Le wifi au Cr@ns

Antoine Durand-Gasselin

Cachan Réseau À Normale Sup'

January 12, 2010

Le wifi au Cr@ns

Quelques chiffres

- 50 bornes en production
- 1500 machines enregistrées
- 80 machines wifi connectées en heure de pointe (contre 550 en filaire)
- Environ 3% du traffic

Le plan

Le Wifi

Son modèle OSI

- Couche physique: Les ondes radio (802.11{b,g,n}:2,4GHz, 802.11a: 5GHz)
- Couche de lien: 802.11{a,b,g,n}
  - frame:

MAC header	payload?	fcs

  - Trois type de frames:
    - Management (beacon, probe, association, authentication)
    - Control (ACK, RTS, CTS)
    - Data
- Couche réseau: IP

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)

Deux *Services Set* déployés

Sur la partie CROUS du campus

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

Sur la partie ENS

- Les bornes diffusent le SSID “ENS Cachan”, en clair. Les bornes acheminent le traffic sur le VLAN 4 (Hotspot).
- Les bornes écoutent le SSID “Cr@ns”, mais ne le diffusent pas, ce traffic est acheminé sur le VLAN 3.
- Ces bornes sont branchées sur le réseau de l’ENS, qui propage ces vlans jusqu’à multiprise-wifi

Le chiffrement du Wifi

Les différents types de chiffrement

- Aucun
- WEP (Wired Equivalent Privacy) – très faible
- WPA (WiFi Protected Access) – première implémentation de 802.11i, repose sur le TKIP (Temporal Key Integrity Protocol). 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

L'ancienne solution

Une solution basée sur l'IPSec

- Filtrage MAC
- Chiffrement IPSec, donc de la couche réseau
- Le routeur wifi sous OpenBSD
  - gestion d'IPSec par isakmpd
  - support OpenSSL de freeradius
- Solution professionnelle, configuration exotique côté client

Avantages et inconvénients

- Le WPA2 nécessite un meilleur lien WiFi
- Plus de travail pour la borne
- La nouvelle solution préserve mieux les bornes (pas de mise à jour quotidienne)

WPA2-Enterprise et RADIUS

Authentification RADIUS

- RADIUS est un protocole de centralisation d'authentification et d'autorisation
- La borne est l'authenticator, et va faire la conversion EAP-RADIUS. Si l'authentification réussit, elle va générer une PMK, clef WPA à usage unique.
- Le protocole est sécurisé au moyen d'un tunel TLS, l'authenticité du serveur est assurée par un certificat.

Au Cr@ns

- Utilisation sur gordon d'un serveur freeRADIUS recompilé avec le support OpenSSL
- Le secret partagé, doit être en clair. freeRADIUS peut le récupérer dans une base LDAP.

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

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
- Plusieurs versions avec différences subtiles: v1, v2, v2.2, v3, v4

Matériel utilisé

Et en plus, on utilise

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

Couverture

- Couverture totale 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

OpenWRT

Kamikaze

- 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
  - Noyau linux 2.4.35
  - Utilisation du driver de Broadcom (bcm47xx)

Les déboires du driver actuel

- Pas de SSID multiple
- Caching des authentifications ?
- Fonctionne sur un 2.4
- OpenWRT 8.09.2 recommende l'utilisation de brcm47xx 2.4
- Attente du driver b43 (pour le SSID multiple)

Nouvelles bornes

Pourquoi ?

- Processeur plus puissant pour gérer plus de clients et de SSID
- Chipset Atheros
- Aucun problème de compilation (pour les bornes supportés par OpenWRT)
- Mais flashage parfois difficile

Conclusion

Future work

- Un réseau fonctionnel, mais qui pourrait être amélioré
- Améliorer la sécurité ?
- Une couverture à peaufiner
- Investir dans des nouvelles bornes plus puissantes