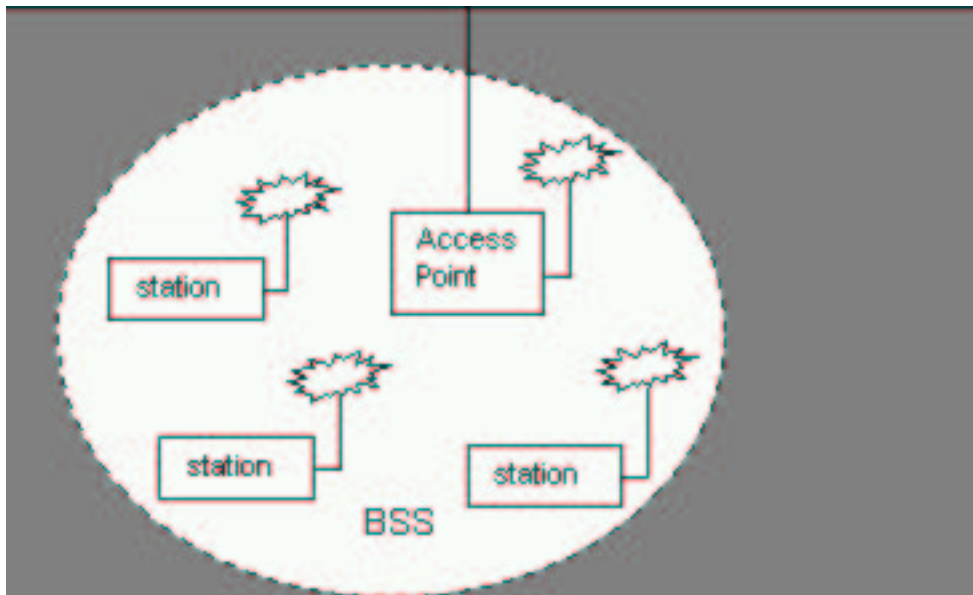
802.11 IBSS (ad-hoc) (Indp. Basic Service Set)

- Communication directe (peer-to-peer)
- Limitation au niveau de la distance (sauf via routage)
- Utilisation de protocole de routage dynamique difficile (p.ex. AODV)



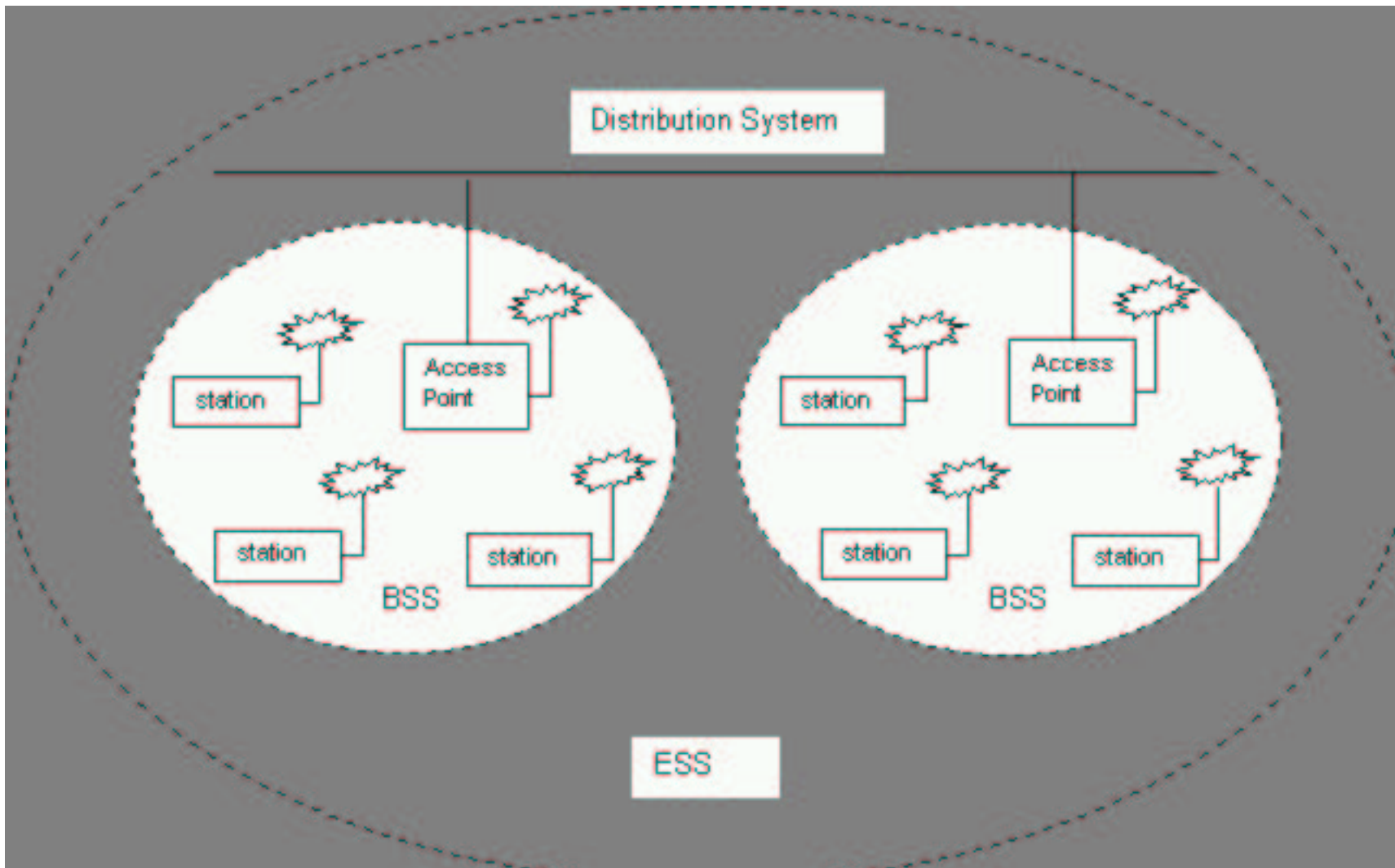
802.11 BSS (infrastructure mode)

- Communication indirecte (via l'access-point)
- Double la distance
- Simplifie l'accès à un autre réseau
- Génération de trames pour la gestion (Beacon frame)



802.11 ESS (Extended Service Set)

- Extension de la mobilité
- Communication entre access-point



Attaques

- Attaque 'diversity'
- Attaque sur la puissance
- Attaque sur le SNR
- Attaque sur la couche réseau (ARP Poisoning)

802.11 Authentication & WEP

■ Open System authentication

- Simple (null type auth)

■ Shared key authentication (via WEP Wired Equivalent Privacy)

- Shared secret key (encryption key = authentication key!)
- Encryption des trames data (et... une partie des trames de gestion)

■ station (request) auth_frame -> AP

■ AP (send) auth_frame rand(128bytes) -> station

■ station (send) encrypt(rand(128bytes)) -> AP

■ AP (send) ok if match / nok -> station

WEP (IV) (40 bits) - (104 bits)

- shared key (40 bits) + IV (initialization vector) (24 bits)
- = 64 bits

- $ICV = CRC-32 + IV$

- shared key (same) + IV (evolution)

- Prediction de (SharedKey, IV) (IP)

- Attaques passives (p.ex. aircsnort, wepcrack...)

Sécurité - Bonne pratiques

- Limitation de la propagation du signal
- Politique de sécurité
- Protection à tous les niveaux OSI
- Réseaux wireless = réseaux externes (DMZ-FW)
- Configuration complète (! conf. par défaut)
- VPN (PPTP, XAUTH, L2TP..) (! aux différentes versions)
- EAP (Extensible Authentication Protocol)

Références

- <http://lists.clussil.lu/wireless.html>
- <http://csrc.nist.gov/publications/>
- (NIST Special Publication 800-48)

Sécurité - Auditing

■ Objectifs

- Détecter des réseaux inconnus (p.ex. dans l'entreprise)
- Détecter des clients mal configurés
- Evaluer la sécurité du réseau WiFi
- Valider la politique de sécurité

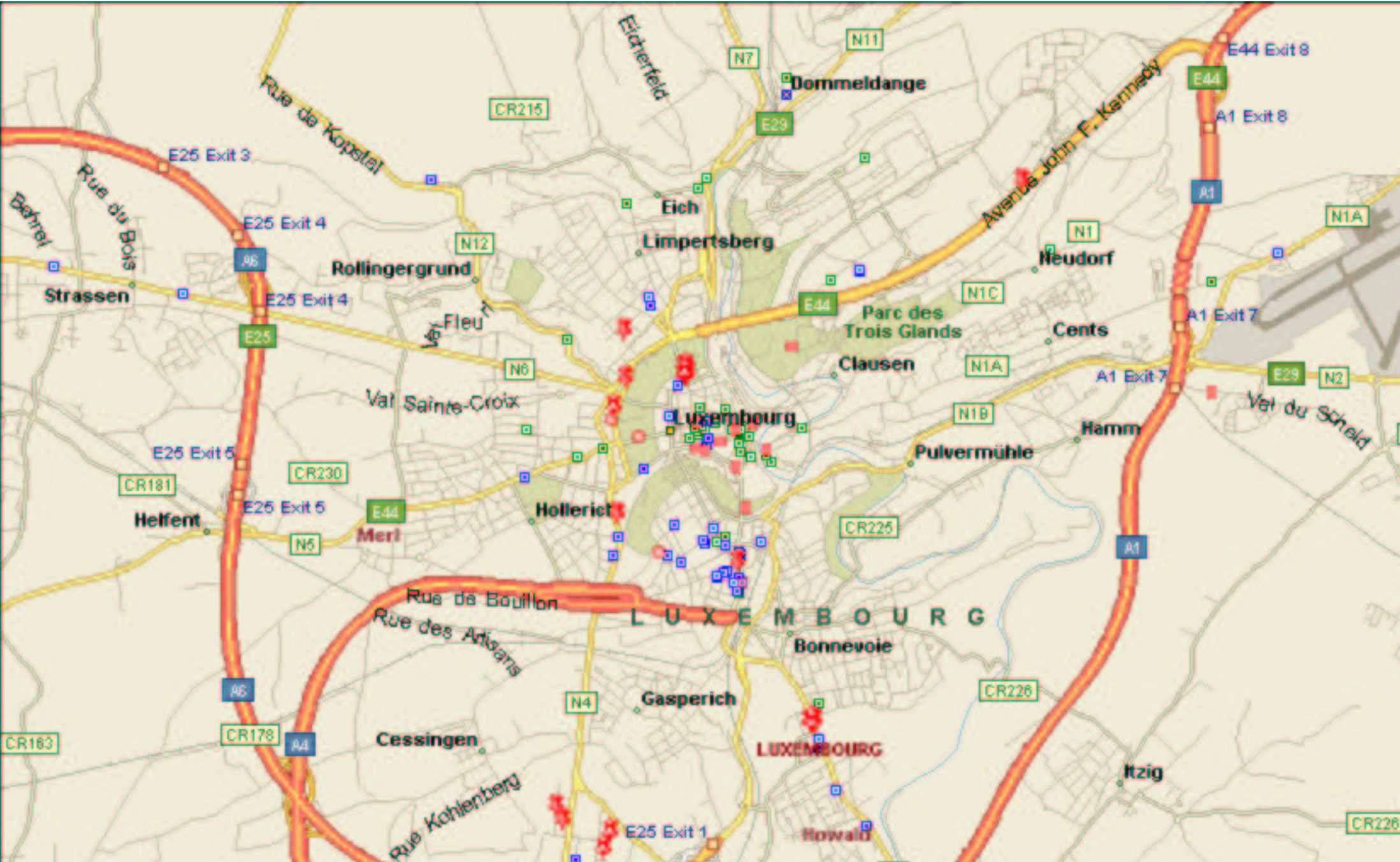
■ Méthodes et outils

- "War driving" dans la zone couverte par l'audit,
- Analyse passive (Beacon frame, Broadcast,...)
- Analyse active (Tests d'intrusion,...)
- Tools : Kismet, Netstumbler,...

Luxembourg ("war driving")

- Comment ?
- Pourquoi ?
- Résultats ?
 - 2002 -> 20 (AP) (30% en WEP)
 - 2003 -> 60 (AP) (50% en WEP)
 - Les bonnes pratiques respectées ?
 - Entreprises et privés. (50% - 50%)

Carte "war driving"



Technologies mobiles et sécurité

■ GSM/GPRS

- Faille chiffrement, authentification
- Pas (encore) de sécurité end-to-end (entre GSM et BS)

■ Bluetooth

- Selection des modes de sécurité
- Sécurité est basée sur le code PIN

■ RF propriétaire

- Manque de transparence

■ IrDA

- Pas de sécurité

Conclusion

- Vérifier la compatibilité, norme avec les standards
- Un réseau mobile est un réseau externe (séparation)
- Une politique de sécurité dans l'entreprise est requise
- Auditer votre infrastructure mobile

Q&A

- `adulau@conostix.com`
- `adulau@foo.be`