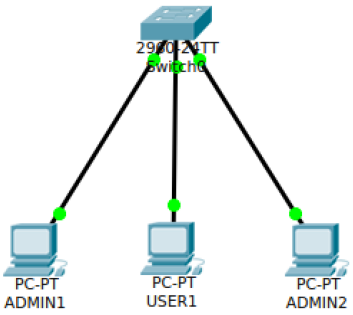
TP Service sur réseaux N°2 - MMI1 - Semestre 2

Introduction

Ce TP a pour objectif de mettre en application les VLAN et d'introduire la notion de sécurité d'accès au réseau physique par les mécanismes de limitation de propagation de VLAN et de sécurité lié au port.

Les VLAN

Saisir le schéma suivant sur Packet Tracer.



1. Nous allons créer 2 VLAN:

   VLAN 10, qui s'appelera « ADMIN »

   VLAN 20, qui s'appelera « USER »

   Procédure pour créer un vlan:

   ```
   Switch>enable
   Switch#conf t
   Switch(config)#vlan 10
   Switch(config-vlan)#name ADMIN
   ```

   Terminez la saisie de la configuration en tapant CTRL+Z.

   Vérifiez la configuration par la commande :

   ```
   Switch>show vlan
   ```

2. Affectez à chacun de vos PC une adresse IP en fonction du plan d'adressage (ci-dessous) fourni.

   Les PC du VLAN 10 font parti du réseau : 192.168.10.0/24

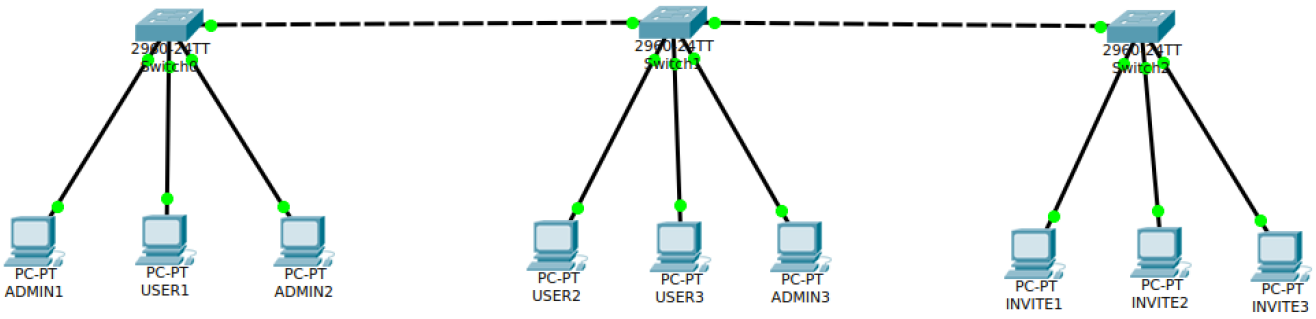
   Les PC du VLAN 20 font parti du réseau : 192.168.20.0/24

3. Affectez les ports des switchs reliés à un PC au bon VLAN, grâce aux commandes suivantes :

   ```
   Switch>enable
   Switch#conf t
   Switch(config)#interface fast 0/1
   Switch(config-if)#switchport mode access
   Switch(config-if)#switchport access vlan 10
   ```

4. Testez votre architecture par des ping. En particulier vérifiez que :
   1. le PC ADMIN1 peut pinger le PC admin2
   2. le PC USER1 ne peut pas pinger les PC ADMIN

5. Etendez votre réseau selon le schéma ci-dessous. Un nouveau VLAN est à créer : le VLAN 30 appelé INVITE.



6. Affectez à chacun de vos nouveaux PC une adresse IP en fonction du plan d'adressage.

   Les PC du VLAN 30 font parti du réseau : 192.168.30.0/24

7. Configurez les liens entre les switch en mode access. Positionnez-les dans le VLAN USER. La communication entre les postes de ce VLAN est-elle correcte ?
8. Configurer les liens entre switches en mode access dans le VLAN ADMIN. PC-PT USER1 peut-il encore pinger PC-PT USER2 ?
9. Lancez en mode simulation un ping entre 2 PC ADMIN. Analyser, en mode pas à pas (Capture & Forward), les trames circulant sur les liens.
10. Retirer la configuration « mode access » sur les ports reliant les switchs.

```
Switch>enable
Switch#conf t
Switch(config)#interface fast 0/24
Switch(config-if)#no switchport mode access
Switch(config-if)#no switchport access vlan 10
```

11. Configurez les liens entre chaque switch en mode trunk.

```
Switch>enable
Switch#conf t
Switch(config)#interface fast 0/24
Switch(config-if)#switchport mode trunk
```

12. Lancez en mode simulation un ping entre 2 PC ADMIN. Analyser, en mode pas à pas (Capture & Forward), les trames circulant sur les liens. Observez les onglets 'Inbound PDU Details' et 'Outbound PDU details' Quelles caractéristiques ont ces trames ?
13. Regardez sur chaque lien trunk, les VLAN autorisés.

```
Switch>show interfaces switchport
```

14. Le switch 3 est situé dans une salle libre service, afin d'ajouter un peu de sécurité, enlevez sur le trunk des switchs 2 et 3 le transport du VLAN ADMIN et confirmez la configuration en visualisant la liste des VLAN autorisés pour cette interface.

```
Switch>enable
Switch#conf t
Switch(config)#interface fast 0/24
Switch(config-if)#switchport trunk allowed vlan remove 10
```

15. Vous pouvez confirmer votre configuration en regardant la table des adresses mac : si vous ne voyez aucune MAC dans le vlan 10, alors ce VLAN est correctement filtré.

```
Switch>show mac-address-table
```

16. Pour plus de sécurité, effacez le VLAN 10 du switch 3

```
Switch>enable
Switch#conf t
Switch(config)#no vlan 10
```

17. Jusqu'à présent la sécurité était limité par la possibilité d'accès physique aux prises réseaux ou aux switches. Positionner un poste de type USER sur un port associé au VLAN ADMIN, par exemple le port 3 du switch 1. Peut-il avoir accès à ce VLAN ?
18. Ajouter une sécurité liée à l'adresse MAC pour que l'utilisation frauduleuse d'un poste non autorisé soit impossible. Configurez le port 3 du switch 1 de la façon suivante :

```
Switch>enable
Switch#conf t
Switch(config)#interface fast 0/3
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address H.H.H
```

Contrôlez la configuration

```
Switch>enable
Switch#show port-security interface fa 0/3
```

19. Tentez maintenant un accès frauduleux en branchant un PC USER sur le port que vous venez de protéger. Changez l'adresse IP du PC afin d'être dans le même plan d'adressage que le VLAN ADMIN, et observez le comportement du switch. Que s'est-il passé ? Revenir à une situation normale :

```
Switch>enable
Switch#conf t
Switch(config)#interface fast 0/3
Switch(config-if)#shut
Switch(config-if)#no shut
```