



Epreuve de Pratique des Techniques Informatiques

Nom et prénom : ALO David

Nature de l'activité

Création de VLAN avec port monitoring et Spanning Tree

Contexte : Une entreprise avec plusieurs services décide que chacun d'eux soit indépendant et ne puissent pas communiquer. Cependant, il n'est pas question d'avoir un nombre important de matériels, la simplicité d'administration est recommandée et une tolérance de panne est à envisager.

Objectifs :

- Création d'un réseau par service
- limiter l'achat de matériel
- avoir une tolérance de panne

Compétences mises en œuvre pour la réalisation de cette activité

C22	Installer et configurer un réseau
C23	Installer et configurer un dispositif de sécurité
C26	Installer un périphérique
C34	Surveiller et optimiser le trafic sur le réseau

Conditions de réalisations

Matériels :

- 2 switches administrable
- 4 postes

Logiciels :

- Windows XP
- Hyperterminal
- putty
- Wireshark (analyseur de trames)

Durée : 45 mn

Autres contraintes et difficultés : Rien n'est installé sur le nouveau serveur

Description de l'activité réalisée

Situation initiale : Les services communiquent tous les uns avec les autres générant ainsi des failles de sécurité.

Situation finale : Tous les services sont tous indépendant.

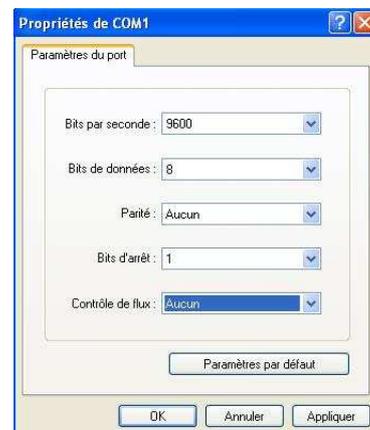
I. Configuration du switch

Dans un premier temps, il est nécessaire pour administrer le switch, de se connecter au switch par le port COM et lancer l'hyper-terminal.

L'hyper-terminal demande certains paramètres de transmission afin de pouvoir communiquer avec le matériel connecté. Ils sont spécifiques à chaque matériel.

Propriete du switch sur COM :

Bits par seconde : 9600
 Bits de données : 8
 Parité : aucun
 Bit d'arrêt : 1
 Contrôle de flux : aucun



Enfin appuyer deux fois sur entrer pour accéder à l'administration du switch.

Il est préférable de commencer par une réinitialisation du switch afin de ne pas se soucier d'une configuration préexistante.

```
# erase startup-config (attendre et suivre les instructions)
```

Une demande de reboot est alors requise. Le switch se met à clignoter et nous montre qu'il se réinitialise.

Pour permettre d'administrer le switch à distance, on lui attribue une adresse IP : 192.168.10.10/24. Ainsi, par le biais d'un navigateur ou du service telnet, il sera possible d'apporter n'importe quelle modification au switch administrable.

```
#menu (pour accéder au menu)
```

```
#voulez-vous sauvegarder la configuration (valider)
```

Switch configuration / IP configuration / Ipconfig DHCP : Manual

IP Adress : 192.168.10.10/24

Subnet Mask : 255.255.255.0

Nous avons donc attribué une adresse IP au switch de 192.168.10.10

Nous pouvons désormais configurer le switch avec le protocole HTTP à partir du navigateur en tapant l'adresse 192.168.10.10 ou par le biais de putty.

II. Configuration des postes clients

Nous allons attribuer une adresse à chacun des postes :

Poste 1 : 192.168.10.1 (direction)

Poste 2 : 192.168.10.2 (direction)

Poste 3 : 192.168.10.3 (commercial)

Poste 4 : 192.168.10.4 (commercial)

A ce niveau, aucun VLAN n'est configuré et on peut vérifier que chacun des postes peut communiquer avec tous les autres.

III. Création de VLAN

Toujours en utilisant le logiciel Hyper Terminal, nous allons créer un VLAN par service.

Il restera toujours un VLAN par défaut et son ID sera 1.

Pour la direction, nous allons attribuer l'ID : 2 et le nom de VLAN : direction

Pour le commercial, nous allons attribuer l'ID : 3 et le nom de VLAN : commercial

```
VLAN Menu / VLAN Name /      VLAN ID :
                               Name :
```

La méthode des VLAN par port est choisit pour plusieurs raisons :

- C'est la plus simple à monter
- Le réseau et la sécurité sont aussi performants qu'avec les autres méthodes

Les VLAN créés, il faut maintenant les attribuer aux machines.

Dans le VLAN menu :

->3. VLAN port assignement

```
=====CONSOLE – MANAGER MODE=====
          Defaut VLAN      direction      commercial
port 1 : direction        No            Untagged     No
port 2 : direction        No            Untagged     No
port 3 : commercial       No            No            Untagged
port 4 : commercial       No            No            Untagged
```

Ne pas oublier de sauver.

Résultat :

Les postes 1 et 2 ping entre eux car ils font parti du même VLAN « direction »

Les postes 3 et 4 ping entre eux car ils font parti du même VLAN « commercial »

Il est impossible d'atteindre le VLAN direction à partir du VLAN commercial et vice-versa

Avec Wireshark, on voit bien qu'aucun paquet broadcast (ARP) ne passe sur un VLAN différent.

Les postes 1 à 4 sont sur le même réseau et pourtant les services sont bien indépendants.

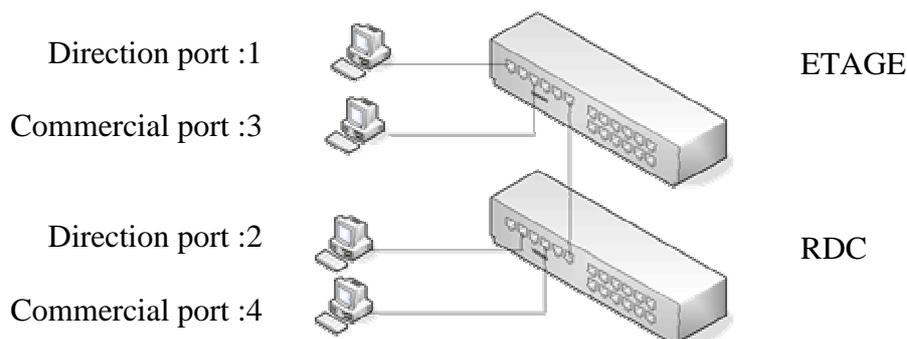
Pour le bon fonctionnement d'un administration à distance, nous sommes obligé de mettre les différents VLAN sous des réseaux différent. Nous allons alors créer des VLAN avec comme sous réseaux : 192.168.10.0 et 192.168.11.0.

IV. Insertion d'un deuxième switch

Il est fréquent de trouver plus d'un switch dispatché dans un établissement. Ici nous allons considérer que les services sont dispatchés sur 2 étages.

Pour pouvoir ajouter un autre switch et donc disposer de 24 ports supplémentaires, il est nécessaire de garder la même configuration des VLAN. Seul l'ID est important, car c'est avec lui que les switches vont échanger.

Un lien physique sera monté entre les 2 switches. Dans ce lien passeront les trames du VLAN direction et du VLAN commercial. Afin de reconnaître a quel VLAN appartienne ces trames, nous devons tagger ce port sur le switch 1 et sur le switch 2. Toutes les informations passent par un seul câble tout en gardant l'imperméabilité de chacun des VLAN.



IV. Monitorer un port

En tant qu'administrateur réseau, il est important de pouvoir contrôler si les trames circulent correctement sur tout le réseau. Les VLAN peuvent être un frein à la visibilité du trafic. Monitorer un port présente un intérêt certain et il est très facile à mettre en place.

Menu / Switch Configuration / Network Monitoring Port

```

=====CONSOLE – MANAGER MODE=====
Monitoring port : 2
port 4 : action monitor

```

Le port 2 verra alors toutes trames du port 4 avec Wireshark.

Il est ainsi possible de voir tous les échanges entre les 2 switches en monitorant le port 6 (lien physique les reliant)

VI. Gérer la tolérance de panne

Afin de gérer la tolérance de panne, on peut proposer l'échange entre les 2 VLAN avec 2 câbles plutôt qu'un seul. En effet, le lien établi sur les ports 6 qui permet la communication entre les switches et leurs vlans respectifs, devient un lien critique puisqu'il est unique.

Grâce aux 2 liens, si un des deux vient à dysfonctionner, l'autre prend le relais.

Cependant, un phénomène se produit quand l'on relie 2 switches avec 2 câbles, il s'agit du phénomène de boucle qui pollue tout le réseau et l'empêche de fonctionner correctement. Les échanges sont alors interrompus. Avec Wireshark, on s'aperçoit que le nombre de paquets échangé est anormalement élevé.

Pour résoudre le problème, on doit activer le protocole « spanning tree ». Le « Spanning tree » permet de casser cette boucle en désactivant les ports du lien de « secours ». De par le protocole STP (802.1d), il va désactiver le lien concerné, en se basant sur un système de coût qu'il va négocier lui-même (par défaut). Si le lien actif vient à défaillir, il va automatiquement activer le lien de « secours ».

Analyse des résultats obtenus

Objectif atteint : On dispose d'un cd d'installation automatisé qui propose des environnements pré configurés

Bilan de l'activité : On peut maintenant facilement installer Windows Xp avec ses logiciels. De plus si nous devons utiliser ce cd pour des postes identiques on peut intégrer les pilotes pour le matériel.