Le WiFi

Michel Blockelet

7 Novembre 2007

Introduction

- WiFi : vu comme un moyen d'accès sans fil à Internet
- Réseau WiFi du CR@NS déployé un peu partout sur le campus (aussi bien du côté de la résidence du CROUS que de l'ENS)

Qu'est-ce que c'est ?

- WiFi : **Wi**reless **Fi**delity (mais ça ne vient pas de là)
- Nom commercial de la norme IEEE 802.11, norme permettant de connecter entre eux des équipements informatiques sans fil
- Présent aujourd'hui dans de nombreux équipements informatiques : ordinateurs, PDA, ou même téléphones et cadres photos !

Le WiFi aujourd'hui

- Aujourd'hui, norme la plus répandue : IEEE 802.11g
- Débit atteignant jusqu'à 54 Mb/s
- WiFi déployé un peu partout, des entreprises (permettre à un employé de rester connecté tout en se déplaçant) aux particuliers (réseau WiFi domestique, souvent avec les box des FAI) en passant par des lieux publics (restaurants, cafés)

Modes de fonctionnement

Mode Ad-Hoc

- Juste des cartes WiFi dans les équipements
- Les équipements se connectent tous entre eux
- Avantage : pas besoin de bornes
- Inconvénients : lent, pas les services d'une borne (contrôle de ceux qui accèdent au réseau par exemple)

Mode Infrastructure

- Une borne WiFi
- Des cartes WiFi dans les équipements
- Les équipements se connectent tous à la borne
- Inconvénient : portée limitée à celle de la borne

Le roaming

- Roaming : rester connecté à un réseau tout en se déplaçant
- Par exemple, réseaux GSM : on peut continuer une communication alors qu'on change de cellule
- Réseaux WiFi : même chose, la carte WiFi s'occupe de s'associer aux bornes ayant le même SSID afin d'assurer la continuité de la connexion (mais mobilité moindre que le GSM !)

Intérêt

Pouvoir se connecter de n'importe où

- Être connecté dans la chambre de quelqu'un d'autre sans utiliser son câble
- Être connecté hors de sa chambre (à la Kfêt, sur les pelouses, ...)
- Être connecté lors d'interventions sur le réseau (câblage, réparation de switchs ou de bornes)
- Être connecté depuis l'ENS

Infrastructure

Bornes

- Bornes WiFi Linksys WRT54g
- Bornes “domestiques”, peu coûteuses, petites et faciles à installer
- Flashées avec un firmware spécial Cr@ns, basé sur OpenWRT
- Ne fonctionnent que sur le réseau du Cr@ns (il faut les démonter pour les reflasher !)

Ragnarok

- Serveur BSD (le seul au Cr@ns)
- Gère tout ce qui concerne le WiFi

Problèmes

On veut garantir la confidentialité et l'authenticité des données des adhérents

- Ethernet : câbles et switchs donc il faut avoir un accès physique à l'infrastructure
- WiFi : ondes donc n'importe qui peut écouter et répéter les paquets

Solutions possibles

Cryptage des données

Au niveau de la transmission

- Cryptage entre la machine et la borne WiFi
- WEP cassable très facilement
- WPA : pas encore très étudié, mais des faiblesses ont déjà été trouvées, on ne peut pas le considérer comme sûr

Au niveau des données transmises

- Cryptage entre la machine et Ragnarok
- VPN : utilisé à la base pour crypter des données transmises par Internet
- Solution retenue : IPSec

Connexion au réseau du Cr@ns par le WiFi

Connexion au réseau WiFi

- Réseau WiFi "Cr@ns" ouvert ; n'importe qui peut se connecter
- DHCP assuré par Ragnarok
- Accès limité : on ne peut acccéder qu'à des pages statiques expliquant le fonctionnement du WiFi

Cr@nsWiFi

- Logiciel (écrit en Python) automatisant la connexion IPSec, en utilisant une clé IPSec aléatoire donnée préalablement à l'adhérent
- Un tunnel IPSec est ouvert entre l'adhérent et Ragnarok, assurant la confidentialité et l'authenticité
- (Le démon d'échange des clés IPSec, ISAKMP, est présent de base sur OpenBSD.)

Réseau WiFi de l'ENS

Issu d'un accord entre l'ENS et le Cr@ns

Accès au réseau de l'ENS

- Certaines bornes configurées en Hotspots
- Diffusent alors le SSID "ENS Cachan"
- Réseau ouvert, connexion en tant que personnel ou en tant qu'invité
- On est alors connecté au réseau de l'ENS avec certaines limitations (quand on est en invité)

On peut toujours accéder au réseau du Cr@ns en forçant le SSID Cr@ns, la borne fonctionne alors comme une borne normale.
(Le Vlan Wifi est le même entre le réseau du Cr@ns et celui de l'ENS.)

Limitations

- Portée : portée théorique de 100m, limitée surtout par les murs dans les résidences
- Services : tous sauf la télé (débit trop petit)
- Bien plus lent que l'Ethernet : débit Ethernet = 100 Mb/s, débit théorique du WiFi = 54 Mb/s, débit réel décroissant en fonction de la distance à la borne

Mise en route d'une borne

- Flasher les bornes avec le firmware (firmware "générique" (pas de configuration spécifique à la borne)) avec le logiciel linksys-tftp
- Inscrire les informations sur les bornes dans la base LDAP : nom, adresse MAC, prise, hotspot, position
- Et puis c'est tout !

Mise à jour des bornes

- La borne devient active après la première mise à jour
- Ragnarok s'occupe de la mise à jour des bornes en fonction des informations de la base LDAP
- Processus wifi-update sur chacune des bornes : se connecte à ragnarok pour récupérer la mise à jour
- Elle active alors l'interface WiFi, et choisit le canal par le script channelchooser

Contenu de l'archive

- Script update.sh
- Fichiers de configuration (init.d, crontab)
- Fichiers générés à partir de la base LDAP
- Mises à jour des scripts

Update.sh

- Script de configuration de la borne
- Script exécuté à chaque mise à jour
- Met à jour les variables de configuration
- Redémarre les services
- Relance par exemple le script de choix de canal
- (Le fait de façon aléatoire)

Autres fichiers de configuration

- /etc/nvram.updates : variables de configuration (nom/ip de la borne, mac/ip des passerelles, etc.), généré à partir de la configuration inscrite dans la base LDAP
- /etc/macip : fichier de correspondance MAC/IP (le DHCP est assuré par Ragnarok mais les bornes vérifient la correspondance MAC/IP des bornes)

Programmes rémanents

- check-connection : vérifie que la borne arrive encore à se connecter à Ragnarok, désactive l'interface WiFi sinon
- counter-measure : essaie de redémarrer l'interface WiFi en cas de problème, redémarre carrément la borne s'il a été appelé trop de fois
- arp-forwarder/dhcp-fwd : transmettent les requêtes ARP et DHCP à ragnarok
- dropbear : serveur ssh léger

Avancées futures du WiFi

Deux nouvelles technologies :

Norme 802.11n

- Débit théorique de 540 Mb/s
- Non finalisée, attendue pour 2008
- Déjà implantée dans certains routeurs WiFi

WiMAX

- Worldwide Interoperability for Microwave Access
- Nom commercial de la norme IEEE 802.16
- Portée théorique de plusieurs kilomètres
- But : déployer le WiFi à l'échelle d'une ville

Plans de la DSI

(Ressort de la réunion Cr@ns-DSI du Vendredi 19 Octobre)

- Remplacer le réseau WiFi existant
- Placer des bornes professionnelles (Cisco)
- Téléphones VoIP passant par le réseau WiFi pour le personnel
- Utiliser plein de logiciels propriétaires pour gérer de façon globale le réseau

Conclusion

Généralisation du WiFi

- WiFi très utilisé par les entreprises comme par les particuliers (même quand ça ne sert à rien !)
- Projets de réseaux WiFi avec une grande couverture (comme les réseaux GSM) -> Neuf Telecom
- WiFi implanté dans tout et n'importe quoi comme équipements !

Il faut continuer à implanter le WiFi sur le campus !