

Les switches du Cr@ns

Olivier Iffrig

Cr@ns

8 décembre 2009

1 Introduction

2 Fichier de configuration du switch

3 Configurer le switch

Introduction

Matériel utilisé
Plan du réseau
Authentification

Fichier de
configuration
du switch

Configuration
générale
VLANs
Prises
Administration
Divers

Configurer le
switch

Configuration
manuelle
Scripts Python
de gestion des
switchs

Fin

1 Introduction

Matériel utilisé

Plan du réseau

Authentification

Olivier Iffrig

Introduction

Matériel utilisé

Plan du réseau

Authentification

Fichier de
configuration
du switch

Configuration
générale

VLANs

Prises

Administration

Divers

Configurer le
switch

Configuration
manuelle

Scripts Python
de gestion des
switchs

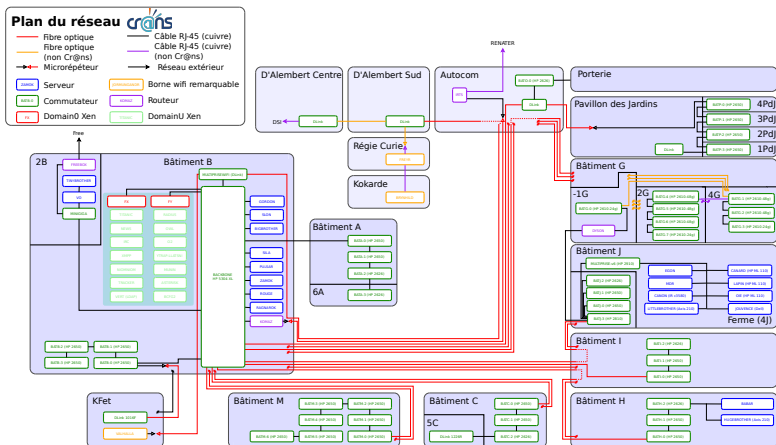
Fin

Matériel utilisé

HP ProCurve 26xx



Plan du réseau



Authentification

- Protocole RADIUS, serveur FreeRADIUS sur sable et radius
- Lance `radius_auth.py` qui gère l'authentification
- Permet d'affecter les VLANs de manière dynamique et de centraliser l'authentification

② Fichier de configuration du switch

Configuration générale

VLANs

Prises

Administration

Divers

- Le header doit correspondre au switch utilisé
- `hostname` Nom du switch
- SNMP
- Date/heure, timeout, logs (sur vo), IP du switch

Configuration générale

```
; J9085A Configuration Editor; Created on  
release #R.11.25
```

```
hostname "batg-7"
```

```
-----  
                Snmp  
snmp-server contact "root@crans.org"  
snmp-server location "Batiment G"  
;A faire a la main  
snmpv3 enable  
snmpv3 restricted-access  
;snmpv3 user "initial"  
snmpv3 user "crans"  
snmpv3 group ManagerPriv user "crans" sec-model  
ver3  
snmp-server community "public" Operator
```

```
-----  
                Heure/date  
time timezone 60  
time daylight-time-rule Western-Europe  
snmp server 10.231.136.3  
timesync snmp  
snmp unicast
```

```
-----  
                Misc  
console inactivity-timer 30
```

```
-----  
                Logs  
logging 10.231.136.12
```

```
-----  
                IP du switch  
ip default-gateway 10.231.136.4
```


VLANs

- `vlan` Numéro
- `name` Nom
- `[un]tagged <prises>`
- `[no] ip address`
Adresse IP sur le VLAN
- IGMP (multicast)

```
vlan 1
  name "DEFAULT.VLAN"
  untagged 25-26
  no ip address
  ip igmp
  no ip igmp querier
  exit
vlan 2
  name "Adm"
  tagged 25-26
  ip address 10.231.136.97 255.255.255.0
  exit
```

Introduction

Matériel utilisé
Plan du réseau
Authentification

Fichier de configuration du switch

Configuration
générale
VLANs
Prises
Administration
Divers

Configurer le switch

Configuration
manuelle
Scripts Python
de gestion des
switchs

Fin

- `aaa port-access mac-based`

`<num>`

- `addr-limit <n>`
Nombre de MAC autorisées
- `logoff-period` Expiration
de l'authentification
- `unauth-vid VLAN` à
utiliser en cas d'échec
d'authentification

- `flow-control` Contrôle du flood
- `no lacp` Pas d'agrégation de liens

```
aaa port-access mac-based 7
aaa port-access mac-based 7 addr-limit 3
aaa port-access mac-based 7 logoff-period 3600
aaa port-access mac-based 7 unauth-vid 1
interface 7
  enable
  name "Chambre_G149"
  flow-control
  no lacp
exit
```

Administration

- Pas de telnet ni d'interface web

```
no telnet-server
```
- Désactivation des interfaces SSH inutiles

```
no web-management  
aaa authentication ssh login public-key none  
aaa authentication ssh enable public-key none  
ip ssh
```
- SSH autorisé pour les machines d'administration

```
ip authorized-managers 10.231.136.0 255.255.255.0  
ip ssh filetransfer
```

Introduction

Matériel utilisé
Plan du réseau
Authentification

Fichier de configuration du switch

Configuration
générale
VLANs
Prises
Administration
Divers

Configurer le switch

Configuration
manuelle
Scripts Python
de gestion des
switchs

Fin

Divers

- DHCP snooping
- Protection contre les boucles
- Serveurs radius
- Filtrage MAC

```
dhcp-snooping vlan 1
dhcp-snooping trust 25-26
no dhcp-snooping trust 1-24,27-28
dhcp-snooping authorized-server 138.231.151.1
; Activation
dhcp-snooping
;
loop-protect disable-timer 30
loop-protect transmit-interval 3
loop-protect 1-24,27-28
;
radius-server dead-time 2
radius-server host 10.231.136.72
radius-server host 10.231.136.9
;
aaa port-access mac-based addr-format multi-colon
;
no cdp run
no stack
```

③ Configurer le switch

Configuration manuelle

Scripts Python de gestion des
switchs

Configuration manuelle

- Se connecter à rouge (ou zamok)
- Envoyer le fichier dans `/cfg/startup-config` sur le switch

Scripts Python de gestion des switchs

- `gestion/hptools.py` Communication avec un switch
- `gestion/majswitch.py` Mise à jour du firmware d'un switch
- `gestion/gen_confs/switchs.py` Génération du fichier de configuration

Olivier Iffrig

Introduction

Matériel utilisé
Plan du réseau
Authentification

Fichier de configuration du switch

Configuration
générale
VLANs
Prises
Administration
Divers

Configurer le switch

Configuration
manuelle
Scripts Python
de gestion des
switchs

Fin

Questions ?