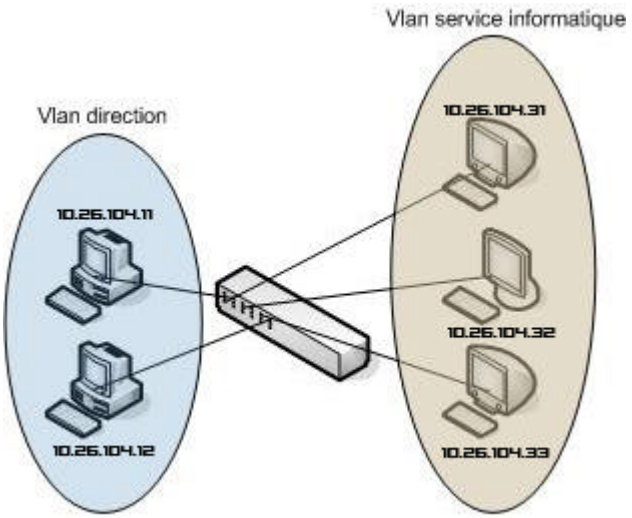
Mise en place d'un réseau sécurisé par VLAN
Contexte : Dans le cadre de la mise en place d'un réseau, il nous est demandé d'assurer la confidentialité et la sécurité de celui-ci à l'aide de Vlan. Objectifs : Sécuriser et segmenter le réseau pour en augmenter les performances et la fiabilité.

Description de l'activité réalisée
Situation initiale : *Le réseau n'est pas segmenté, et la sécurité est inexistante, toutes les stations ont accès à l'ensemble du réseau.* Situation finale : *Après la réalisation de l'activité, le réseau est segmenté, les domaines de collisions sont séparés et réduits et la sécurité entre les deux réseaux virtuels est accrue.*
Outils utilisés : Nous avons utilisé un commutateur Cisco Catalyst 2900 series XL avec un logiciel serveur TFTP pour sauvegarder la configuration du commutateur.

Déroulement de l'activité :

Nous devons mettre en place deux réseaux virtuels à accès sécurisé sur notre commutateur. Le réseau du service informatique (*IP:10.26.104.31-33 masque : 255.255.255.0*) et celui de la direction *(IP : 10.26.104.11-12 masque : 255.255.255.0*). De plus, seul le pc du responsable informatique (IP : 10.26.104.32) doit avoir accès au commutateur pour en assurer les modifications.



1. Configuration du commutateur Cisco

   - Principe

Le système de VLAN (Virtual Local Area Network) permet de procéder a un regroupement logique de certains ports d'un commutateur pour simuler un LAN (Local Area Network).
Concrètement nous allons utiliser les vlan pour séparer deux réseaux différents et créer une segmentation qui va réduire le domaine de collisions tout en assurant une parfaite sécurité.

   - Mise en place des vlan

Commençons par mettre en place nos vlan dans notre configuration.
Pour cela il nous faut nous connecter sur le commutateur grâce au port console et s'identifier en mode « enable » (cf. : utilisateur privilégié).

Créons notre premier vlan qui va correspondre au réseau du service informatique :

```
switch_test#vlan database
switch_test (vlan)#vlan 2 name informatique
VLAN 2 added:
Name: informatique
```

créons ensuite notre deuxième vlan pour le réseau de la direction

```
switch_test#vlan database
switch_test (vlan)#vlan 3 name direction
VLAN 3 added:
Name: direction
```

?? Attribution des ports aux différents vlan

Une fois nos vlan créés il nous faut attribuer les ports correspondants aux différents services sur les vlan.
Pour le port 1 du commutateur qui sera sur le réseau du service informatique :

```
switch_test#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch_test(config)#interface Fa0/1
switch_test(config-if)#switchport access vlan 2
```

Pour le port 2 du commutateur qui sera sur le réseau de la direction :

```
switch_test#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch_test(config)#interface Fa0/2
switch_test(config-if)#switchport access vlan 3
```

?? Attribution d'une ip au commutateur

Pour permettre l'accès en telnet sur le commutateur nous allons lui attribuer une adresse ip accessible depuis réseau informatique :

```
switch_test#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch_test(config)#interface vlan 2
switch_test(config-subif)#ip address 10.26.104.253 255.255.255.0
```

Définissons ensuite cette interface comme l'interface principale du commutateur :

```
switch_test#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch_test(config)#interface vlan 2
switch_test(config-subif)#management
```

?? Mise en place de la liste d'accès

Nous devons n'autoriser l'accès par telnet que depuis l'adresse ip du responsable informatique.
Pour cela nous allons créer une access list :

```
switch_test#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch_test(config)#access-list 1 permit 10.26.104.32
switch_test(config)#access-list 1 deny any
```

Cette access list aura pour effet de n'accepter que l'utilisateur de l'ip 10.26.104.32.
Appliquons maintenant cette access list sur les sessions telnet :

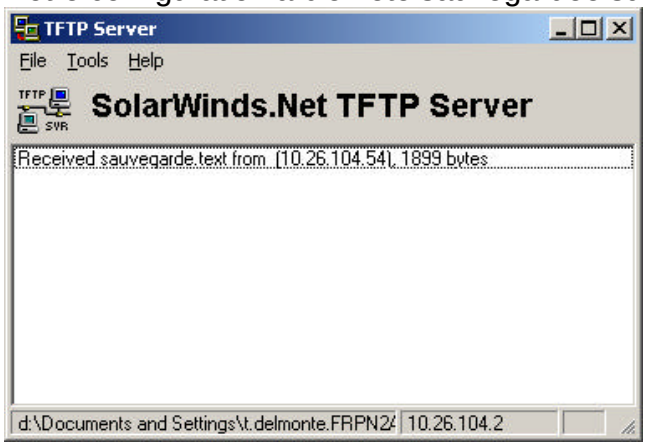
```
switch_test#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch_test(config)#line vty 0 4
switch_test(config-line)#access-class 1 in
```

2. Sauvegarde de la configuration

Pour s'assurer de toujours être en mesure de répliquer la configuration du commutateur en cas d'erreur ou de dysfonctionnement de celui – ci, nous allons sauvegarder la configuration actuelle sur un serveur tftp installé sur une station Windows 2000 pro du réseau informatique.
Nous installons le serveur tftp solarwinds 2003 sur la station d'ip 10.26.104.2.
Nous pouvons maintenant procéder à la sauvegarde de la configuration :

```
switch_test#copy flash:config.text tftp://10.26.104.2/sauvegarde.text
Address or name of remote host [10.26.104.2]? 10.26.104.2
Destination filename [sauvegarde.text]? sauvegarde.text
!!
1899 bytes copied in 0.598 secs
```

Notre configuration a bien été sauvegardée sur notre station :



3. Vérification à l'aide de test

Nous pouvons maintenant vérifier notre configuration a l'aide de plusieurs tests.

?? Test de la sécurité entre les vlan

Plaçons nous, sur une station du réseau de direction et faisons un ping sur le réseau informatique :

```
C:\>ping 10.26.104.31
Pinging 10.26.104.31 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 10.26.104.31:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Le réseau informatique est bien inaccessible depuis le réseau de direction

Effectuons le même test depuis le réseau informatique vers le réseau de direction :

```
[root@unix /]# ping 10.26.104.11
PING 10.26.104.11 (10.26.104.11) 56(84) bytes of data.
--- 10.26.104.11 ping statistics ---
173 packets transmitted, 0 received, 100% packet loss, time 172037ms
```

?? Test de l’accès en telnet au commutateur

Testons la sécurité de l’accès en telnet sur le commutateur.
Effectuons un essai de connexion en telnet via un poste du réseau informatique.

```
C:\>telnet 10.26.104.253
Connecting To 10.26.104.253...
Could not open a connection to host on port 23 : Connect failed
```

Effectuons ce même test depuis la station du responsable informatique qui est autorisé à se connecter dans l’access list :

```
[root@unix /]# telnet 10.26.104.54
Trying 10.26.104.54...
Connected to 10.26.104.54.
Escape character is '^]'.
###################################
#              Switch Test          #
#                                   #
###################################
User Access Verification
Password:
switch_test>
```

Le poste du responsable informatique est donc le seul à pouvoir se connecter sur le commutateur en telnet.

Les deux vlan ne peuvent donc pas communiquer. Seul les personnes dont les postes sont branchés sur des ports, où les vlan attribués correspondent, pourront communiquer entre eux.
Le responsable informatique est la seule personne à avoir un accès sur le commutateur.