






BTS SIO

DHCP + VLAN



Aleksandar Nikolic

PLAN DE LA SITUATION

-  Introduction.....
-  Contexte et objectifs du projet....
-  Technologies et outils utilisés.....
-  Démarche mise en place.....
-  Conclusion.....

INTRODUCTION

Dans le cadre de mon projet professionnel, j'ai été chargé d'intervenir pour le compte de l'entreprise Securitas, spécialisée dans la sécurité privée.



Securitas est une entreprise internationale spécialisée dans la sécurité privée.

Elle propose des services de surveillance humaine, de sécurité mobile, de télésurveillance et de solutions électroniques pour protéger les biens et les personnes.

En France, Securitas compte environ 17 000 employés et intervient auprès d'entreprises de tous secteurs pour garantir leur sécurité.

La mission consistait à concevoir un Template de configuration réseau destiné à automatiser et uniformiser la configuration d'une centaine de switchs récemment livrés.

CONTEXTE ET OBJECTIFS

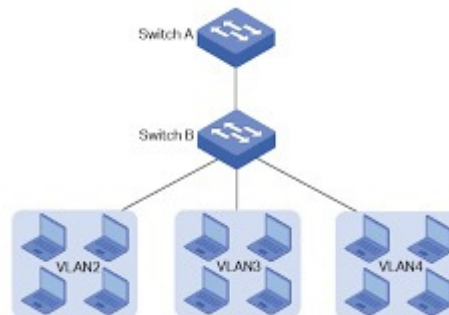
DU PROJET

Les switches étaient livrés en version d'usine et nécessitaient une mise à jour du firmware afin d'être conformes aux standards techniques et sécuritaires de l'entreprise.

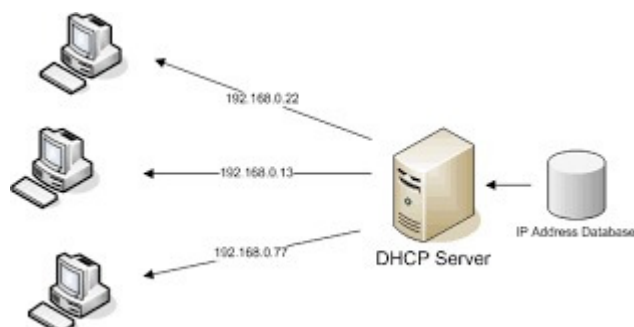
Standards techniques et sécuritaires de l'entreprise.

Une fois les mises à jour terminées, j'ai également eu pour responsabilité de :

- Créer et configurer des VLANs pour séparer les différents services (RH, Technique, Commercial) sur le réseau.



- Configurer un serveur DHCP pour automatiser l'attribution des adresses IP selon les VLANs.



L'objectif global était de structurer, sécuriser et standardiser le réseau interne de Securitas à travers des actions de mise à jour matérielle et de configuration logique adaptées à leurs besoins.

TECHNOLOGIES ET OUTILS

UTILISÉS

Switchs

- Switchs livrés par Securitas, nécessitant une mise à jour du firmware et la création de VLANs.

C9200-24P-E



Clé USB au format FAT32

- Une clé USB au format FAT32 contenant le fichier de mise à jour du firmware.
- Utilisée pour flasher directement les switchs via leur port USB intégré.

Template de configuration fourni par les ingénieurs

- Document transmis par l'équipe technique de Securitas.
- Contenait : Les paramètres attendus après la mise à jour.

DHCP Server

Serveur DHCP permettant d'attribuer automatiquement une adresse IP aux postes clients connectés aux VLANs.

- Chaque VLAN dispose de sa propre plage IP attribuée par le serveur DHCP.

VLANs

- VLAN 10 : Service Administratif
- VLAN 20 : Service Technique
- VLAN 30 : Service Commercial
- Créés pour séparer le réseau en fonction des différents services de l'entreprise.

DÉMARCHE MISE EN PLACE

1. Préparation des équipements

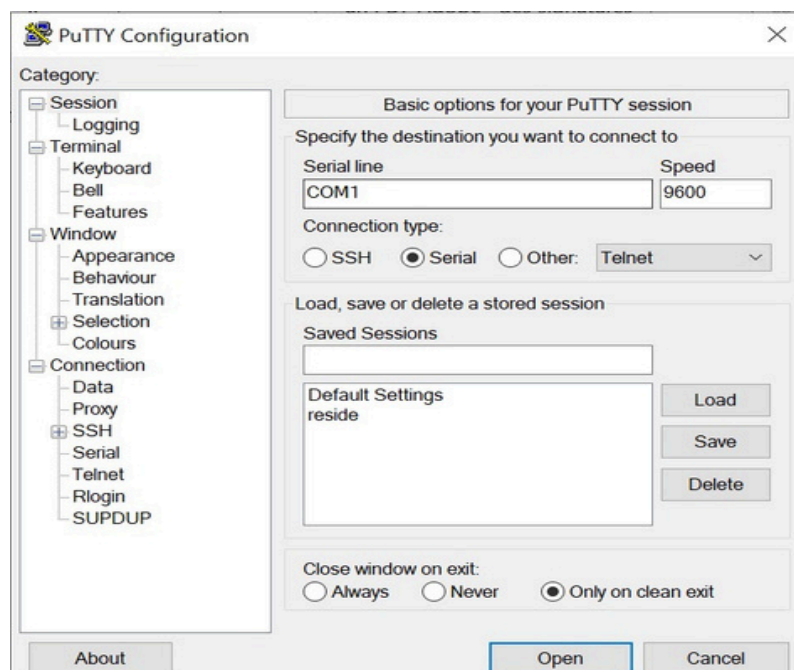
- **Branchement physique** des switches : alimentation et connexion console.
- **Préparation de la clé USB** formatée en FAT32 contenant les fichiers de mise à jour firmware.
- **Préparation du fichier de configuration** fourni par les ingénieurs (template) avec les VLANs à créer et les paramètres réseau attendus.

C9200-24P-E



2. Accès aux switches avec PuTTY

- Utilisation du logiciel **PuTTY** pour établir une connexion en **console série** aux switches.
- Connexion directe pour permettre la configuration initiale et vérifier l'état des équipements.



3. Implémentation de la configuration

Création des VLANs selon les besoins :

- o VLAN 100 → Service Direction
- o VLAN 200 → Service Maintenance
- o VLAN 300 → Service Sécurité
- o
- **Configuration du DHCP** pour que chaque VLAN puisse recevoir des adresses IP automatiquement.
- **Application des paramètres réseau** selon le fichier de template (interfaces, passerelles, scopes IP).

```
# Entrer en mode configuration
configure terminal

# Création des nouveaux VLANs
vlan 100
  name Direction
exit

vlan 200
  name Maintenance
exit

vlan 300
  name Sécurité
exit

# Configuration des interfaces pour affecter les ports aux VLANs
interface range GigabitEthernet0/1-10
  switchport mode access
  switchport access vlan 100
exit

interface range GigabitEthernet0/11-20
  switchport mode access
  switchport access vlan 200
exit

interface range GigabitEthernet0/21-30
  switchport mode access
  switchport access vlan 300
exit

# Sauvegarde de la configuration
write memory
```

```
# Entrer en mode configuration
configure terminal

# Activer le service DHCP
service dhcp

# Définir le pool DHCP pour le VLAN 100 (Direction)
ip dhcp pool VLAN100_DIRECTION
  network 192.168.100.0 255.255.255.0
  default-router 192.168.100.1
  dns-server 8.8.8.8
exit

# Définir le pool DHCP pour le VLAN 200 (Maintenance)
ip dhcp pool VLAN200_MAINTENANCE
  network 192.168.200.0 255.255.255.0
  default-router 192.168.200.1
  dns-server 8.8.8.8
exit

# Définir le pool DHCP pour le VLAN 300 (Sécurité)
ip dhcp pool VLAN300_SECURITE
  network 192.168.300.0 255.255.255.0
  default-router 192.168.300.1
  dns-server 8.8.8.8
exit

# Sauvegarder la configuration
write memory
```

4. Mise à jour du firmware

- Insertion de la **clé USB** dans les switchs.
- Mise à jour du firmware lancée depuis l'interface CLI (menu dédié ou commandes spécifiques).
- Vérification après redémarrage que la **version du firmware** correspond bien à celle attendue.

```
10 : faire la mise à jour firmware  
Avoir une clé USB au format FAT32, mettre le fichier 'WC_16_11_0023.swi' dessus.
```

```
autoriser l'utilisation de clé USB :  
usb-port
```

```
faire l'upgrade  
copy usb flash WC_16_11_0023.swi primary
```

```
reload car il ne se fait pas automatiquement  
Après reboot, vérifier la version active : 'show version'
```

```
remettre le port usb en mode inutilisable :  
no usb-port
```

```
faire une sauvegarde:  
wr mem
```

5. Tests et validation

- **Test du DHCP** : vérification que les postes clients obtiennent bien une adresse IP automatiquement dans le bon VLAN.
- **Test de connectivité** : tests de ping entre équipements pour valider la communication (ou l'isolement) entre VLANs.
- **Vérification de la version firmware** sur chaque switch pour confirmer la réussite de la mise à jour.

VLAN:

```
bash
```

```
show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Gi0/31-48
100	Direction	active	Gi0/1-10
200	Maintenance	active	Gi0/11-20
300	Sécurité	active	Gi0/21-30

Commande CLI ou sur un poste client :

```
bash
```

```
ping 192.168.100.11
```

```
ping 192.168.200.12
```

```
ping 192.168.300.13
```

DHCP :

```
bash
```

```
show ip dhcp binding
```

```
ruby
```

IP address	Client-ID/Lease	expiration
192.168.100.11	01:00:11:22:33:44:55	23h59m
192.168.200.12	01:00:66:77:88:99:aa	23h59m
192.168.300.13	01:00:bb:cc:dd:ee:ff	23h59m

VERSION FIRMWARE :

```
bash
```

```
show version
```

CONCLUSION

Ce projet m'a permis de répondre à une demande concrète de l'entreprise Securitas, qui m'a confié la mission de concevoir un Template de configuration pour le futur déploiement de plusieurs dizaines de switchs réseau. L'objectif était de préparer un modèle standard intégrant :

- La création de VLANs pour organiser le réseau en fonction des services (Direction, Maintenance, Sécurité),
- La configuration d'un serveur DHCP pour automatiser l'attribution des adresses IP,
- Et la mise à jour des firmwares pour garantir la sécurité et la compatibilité des équipements.

L'ensemble des configurations a été testé et validé avec succès sur un switch pilote. Ce modèle pourra ainsi être réutilisé rapidement et en toute sécurité pour équiper les futurs sites de l'entreprise, tout en assurant une homogénéité du réseau.

Pistes d'amélioration :

- Automatiser les mises à jour et configurations avec des scripts ou des outils de déploiement centralisé (ex : Ansible, Python).
- Mettre en place une supervision réseau pour suivre en temps réel l'état des VLANs, du DHCP et des switchs.

- Sécuriser les communications inter-VLANs grâce à l'utilisation d'ACL (Access Control List) si nécessaire.
- Documenter et centraliser le Template dans un référentiel accessible pour l'équipe IT.