802.11(a|b...)

Introduction, sécurité et attaques.

Alexandre Dulaunoy -- alex@foo.be -- GT/Clussil 29/01/2002

Plan

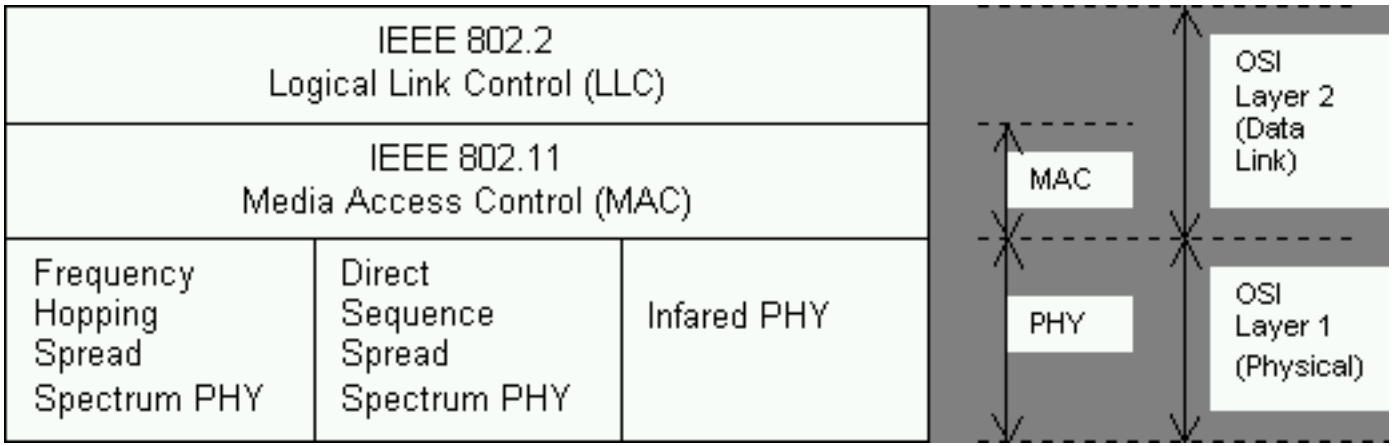
- 802.11 Introduction
- 802.11 IBSS (ad-hoc)
- 802.11 IBSS (infrastructure mode)
- 802.11 ESS
- 802.11 Authentication & WEP
- WEP (IV)
- Sécurité
- Luxembourg

802.11

- Standard IEEE-802.11-1997 (WLAN)

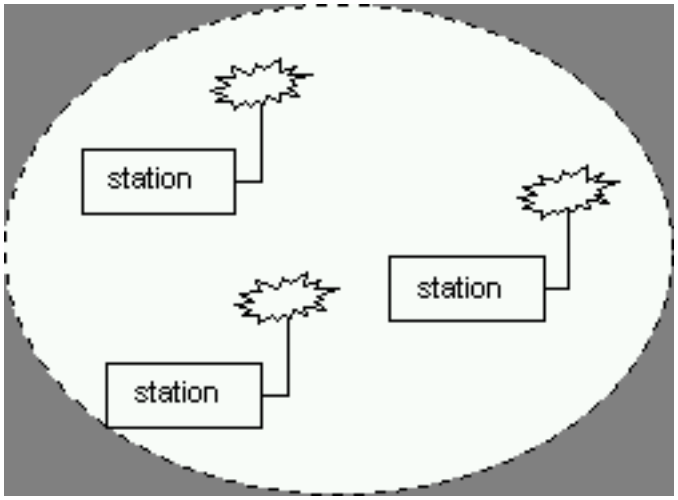
- Comparable à 802.3 en terme de fonctions

  - Operation wireless de plusieurs réseaux (overlapping...)
  - Plusieurs interfaces physiques (FHSS, DSSS, IRA,...)
  - Control de la couche physique
  - Control de la sécurité



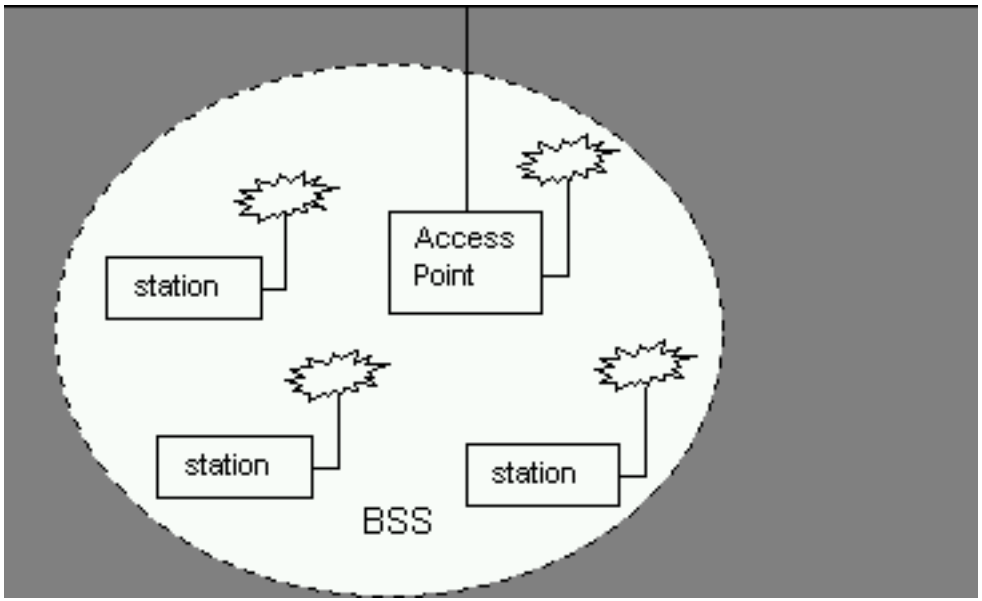
802.11 IBSS (ad-hoc) (Infrastructure Basic Service Set)

- Communication direct (peer-to-peer)
- Limitation au niveau de la distance
- Protocol de routage dynamique difficile (p.ex. AODV)



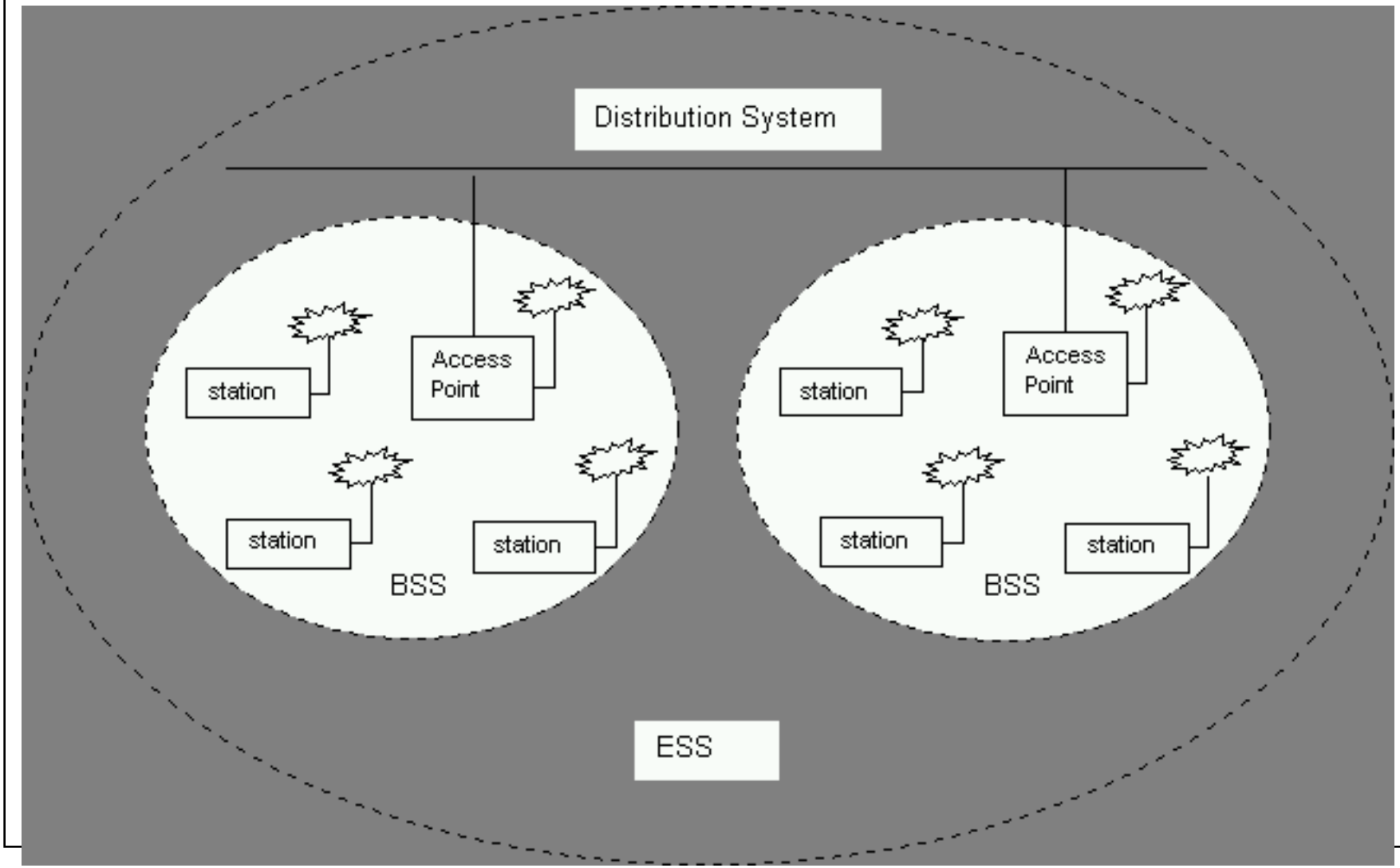
802.11 IBSS (infrastructure mode)

- Communication indirect (via l'access-point)
- Double la distance
- Simplifie l'accès à un autre réseau



802.11 ESS (Extended Service Set)

- Extension de la mobilité
- Communication entre access-point



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)

- 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)

Sécurité

- Protection à tous les niveaux OSI
- Réseaux wireless = réseaux externes (DMZ-FW)
- Configuration complète (!default)
- Attention aux extensions VPN (PPTP, XAUTH, L2TP..)
- EAP (Extensible Authentication Protocol)

Luxembourg ("war driving")

- Comment ?
- Pourquoi ?
- Résultats ?