

TD 5 : Cisco Packet Tracer

Équipe pédagogique : Zhiyi ZHANG, Saeed ALSABBAGH

Objectifs pédagogique

- Découvrir Packet Tracer
- Apprendre à construire un réseau avec Packet Tracer
- Observer de l'apprentissage des adresses MAC d'un switch
- Se connecter au commutateur à l'aide d'une connexion de console
- Parcourir divers modes CLI
- Vérification d'une configuration du commutateur
- Créer une configuration de base du commutateur
- Sauvegarder la configuration du commutateur

1 Cisco Packet Tracer

1.1 Introduction

Cisco Packet Tracer est un logiciel de simulation réseau développé par Cisco Systems. Il nous permet de :

- Concevoir des topologies réseau virtuelle
- Configurer des routeurs, commutateurs, PC, serveurs...
- Simuler la transmission des paquets
- Observer le fonctionnement des protocoles réseau

Il permet de réaliser des travaux pratiques sans matériel réel.

1.2 Interface graphique

1. Barre de menus
Contient les fonctions classique (nouveau projet, ouvrir, sauvegarder...).
2. Barre d'outils principale
Accès rapide aux actions : sélection, déplacement, suppression, ajout de notes, ...
3. **Zone de travail (WorkSpace)**
C'est la partie centrale. On y construit la topologie réseau avec les routeurs, commutateurs, PC... C'est l'espace principal.
4. **Panneau de sélection des équipements(machines, câbles...)**
La sélection se fait en trois niveau. Bien que Packet Tracer propose plusieurs catégories d'équipements, on travaille principalement avec deux catégories : Network Devices et End Devices. Dans la catégorie Network Devices, on utilise principalement les routeurs et les switches. Dans la catégorie End Devices, il existe une sous-catégorie appelée également End Devices. On utilise surtout PC et les serveurs. Il existe également une catégorie très importante représentée par une icône en forme d'éclair. Cette catégorie correspond aux liaisons entre les équipements. Elle permet de choisir le type de câble utilisé pour connecter deux dispositifs.
5. Modes de fonctionnement (en bas à droite)
On a deux modes essentiels :
 - Real-Time : simulation instantanée
 - Simulation : visualisation pas à pas des paquets

2 Construire un premier LAN

2.1 Création d'un réseau

On va créer un premier réseau simple composé de 1 switch et 3 PC.

2.1.1 Ajouter un switch

Allez dans la catégorie Network Devices, cliquez sur Switches, sélectionnez le premier modèle disponible : 2960. Cliquez sur le modèle 2960, puis cliquez dans la zone de travail à l'endroit souhaité. Le switch apparaît alors dans la topologie.

2.1.2 Ajouter les PC

De la même manière, on va ajouter trois PC. Allez dans End Devices, cliquez sur la sous-catégorie End Devices, sélectionnez donc PC. On clique sur le PC, puis cliquez dans la zone de travail pour l'ajouter. Répétez l'opération jusqu'à obtenir 3 PC dans la topologie.

2.1.3 Relier les PC au switch

Maintenant, on va relier les PC au switch. Cliquez sur l'icône en forme d'éclair (Connections). On clique sur le troisième câble (ligne droite) : Copper Straight-Through. Ensuite, on clique sur le PC0, sélectionnez l'interface FastEthernet0, cliquez sur le switch, on sélectionne un port libre (par exemple FastEthernet0/1). La liaison apparaît alors entre le PC et le switch. Répétez pour les deux autres PC. PC1 - Switch (FastEthernet0/2); PC2 - Switch (FastEthernet0/3).

2.1.4 Configuration des adresses IP

Pour que les PC puissent communiquer, ils doivent être dans le même réseau IP. On utilise le réseau suivant : 192.168.1.0/24. Quel est le masque de sous-réseau correspondant ? Quelle est la première adresse IP utilisable ? Et la dernière adresse IP utilisable ? On utilise simplement les trois premières adresses disponibles pour nos trois PC. Double-cliquez sur le PC, allez dans l'onglet Config. Dans le menu à gauche, choisir FastEthernet0. On note d'abord l'adresse MAC du PC. Configurez donc l'adresse IP et le masque. Répétez la même procédure pour chaque PC.

2.1.5 Tester la connectivité

Une fois les adresses IP configurées, on doit vérifier les PC peuvent communiquer. On utilise la commande *ping*. Cliquez sur un PC0, allez dans l'onglet Desktop, cliquez sur Command Prompt. Tapez *ping @ip_PC1*. Est-ce que le ping fonctionne ? Pourquoi ?

2.1.6 Fonctionnement du switch : apprentissage automatique des adresses MAC

Le switch transfère des trames basé sur les adresses MAC. Il construit automatiquement une table MAC. Donc comment le switch apprend-il les adresses MAC ? On affiche la table MAC du switch. Double-cliquez sur Switch0, allez dans l'onglet CLI. Cette interface correspond au terminal de configuration du switch.

L'invite affiché est :

```
Switch>
```

On tape la commande *enable*, l'invite devient :

```
Switch#
```

Pour afficher la table MAC, on tape la commande *show mac-address-table*. Alors, combien d'adresses MAC sont présentes ? Ces adresses MAC appartiennent à quels équipements ? À quels ports sont associées les adresses ?

Depuis le PC0, on effectue un nouveau ping vers le PC2. Sur le switch, affichez la table MAC pour une nouvelle fois, de nouvelles adresses MAC sont-elles apparues ?

2.2 Extension du réseau

En fonction des besoins du réseau, un seul switch peut ne pas suffire pour assurer la communication entre tous les équipements. Il est alors nécessaire d'étendre le réseau.

2.2.1 Ajout d'un nouveau switch

On ajoute donc un deuxième switch (même modèle Cisco 2960). Il faut connecter le nouveau switch au switch existant. Sélectionnez Connections puis cliquez le câble Copper Cross-Over. On connecte le port GigabitEthernet0/1 du switch existant avec le port GigabitEthernet0/1 du nouveau switch. Cette configuration correspond également à une situation réelle. En général, le lien entre deux switches doit transporter le trafic de plusieurs équipements. Il est donc préférable d'utiliser des ports à haut débit (par exemple GigabitEthernet). Concernant l'utilisation du câble croisé, on parlera ce point en détail en M1. Mais si le sujet vous intéresse, vous pouvez chercher les notions de MDI et MDIX.

2.2.2 Ajout de PC sur le nouveau switch

Ajoutez trois nouveaux PC dans la topologie. On connecte PC3, PC4 et PC5 au port FastEthernet0/1, 0/2 et 0/3 du nouveau switch, respectivement.

2.2.3 Configuration des adresses IP

Configurez les adresses IP des trois nouveaux PC comme suit :

- PC3 : 192.168.1.100/24
- PC4 : 192.168.1.101/24
- PC5 : 192.168.1.102/24

N'oubliez pas à noter les adresses MAC. Ces PC appartiennent-ils au même réseau que les premiers ?

2.2.4 Apprentissage des adresses MAC inter-switch

Effectuez des tests de ping entre un PC du premier switch et un PC du second switch. Par exemple, sur PC0, on fait *ping 192.168.1.100*. Après les tests, affichez la table MAC sur les deux switches. Quelles nouvelles adresses MAC apparaissent ? Sur quel port sont-elles associées ? Les adresses MAC des PC distants apparaissent-elles ? À quel port sont-elles liées ?

2.3 Réflexion

- Lorsque le nombre d'hôtes dans le domaine de diffusion augmente, la taille de la table MAC du switch augmente-t-elle ?
- La table MAC contient-elle toutes les adresses MAC des hôtes ?
- Le switch apprend-il les adresses MAC des hôtes inactifs ?
- La taille de la table dépend-elle du nombre total d'hôtes ou du nombre d'hôtes actifs ?

3 Manipulation de base d'un commutateur

3.1 Connexion console au commutateur

Le switch peut être configuré via une interface en ligne de commande (CLI). Comme vous l'avez déjà essayé, dans Packet Tracer, il est possible de double-cliquer sur un équipement, puis de sélectionner l'onglet CLI afin d'accéder à l'interface de configuration.

En réalité, un switch ne dispose pas d'interface graphique. Pour accéder au CLI d'un nouveau switch réel, il est nécessaire de se connecter via le port console à partir d'un autre ordinateur.

On peut considérer que PC1 est la poste d'administration pour configurer Switch0. Donc il faut relier PC1 à Switch0 à l'aide d'un câble console.

On sélectionne Connexions, cliquez le câble Console (bleu clair). On connecte le port RS232 du PC au port Console du switch. Pour accéder à l'interface CLI, allez dans l'onglet Desktop, cliquez Terminal. On laisse les paramètres par défaut, et on clique sur OK.

Le CLI du switch apparaît à l'écran.

Il est important de noter que le PC utilisé pour configurer le switch n'a pas besoin d'être connecté au réseau du switch. La connexion console est une connexion directe, indépendante du réseau.

3.2 Divers modes CLI

3.2.1 Cisco IOS

Cisco IOS (Internetwork Operating System) est le système d'exploitation utilisé par les équipements Cisco (routeurs et switches). Lorsqu'on utilise la CLI pour configurer un équipement, on interagit en fait le système Cisco IOS.

3.2.2 Modes CLI

Le système Cisco IOS fonctionne avec 4 modes.

- **Mode utilisateur**
Invite : `Switch>`
Accès limité aux commandes de base.
- **Mode privilégié**
Invite : `Switch#`
Permet l'accès aux commandes avancées.

- **Mode de configuration globale**

Invite : `Switch(config)#`

Permet de modifier la configuration du switch.

- **Mode de configuration spécifique**

Invite : `Switch(config-if)#` Permet de configurer un élément précis (interface, ligne, VLAN, etc.).

3.2.3 Parcours de divers modes CLI

Maintenant, on va parcourir les divers modes CLI.

- **Étape 1 : en mode d'exécution utilisateur, tapez ?.** Prenez note de la liste de commandes disponibles.

Tant que vous êtes en mode d'exécution utilisateur, seules les commandes de surveillance de base sont disponibles.

- **Étape 2 : utilisation de la commande enable pour passer en mode d'exécution privilégié**

`Switch> enable`

`Switch#`

L'invite passe de `>` à `#`.

- **Étape 3 : en mode d'exécution privilégié, tapez ?**

Prenez note de la liste de commandes disponibles. Vous disposez de commandes supplémentaires par rapport au mode d'exécution utilisateur. Outre les commandes de surveillance de base, vous pouvez également accéder aux commandes de configuration et de gestion.

- **Étape 4 : passage au mode de configuration globale**

`Switch# configure terminal`

`Switch(config)#`

- **Étape 5 : en mode de configuration globale, tapez ?**

Prenez note de la liste de commandes disponibles.

- **Étape 6 : configuration du commutateur SW_Lab05 en tant que nom d'hôte**

`Switch(config)# hostname SW_Lab05`

`SW_Lab05(config)#`

- **Étape 7 : passage au mode de configuration d'interface pour VLAN1**

`SW_Lab05(config)# interface vlan 1`

`SW_Lab05(config-if)#`

Cette commande passe en mode de configuration d'interface pour VLAN1.

- **Étape 8 : configuration de VLAN1 avec 192.168.1.50/24 et activation de l'interface**

Utilisez les commandes `ip address` et `no shutdown` pour affecter l'adresse IP / le masque de sous-réseau approprié et pour activer l'interface.

```
SW_Lab05(config-if)# ip address 192.168.1.50 255.255.255.0
SW_Lab05(config-if)# no shutdown
```

- **Étape 9 : sortie du mode de configuration d'interface**

Exécutez la commande `exit` pour quitter le mode de configuration d'interface et passez en mode de configuration globale.

- **Étape 13 : passage au mode de configuration pour la ligne de console**

```
SW_Lab05(config)# line console 0
SW_Lab05(config-line)#
```

- **Étape 14 : retour au mode d'exécution privilégié à l'aide de la commande `end`**

```
SW_Lab05(config-line)# end
```

Voilà, maintenant vous êtes familiarisés avec les différents modes du Cisco IOS et ainsi qu'avec les transitions entre ces modes.

3.3 Visualisation de la configuration

Avec les manipulations de la section précédente, on a vu qu'il est possible de configurer les équipements via l'interface en ligne de commande. Dans cette section, on va voir comment visualiser la configuration, c'est-à-dire comment vérifier si celle-ci a été correctement réalisée.

Pour afficher la configuration et les informations des interfaces, on utilise la commande `show`. Cette commande s'exécute en mode privilégié. Il nous faut l'inviter comme suit :

```
SW\_Lab05#
```

3.3.1 Configuration globale du switch

La commande la plus courante, et aussi la plus importante, est celle qui permet d'afficher la configuration actuelle du switch. Examinez la configuration en cours d'exécution en exécutant la commande `show running-config`. Combien d'interfaces FastEthernet le commutateur possède-t-il ? Et combien d'interfaces GigabitEthernet ? Quelle est la plage de valeurs affichée pour les lignes vty ?

3.3.2 Configuration/Informations des interfaces

Examinez les propriétés par défaut de l'interface FastEthernet utilisée par PC1 à l'aide de la commande `show interface FastEthernet0/2`. L'interface est-elle activée ou désactivée ? Quelles sont les informations qu'on trouve dans `show interface` ?

3.3.3 Configuration/Informations du VLAN

Examinez les paramètres du réseau local virtuel par défaut pour le commutateur à l'aide de la commande `show vlan`. Quel est le nom de VLAN1 ? Quels ports se trouvent dans ce VLAN ? Le VLAN1 est-il actif ?

Examinez les caractéristiques de l'interface virtuelle VLAN1 en exécutant la commande `show interface vlan1`.

3.4 Configuration de base du commutateur

3.4.1 Définition des mots de passe

Tout d'abord, on veut pas que n'importe qui puisse brancher un câble console sur le switch et commencer à taper des commandes de configuration. On souhaite donc configurer un mot de passe afin de protéger l'accès au switch. Passez en mode de configuration de ligne pour la console. Définissez le mot de passe de connexion sur la valeur **cisco**.

```
SW_Lab05# configure terminal
SW_Lab05(config)# line console 0
SW_Lab05(config-line)# password cisco
SW_Lab05(config-line)# login
SW_Lab05(config-line)# exit
```

La commande password permet de définir le mot de passe. La commande login permet d'activer la vérification du mot de passe lors de la connexion. De la même manière, configurez également les lignes vty 0 à 15 en utilisant le mot de passe **cisco**.

```
SW_Lab05# configure terminal
SW_Lab05(config)# line vty 0 15
SW_Lab05(config-line)# password cisco
SW_Lab05(config-line)# login
SW_Lab05(config-line)# exit
```

Pourquoi on utilise les lignes VTY ? Les lignes VTY permettent d'accéder au switch à distance via Telnet/SSH. On distingue donc Console - accès local (câble console); VTY - accès distant via le réseau. Un ingénieur réseau ne peut pas se déplacer sur site à chaque fois pour configurer un équipement. Les lignes VTY permettent justement de rendre possible la configuration à distance, sans intervention physique sur l'équipement.

On a déjà configuré une adresse IP sur VLAN1 (192.168.1.50/24). Cette adresse IP sert d'adresse de gestion du switch. (**Mais attention : Ce n'est pas une fonction de routage. C'est uniquement pour l'administration. Un switch classique est un équipement de couche 2 - liaison de données.**)

Sur n'importe quel PC du même réseau, allez dans l'onglet Desktop - Command Prompt, on tape telnet 192.168.1.50.

Si :

- l'adresse IP du PC est bien configurée
- les lignes VTY sont configurées avec password et login
- l'interface VLAN est activé

alors l'accès au switch à distance fonctionne.

Tout à l'heure, on a configuré un mot de passe d'accès (console / VTY). Ainsi, toute personne qui accède à l'interface CLI doit s'authentifier. Cependant, cela ne suffit pas. Même après s'être connecté, un utilisateur peut taper la commande enable pour passer en mode privilégié, qui permet de modifier la configuration du switch. Il est donc également nécessaire de protéger cette commande. Pour cela, on configure un mot de passe avec :

```
SW_Lab05(config)# enable secret lsin606
```

Bon, l'accès au mode privilégié est aussi sécurisé.

3.4.2 Activation du chiffrement des mots de passe

On affiche la configuration actuelle du switch. Peut-on retrouver les mots de passe d'accès et enable ? Par défaut, certains mots de passe (password) configurés sur le switch peuvent apparaître en clair dans la configuration. Cela pose un problème de sécurité. On a aussi une solution : activer le chiffrement.

```
SW_Lab05(config)# service password-encryption
```

Cette commande permet de chiffrer les mots de passe configurés avec *password*.

3.5 Résumé

Lorsqu'on met en service un switch, certaines opérations sont essentielles.

- **Changez le nom du switch**
Permet d'identifier clairement l'équipement dans le réseau.
- **Protéger l'accès console**
Empêcher un accès physique non autorisé.
- **Protéger l'accès distant (VTY)**
Permet la gestion à distance (Telnet ou SSH).
- **Protéger le mode privilégié**
Sécuriser la commande enable.
- **Chiffre les mots de passe**
Éviter qu'ils apparaissent en clair dans la configuration.
- **Configurer une adresse IP de gestion**
Donner une adresse au switch (via une interface VLAN). Il n'est pas obligatoire d'utiliser le VLAN 1, et il est même recommandé d'utiliser un autre VLAN pour la gestion.

Après avoir réalisé les différentes étapes de configuration, il est important de vérifier et sauvegarder la configuration. Pour vérifier la commande, on sait déjà, on utilise donc **show running-config**. Mais le running-config est stockée en mémoire. C'est-à-dire que en cas de redémarrage ou de coupure de courant, toute la configuration dans la running-config est perdue.

Lorsque le switch redémarre, il ne recharge pas la running-config. Il charge la configuration enregistrée, appelée : startup-config. Pour éviter toute perte de configuration, il est donc indispensable d'enregistrer les modifications avec :

```
SW_Lab05# copy running-config startup-config
```

Bien sûr, on peut vérifier le contenu de la configuration sauvegardée en utilisant la commande **show startup-config**.