Présentation du réseau et des services Crans

Daniel STAN

Cachan Réseau à Normale Sup'

Mardi 6 octobre 2015

Sommaire

1. Ethernet et Internet
2. Infrastructure logicielle
3. Les services

Avant de commencer

Si vous êtes apprentis et que vous vous ennuyez...

Un petit listing, sur zamok

```
dstan@zamok$  whos --crans > listing
```

Sommaire

1. Ethernet et Internet
   - Notre réseau
   - Plusieurs réseaux ethernet
   - Le WiFi
   - Réseau Internet
   - Les autres
2. Infrastructure logicielle
3. Les services

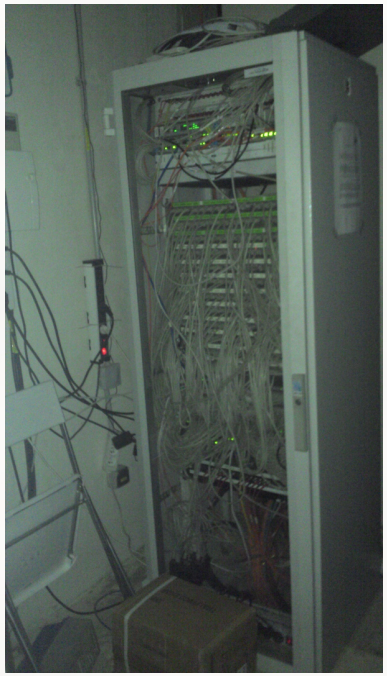
Notre réseau

Plan du réseau

Plan général

- Une dizaine de locaux techniques
- Cœur de réseau au bâtiment B
- Câble RJ45 vers chaque chambre
- . . . ou borne WiFi
- Fibres entre les bâtiments (gigabit)
- Commutateurs réseaux (switchs), en étoile : bat$x-$n

Brassage



- Chambre/local (ex : G999)
- Prise sur switch (ex : g925, batg-9, prise 25)
- Correspondance stockée dans une base SQL

Un besoin d'isolement ?

Achat de plusieurs switchs ?

Un besoin d'isolement ?

Achat de plusieurs switchs ?

- Utilisation du tagging de vlan
- Virtuellement, plusieurs réseaux ethernet
- Permet d'isoler les serveurs Crans, les machines infectés, etc
- Voir liste des Vlan id utilisés
- Transparent pour la machine connectée (detagging) en extrémité
- Certains Vlans sont propagés côté ENS

Radius (version filaire)

- Protocole d'authentification
- Transparent pour l'utilisateur en filaire (le switch est client)
- À la fin du processus, le switch détaggue le vlan donné par radius

Radius (version filaire)

- Protocole d'authentification
- Transparent pour l'utilisateur en filaire (le switch est client)
- À la fin du processus, le switch détaggue le vlan donné par radius
- Radius décide du vlan (adresse MAC, prise, etc)

Le WiFi

- Bornes Ubiquiti {Nano,Pico}Station, UniFi
- $x bornes actives sur le campus (cf Plan)

Le WiFi

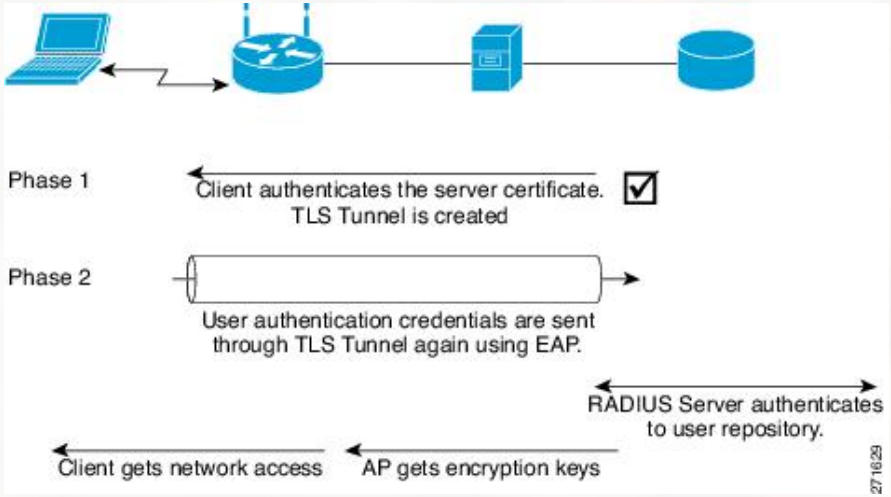
- Bornes Ubiquiti {Nano,Pico}Station, UniFi
- $x bornes actives sur le campus (cf Plan)
- Points techniques
  - WiFi n (principalement 2,4Ghz, et 5Ghz)
  - Linux embarqué (OpenWrt)
  - Management IPv6
  - Pwer over Ethernet (PoE)
  - Points d'accès en zone ENS
  - Quelques ponts WiFi hors campus

WiFi et authentification

- WPA2 Entreprise (EAP)
- Protocole EAP choisi : PEAP+MsChapV2 (login anonyme+login+mdp)
- À la fin, le client et la borne communiquent de manière chiffrée
- La borne relaie la requête EAP via le protocole Radius
- Radius authentifie en EAP (adresse MAC, login, mdp)

WiFi et authentification

- WPA2 Entreprise (EAP)
- Protocole EAP choisi : PEAP+MsChapV2 (login anonyme+login+mdp)
- À la fin, le client et la borne communiquent de manière chiffrée
- La borne relaie la requête EAP via le protocole Radius
- Radius authentifie en EAP (adresse MAC, login, mdp)



En résumé

- Fibres, câbles

En résumé

- Fibres, câbles
- $x serveurs physiques
- $y serveurs virtuels
- $z switchs
- $t bornes WiFi

En résumé

- Fibres, câbles
- $x serveurs physiques
- $y serveurs virtuels
- $z switchs
- $t bornes WiFi
- 4 caméras
- Imprimante
- Baie de disque

Ressources de l'association

Voir plan d'adressage

Un vlan = un réseau IP

- Les IP sont (souvent) distribuées automatiquement par DHCP
- Pour parler sur Internet, il faut une IP publique

Un vlan = un réseau IP

- Les IP sont (souvent) distribuées automatiquement par DHCP
- Pour parler sur Internet, il faut une IP publique
- 138.231.136.0/21 ->

Un vlan = un réseau IP

- Les IP sont (souvent) distribuées automatiquement par DHCP
- Pour parler sur Internet, il faut une IP publique

- 138.231.136.0/21 -> 2048 IPs
- 138.231.144.0/21 ->

Un vlan = un réseau IP

- Les IP sont (souvent) distribuées automatiquement par DHCP
- Pour parler sur Internet, il faut une IP publique

- 138.231.136.0/21 -> 2048 IPs
- 138.231.144.0/21 -> 2048 IPs

Ces ressources nous sont prêtées par la DSI de l'école (sous-ensemble du 138.231.0.0/16).

Routeur de sortie : odlyd

- Un pied de chaque côté : 138.231.136.4, 138.231.148.4, 138.231.132.47 (etc)
- Parefeu entre les réseaux
- Annonce les routes Crans sur le vlan ENS
- Applique les limitations négociées avec la DSI

Et après ?

Les débits en jeu :

- 500Mbit/s en soirée
- 200Mbit/s en journée
- 8Go de quota d'upload sur les dernières 24h
- Pas de limitation vers la zone ENS

Trois réseaux entre nous et Internet :

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

Les grands oubliés d'une connexion qui marche

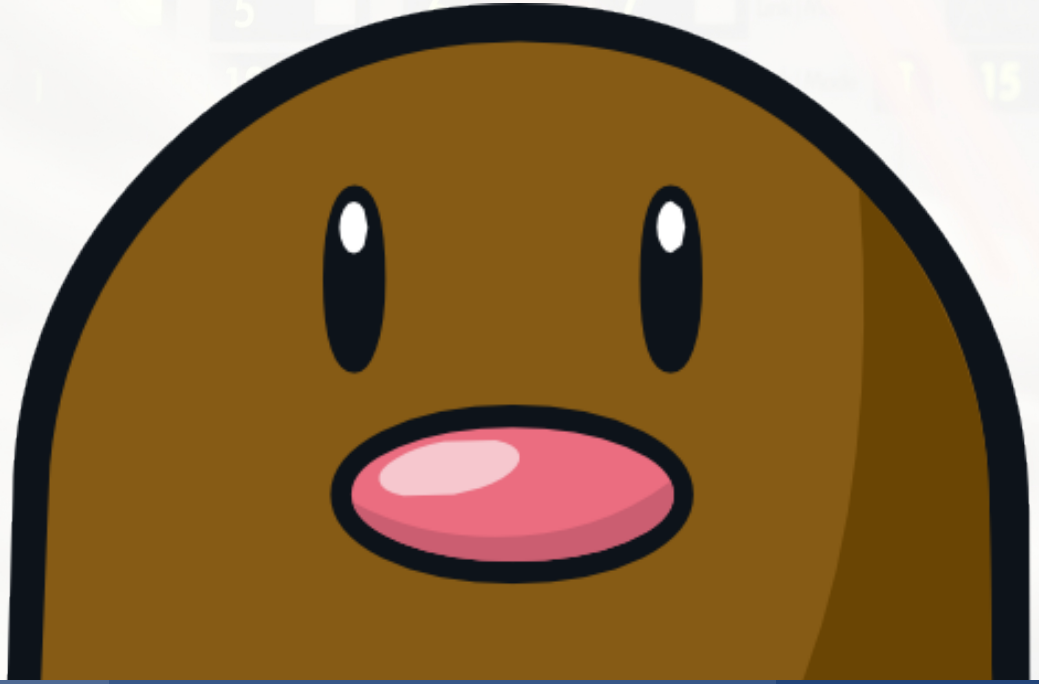
- Les serveurs DNS récursifs
- IPv6
- Les serveurs DNS autoritaires (zone crans.org et zones IP inverses)

Sommaire

1. Ethernet et Internet
2. Infrastructure logicielle
   - Outils internes
   - Base de données
   - Les scripts
   - Surveillance
3. Les services

Réseau ADM

- Vlan "sensible", ne doit pas être propagé publiquement
- La plupart des services sont protégés par simple mot de passe (cranspasswords)
- Accessible depuis un local technique
- Accessible sur *tous* les serveurs (zamok ? !)
- On peut ssh-tunneler !



Les bases de données

- Annuaire LDAP : adhérents, machines, factures
- Interfaçage du compte Crans avec la plupart des services
- Système de réplication automatique

Les bases de données

- Annuaire LDAP : adhérents, machines, factures
- Interfaçage du compte Crans avec la plupart des services
- Système de réplication automatique

Utilisation de bases SQL en interne (intranet, annuaire des prises, upload, etc)

Comment tout cela est géré ?

La plupart des scripts sont situés sur *t*ous les serveurs, dans /usr/scripts/ (montage NFS).

Comment tout cela est géré ?

La plupart des scripts sont situés sur *t*ous les serveurs, dans /usr/scripts/ (montage NFS).
Le code est versionné : gitlab.

Comment tout cela est géré ?

La plupart des scripts sont situés sur *t*ous les serveurs, dans /usr/scripts/ (montage NFS).
Le code est versionné : gitlab.

Et comment qu'on teste ?

- Serveur vo : base ldap de test, annuaire (SQL) de test
- /usr/local/scripts, /usr/local/django
- Serveur apprentis
- La plupart des scripts ont des modes de fonctionnement en test

Surveillance et secours

- Monitoring à l'aide de Munin, Monit, Autostatus
- Surveillance des tentatives d'usurpation d'identité
- Surveillance des locaux sensibles par caméras et enregistrement
- Conservation de certains fichiers journaux conformément aux lois en vigueur.

Surveillance et secours

- Monitoring à l'aide de Munin, Monit, Autostatus
- Surveillance des tentatives d'usurpation d'identité
- Surveillance des locaux sensibles par caméras et enregistrement
- Conservation de certains fichiers journaux conformément aux lois en vigueur.

- Onduleurs
- Deux serveurs de backups dans un local séparé
- Freebox de secours
- Serveur hors campus (OVH/Soyouz) pour redondance mail/DNS

Sommaire

1. Ethernet et Internet
2. Infrastructure logicielle
3. Les services
   - La ferme
   - Le “compte Crans”
   - Stockage et virtualisation
   - Les autres

L'impression (4J)

- Impression laser couleur
- Imprimante : HP MFPM 880
- Facturation : coût réel, compte prépayé
- Bac de sortie : séparation des travaux, agrafage, brochures, perforation
- Accès par digicode (génération aléatoire de code) → `vigile`
- Impression depuis l'intranet (o2), traitement de la tâche par cups (cups) et envoi sur l'imprimante

La TV (cochon, au 4J)

- Plus qu'un seul serveur
- 2 cartes TNT quad-tuner (DVB-T)
- 1 carte satellite (DVB-S)
- Diffusion en multicast
- Utilisation de MumuDVB développé par une nounou

Services aux adhérents

- Mails (webmails, smtp, imap etc)
- Pages personnelles
- Compte ssh sur `zamok`
- Impression
- Compte à vie (ou presque)

Stockage des données : baie de disques (nols)

But : centraliser le stockage à l'aide de matériel fiable.
La baie exporte des volumes à l'aide du protocole iSCSI vers un ensemble de machines.

- Espace disque : env. 8Go par adhérent (stockage des fichiers et des mails)
- Centralisation sur la baie de disques
- Distribution des fichiers par NFS à tous les serveurs (zbee)

Stockage des données : baie de disques (nols)

But : centraliser le stockage à l'aide de matériel fiable.
La baie exporte des volumes à l'aide du protocole iSCSI vers un ensemble de machines.

- Espace disque : env. 8Go par adhérent (stockage des fichiers et des mails)
- Centralisation sur la baie de disques
- Distribution des fichiers par NFS à tous les serveurs (zbee)

Et surtout : une deuxième grappe pour les machines virtuelles.

Virtualisation

- 3 virtualiseurs (kdell, fz, ft)
- Technologie utilisée : linux kvm
- Surcouche proxmox
- Utilisation de la baie de disque (iSCSI) pour centraliser les données
- Migration à chaud
- Machines virtuelles à usage du Crans ou d'autres clubs (FedeRez, bde, gala etc.)

Les grands oubliés

- Le Wiki
- Intranet
- OwnCloud
- Les news
- IRC
- Jabber
- Listes de diffusion (mailman)
- Miroir Debian (et Ubuntu, etc)

Conclusions

- Grand panorama de ce qu'on fait au Crans

Conclusions

- Grand panorama de ce qu'on fait au Crans
- Il y en a pour tous les goûts

Conclusions

- Grand panorama de ce qu'on fait au Crans
- Il y en a pour tous les goûts
- Venez avec vos idées !

Merci de votre attention !