

# Le wifi au Cr@ns

Jonathan Lajus

Cachan Réseau À Normale Sup'

December 13, 2011



## Le wifi au Cr@ns

### Quelques chiffres

- 28 bornes en production
- 1500 machines enregistrées
- 80 machines wifi connectées en heure de pointe



# Le plan

- 1 Le WiFi, Késako ?
- 2 Les bornes
- 3 Dans le réseau du Cr@ns



## Le Wifi

### Son modèle OSI

- Couche réseau: IP
- Couche de lien: 802.11{a,b,g,n}  
frame: 

MAC header	payload?	fcs
------------	----------	-----
- Couche physique: Les ondes radio (802.11{b,g,n}:2,4GHz, 802.11a: 5GHz)

### Une borne, c'est quoi ?

Si l'on bridge l'interface wifi d'une borne avec une interface ethernet, on obtient un switch (un peu hybride)

## Les bornes utilisées

### WRT54G by Linksys

- 802.11g
- Coût très faible (env. 60€)
- Robuste
- MIPS @ 200MHz, chipset Broadcom
- Flashées à l'identique, possibilité de configuration sans reflasher



## OpenWRT

### Kamikaze et Backfire

- À la base, un firmware basé sur linux, Linksys est donc tenu par la GPLv2 de fournir les sources
- Utilisation d'un firmware custom, OpenWRT
  - La majorité des bornes activent tournent sous Backfire
  - Les bornes hs ou dans la zone ENS sont toujours sous Kamikaze

### Les possibilités de Backfire

- Noyau linux 2.6.32.27
- Driver b43 (Libre)
- Possibilité théorique de multi-SSID
- Plus de caching des authentifications

## Matériel utilisé

### Et en plus, on utilise

- Des antennes directionnelles, omnidirectionnelles et paraboliques
- Des boîtiers pour installer les bornes en extérieur
- Du POE

### Couverture

- Couverture bonne des bâtiments A, B, C, PdJ, au moyen de bornes dans les faux-plafonds
- Couverture partielle du H, I, J, M, G, en arrosant par des bornes installées sur les toits

## Nouvelles bornes

### Pourquoi ?

- Remplacer les vieilles bornes pour augmenter la couverture du campus
- Manque d'entropie des bullets
- Processeur plus puissant pour gérer plus de clients et de SSID

### Les bornes achetées

- Des Nanostations/Picostations
- Le firmware est installé
- Portée ?
- Où ?



## Deux types de bornes

### Sur la partie CROUS du campus

Ces bornes:

- sont directement reliées au réseau Cr@ns.
- diffusent le SSID “Cr@ns”, chiffré en WPA2-enterprise
- acheminent ce trafic sur le vlan VLAN 3 (Wifi).

### Sur la partie ENS

Ces bornes:

- sont branchées sur le réseau de l'ENS.
- diffusent le SSID “ENS Cachan” (VLAN 4) (Hotspot).
- écoutent le SSID “Cr@ns” (VLAN 3).

## Gordon

## Usage

- Routeur WiFi
- Serveur DHCP (Plage: 138.231.144.1 à 138.231.152.254)
- Serveur DNS
- Firewall
- Serveur RADIUS
- Réplique de la base LDAP



# Le chiffrement du Wifi

## Les différents types de chiffrement

- Aucun
- WEP – très faible
- WPA – faible, mais ne nécessite pas de matériel spécifique.
- WPA2-PSK – Une clef WPA pour tous les clients
- WPA2-Enterprise – Utilisation d'EAP (Extensible Authentication Protocol)
  - EAP-TTLS
  - EAP-PEAP/MSCHAPv2

## WPA2-Enterprise et RADIUS

### Authentification RADIUS

- RADIUS est un protocole de centralisation d'authentification et d'autorisation
- Gordon vérifie le couple identifiant/mot de passe via RADIUS couplé à la base LDAP. Si l'authentification réussit, il va générer une clef WPA à usage unique.
- Le protocole est sécurisé au moyen d'un tunnel TLS, l'authenticité du serveur est assurée par un certificat.



# Monitoring

## Les différents outils

- <http://wiki.crans.org/WiFi/CarteDesBornes>
- <http://munin.crans.org/gordon.crans.org.html>
- Accès ssh aux différentes bornes
- Les journaux d'évènements
  - Serveur DHCP
  - FreeRADIUS
- SNMP



## Conclusion

### ToDo List

- Résoudre les problèmes dus à la migration vers Backfire:
  - Choix du canal
  - Comptage des clients
- Configuration automatique des bornes au démarrage
- SSID de secours
- Améliorer la sécurité: correspondance id/mac
- Détecter les réseaux pirates et ouverts
- Une couverture à peaufiner
- Investir dans des nouvelles bornes plus puissantes

Merci.

