

# Présentation du réseau et des services Cr@ns

Olivier Iffrig

Cachan Réseau à Normale Sup'

Mardi 4 octobre 2011



# Sommaire

- 1 Architecture physique
  - Connexion avec l'extérieur
  - Notre réseau
  - Le wifi

- 2 Les services
  - Les services de base
  - Le "compte Crans"
  - Les autres services

- 3 Sécurité et surveillance
  - Sécurité
  - Surveillance



# Sommaire

- 1 Architecture physique
  - Connexion avec l'extérieur
  - Notre réseau
  - Le wifi
- 2 Les services
- 3 Sécurité et surveillance



# Connexion avec l'extérieur

Trois réseaux entre nous et Internet :

- ▶ l'ENS (DSI)
- ▶ Rubis (Val de Bièvre)
- ▶ Renater (Education Recherche National)



# Notre réseau

- ▶ Un routeur/firewall : komaz
- ▶ Entre chaque bâtiment : fibres en gigabit
- ▶ Dans chaque bâtiment : switchs manageables en étoile
- ▶ Dans chaque chambre : 100Mb
- ▶ Un serveur de secours dans un datacenter d'Ovh (Ovh)



# Notre réseau

Plan du réseau

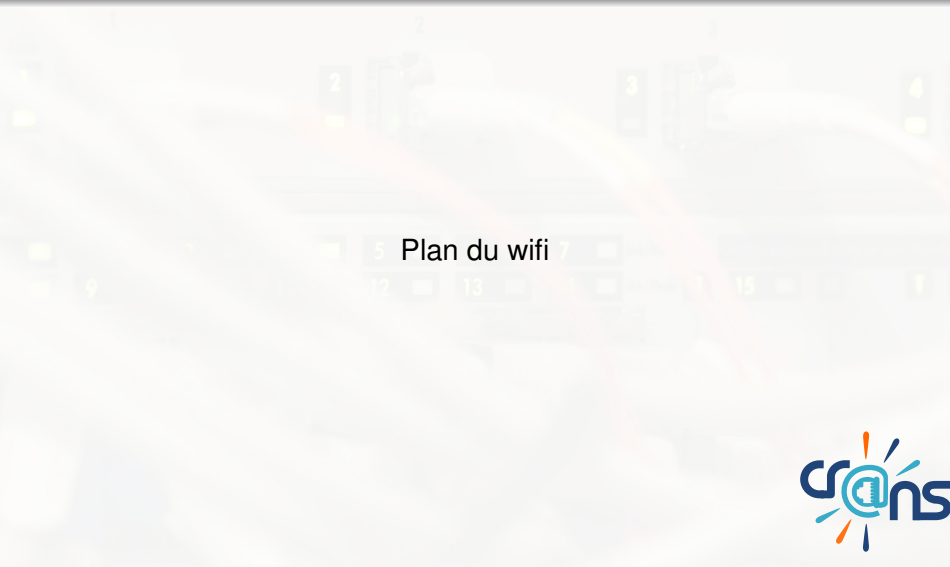


# Le wifi

- ▶ Utilisation de bornes Linksys WRT-54G
  - Pas cher
  - À peu près fiable
  - Avec Linux embarqué
- ▶ Couverture étendue
  - Env. 70 bornes sur le campus
  - Possibilité de couvrir ARPEJ (si l'ENS se bouge)
- ▶ Points techniques
  - OpenWRT
  - WPA2 Enterprise
  - Antennes



# Le wifi



Plan du wifi





# Sommaire

## 1 Architecture physique

## 2 Les services

- Les services de base
- Le “compte Crans”
- Les autres services

## 3 Sécurité et surveillance



# Le DHCP

- ▶ Permet la configuration automatique des machines sur le réseau
- ▶ Présent sur `sable` pour les machines fixes et sur `gordon` pour le wifi



# Le DNS

- ▶ Permet la résolution des noms en IP et inversement
- ▶ Exemple : zamok.crans.org ↔ 138.231.136.1
- ▶ Gestion des zones crans.org, crans.ens-cachan.fr, clubs.ens-cachan.fr
- ▶ Sous-domaines : adm, wifi, ferme, tv, v6
- ▶ Gestion des IPv4 de 138.231.136.0 à 138.231.151.255
- ▶ Gestion des IPv6 dans la plage 2a01:240:fe3d::/48
- ▶ Plusieurs serveurs : sable (maître), sila, rouge, titanic, ovh et gordon (wifi uniquement)



# Stockage des données

- ▶ Mails
- ▶ Pages personnelles
- ▶ Compte ssh sur `zamok`
- ▶ Impression
- ▶ Compte à vie (ou presque)



# Stockage des données

- ▶ Espace disque : env. 2Go (stockage des fichiers et des mails)
- ▶ Centralisation sur la baie de disques (`slon`)
- ▶ Renvoyées par iSCSI sur `fx` ("temporairement")
- ▶ Distribution des fichiers par NFS
- ▶ Authentification grâce à une base LDAP (avec réplicats sur différents serveurs)



# La gestion des mails

- ▶ Utilisation exclusive de Postfix
- ▶ Filtrage anti-virus par Amavis/Clamav
- ▶ Utilisation d'une greylist pour réduire le spam
- ▶ Serveur principal : `rouge`
- ▶ Livraison des mails par `zamok`
- ▶ Possibilité aux adhérents d'utiliser Procmail et Spamassassin
- ▶ Serveurs secondaires : `redisdead`, `Freebox (titanic)` et `ovh` (forwardent uniquement les mails à `rouge`)
- ▶ Pour lire ses mails : POP/IMAP (`dovecot`), Webmails (`horde` et `roundcube`), disponibles sur `owl (domU)`



# Les pages perso

- ▶ Utilisation d'apache2
- ▶ Sites perso et de clubs servis par `zamok`, PHP disponible (mais restrictions)
- ▶ Autres sites de l'association sur `niomniom` (domU)



# L'impression

- ▶ Impression laser couleur
- ▶ Imprimante : Canon iRC 3580
- ▶ Facturation : coût réel, compte prépayé
- ▶ Bac de sortie : séparation des travaux, agrafage, brochures
- ▶ Accès par digicode (génération aléatoire de code) → vigile





## Le wiki

- ▶ Site web collaboratif
- ▶ Première source d'informations pour tout ce qui concerne le campus
- ▶ Pages publiques (accessibles sur <http://www.crans.org>)
- ▶ Utilisation de MoinMoin sur `niomniom`



# Les news

- ▶ Serveur installé sur un domU de fz, news
- ▶ Utilisation d'Inn



# La TV

- ▶ Trois serveurs de diffusion : dindon, lapin et oie
- ▶ Un serveur pour les vignettes et le DNS : vache
- ▶ 5 cartes TNT, 11 cartes Satellite
- ▶ Diffusion en multicast
- ▶ Utilisation de MumuDvb développé par une nounou



# Le proxy

- ▶ 50% des requêtes sont prises dans le cache
- ▶ Permet également de mettre en place des restrictions pour certains adhérents
- ▶ Les requêtes portant sur des fichiers présents sur le ftp local sont redirigées grâce à jesred
- ▶ Filtrage des pubs disponible avec privoxy
- ▶ En cas de coupure par l'ENS passage par le réseau Free
- ▶ Proxy transparent
- ▶ Utilisation de squid sur `sable`



## Divers services

- ▶ Messagerie Jabber (`xmpp`, `domU`)
- ▶ Listes de diffusion (mailman) (`redisdead`, `domU`)
- ▶ FTP public (miroir Videolan, OpenBSD, images ISO de différentes distributions) (`sila`)
- ▶ Nombreux logiciels disponibles sur `zamok` (aussi à la demande)
- ▶ Serveur de temps (`ntp.crans.org`, `sable`)
- ▶ Intranet (gestion de son compte et accès au service d'impression) (`zamok` et `o2`)
- ▶ Paypal (rechargement des comptes impression)



# Sommaire

- 1 Architecture physique
- 2 Les services
- 3 Sécurité et surveillance
  - Sécurité
  - Surveillance



# Sécurité

- ▶ Sauvegarde quotidienne des serveurs sur `babar`
- ▶ Filtrage MAC sur toutes les prises des bâtiments (serveurs `RADIUS` `sable` et `radius`)
- ▶ Nombreux services disponibles en SSL
- ▶ Six sous réseaux séparés (VLANs)
  - réseau filaire (adhérents)
  - réseau WiFi
  - réseau serveurs (transit des données d'administration)
  - réseau appartements de fonction
  - réseau d'isolement (virus et annonces IPv6 pirates)
  - réseau d'accueil (pas encore inscrits)



# Surveillance

- ▶ Surveillance du trafic sortant (upload, p2p, virus...)
- ▶ Surveillance de l'état des services : munin, monit, autostatus
- ▶ Surveillance des locaux sensibles par caméras et enregistrement
- ▶ Conservation de certains fichiers journaux conformément aux lois en vigueur.





# Questions ?

