TP3 - Introduction à l'*IOS*

M. Tellene

I/ Rendu

Le TP comporte des questions. Les réponses devront être rendues dans un fichier pdf sur moodle à la fin de la séance. Vous devrez joindre, aux moments indiqués, des captures d'écrans.

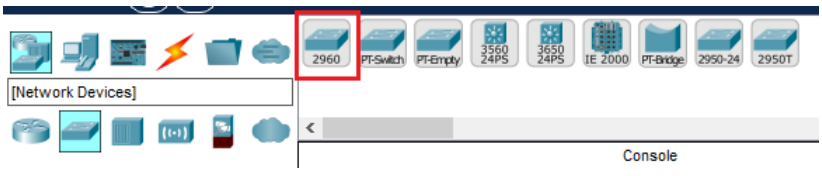
Il vous est fortement conseillé de sauvegarder les commandes entrées dans un fichier texte.

II/ Partie 1 : Configurer un périphérique réseau de base

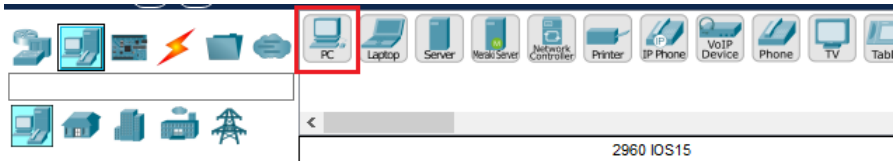
II/1 Topologie

II/2 Câblage du réseau

1. Si ce n'est pas déjà fait, démarrer *Packet Tracer*
2. Commencer par poser le commutateur. Celui utilisé dans le TP est un *Cisco* 2960, il se trouve ici :



   Une fois le commutateur déposé, changer son nom en « S1 ». Pour ce faire, il vous suffit de cliquer sur le nom de l'équipement et d'appuyer sur *Entrée* une fois le nom mis.
3. Poser maintenant un ordinateur, il se trouve ici :



Une fois l'ordinateur déposé, changer son nom en « PC1 ».

4. Raccorder maintenant les deux appareils avec un câble console. Ce câble permet de configurer le matériel *Cisco* à partir de l'ordinateur auquel il est relié. Vous utiliserez ces câbles quand vous devrez configurer les équipements *Cisco*. Ce câble se trouve ici :

En cliquant sur l'icône, le pointeur de la souris se transforme en un connecteur avec un câble pendant dessus.

5. Cliquer sur PC1. Une fenêtre s'affiche, sélectionner l'option « RS-232 »
6. Faire glisser l'autre extrémité de la connexion console vers le commutateur S1, puis cliquer sur le commutateur afin de faire apparaître la liste des ports. Sélectionner le port « Console » afin d'établir la connexion

L'ordinateur et le commutateur sont à présent liés entre eux avec un câble console.

II/3 Établir une session de terminal avec S1

1. Cliquer sur PC1, une fenêtre s'ouvre, sélectionner l'onglet *Desktop*
2. Plusieurs icônes s'affichent à l'écran, cliquer sur celle correspond au *Terminal*
3. **Question :** Quelle est la valeur du paramètre des bits par seconde ?
4. Cliquer sur *Ok*, un terminal devrait s'ouvrir
5. Le message `Press RETURN to get started.` devrait apparaître à l'écran, appuyer sur la touche *Entrée*
6. **Question :** Quelle est l'invite affichée à l'écran ? Indiquer quel est le mode actuel et pourquoi c'est celui-ci.

II/4 L'aide *IOS*

L'*IOS* peut fournir de l'aide sur les commandes en fonction du niveau auquel l'utilisateur accède.

1. **Question :** Que se passe-t-il si l'on tape un commande `?` ? Indiquer les commandes affichées et expliquer l'utilité de la commande `?`.
2. **Question :** Même question, mais avec la commande `t?` ? Indiquer les commandes affichées et expliquer l'utilité de la commande `t?`.

II/5 Les différents mode d'exécution

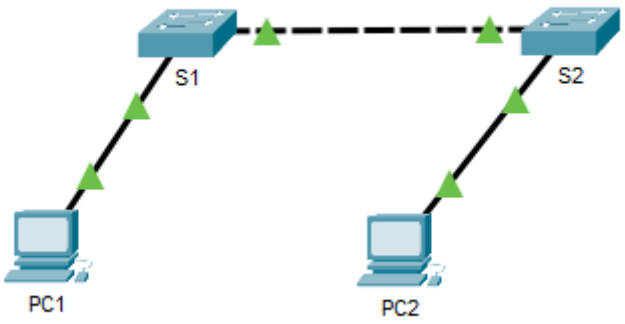
1. Passer en mode d'exécution privilégié
2. **Question :** Quelle commande avez-vous tapé pour arriver dans ce mode d'exécution ? Indiquer quelle est l'invite de commande maintenant.
3. **Question :** Taper la commande `?`. Indiquer les commandes affichées, s'il y en a plus ou moins qu'avec le mode précédent et si cela est logique.

4. En mode d'exécution privilégié, l'une des commandes est `configure`. Entrer cette commande, puis appuyer sur *Entrée*
5. **Question :** Quel est le message affiché à l'écran ? Qu'est-ce que cela implique ?
6. Appuyer sur la touche *Entrée* pour accepter le paramètre par défaut entre crochets : `[terminal]`.
7. **Question :** Quel changement observez-vous sur l'invite ?

   Vous venez d'entrer dans le mode de configuration globale. Ce mode sera examiné en détail plus tard.
8. Revenir en mode d'exécution privilégié
9. **Question :** Quelle commande avez-vous tapé ?

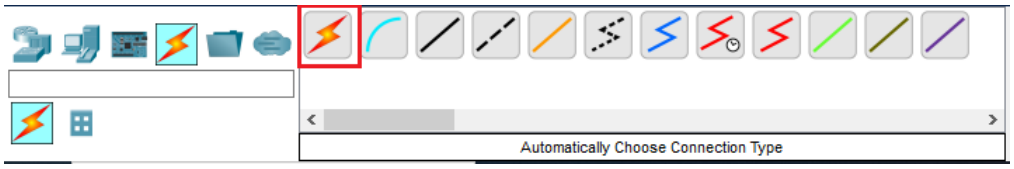
III/ Partie 2 : Mise en oeuvre de la connectivité de base

III/1 Topologie



III/2 Câblage du réseau

Reproduire le câblage de réseau. Afin de faire le câblage, nous utiliserons pour l'instant la manière automatique. Au fur et à mesure de l'année, vous devrez utiliser les bons câbles en fonction des appareils. Le câblage automatique se trouve ici :



TODO Une fois fait, mettre une capture d'écran de votre réseau

III/3 Effectuer la configuration de base des commutateurs `S1` et `S2`

L'accès et la configuration des commutateurs **devra** se faire via le port console depuis les ordinateurs.

III/3.a Configurer `S1` avec un nom d'hôte

Lors de la configuration d'un périphérique réseau, l'une des premières étapes est la configuration d'un nom d'hôte. Ces noms apparaissent dans les invites de commande. Ils ont un rôle important dans la sécurité des réseaux et dans la construction de schémas techniques.

On définit habituellement une convention de nom pour chaque appareil afin d'assurer l'homogénéité du parc (nom en fonction de la position géographique par exemple). Ainsi un commutateur gérant la téléphonie et se trouvant au 1^{er} étage du bâtiment A de l'entreprise pourrait s'appeler `Switch-Phone-BatA-Etage1`.

Voici les règles à respecter pour nommer correctement un périphérique. Le nom :

— commence par une lettre
— ne contient pas d'espace
— se termine par une lettre ou un chiffre
— comporte uniquement des lettres, des chiffres et des tirets
— comporte moins de 64 caractères

Pour configurer un nom d'hôte :

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. Terminez par CNTL/Z.

Switch(config)#hostname Sw-Floor-1
Sw-Floor-1(config)#
```

Pour supprimer le nom attribué à un périphérique :

```
Sw-Floor-1(config)#no hostname
Switch(config)#
```

1. En lançant l'application *Terminal* de `PC1`, configurer le nom d'hôte du commutateur en tant que `S1`
2. **Question :** Quelles commandes avez-vous tapées? Après validation des commandes, l'invite de commande a-t-elle changé? Si oui, comment?

III/3.b Sécurisation des accès au périphérique

Il est recommandé de limiter physiquement l'accès aux périphériques réseaux en les plaçant dans des pièces et des armoires fermées à clé. Toutefois, les mots de passe sont la principale défense contre l'accès non autorisé à ces périphériques.

IOS utilise des modes organisés hiérarchiquement pour faciliter la protection des périphériques. Dans le cadre de ce dispositif de sécurité, *IOS* peut accepter plusieurs mots de passe, ce qui permet d'établir différents privilèges. Il est recommandé d'utiliser des mots de passe différents pour chacun des niveaux d'accès.

Caractéristiques des mots de passe présentés ici :

— sécurisation de l'accès au mode d'exécution utilisateur : mot de passe console - limite l'accès par une connexion console
— sécurisation de l'accès en mode d'exécution privilégié : mot de passe chiffré
— sécurisation de l'accès Telnet : mot de passe `VTY`

Sécurisation de l'accès au mode d'exécution utilisateur

Vous devez sécuriser le port de console des périphériques réseaux. Cela réduit les chances qu'un personnel non autorisé branche physiquement un câble sur le port console de l'appareil pour y accéder.

```
Switch>enable
Switch#configure terminal
Switch(config)#line console 0
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config-line)#end
Switch#exit

Switch con0 is now available
Press RETURN to get started.

User Access Verification
Password:
```

La commande `login` permet d'exiger une authentification à l'ouverture de la session.

Sécurisation de l'accès au mode d'exécution privilégié

Pour sécuriser l'accès au mode privilégié, il faut utiliser la commande `enable secret`. Cette commande offre davantage de sécurité puisque le mot de passe est chiffré.

```
Switch>enable
Switch#configure terminal
Switch(config)#enable secret salut
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#disable
Switch>enable
Password:
Switch#
```

Sécurisation de l'accès Telnet

Les lignes VTY permettent d'accéder à un équipement *Cisco* via Telnet. Par défaut, de nombreux commutateurs *Cisco* prennent en charge jusqu'à 16 lignes VTY, numérotées de 0 à 15 (cela peut varier). En général, 5 lignes VTY sont configurées. Par défaut, ces lignes sont numérotées de 0 à 4.

```
Switch>enable
Switch#configure terminal
Switch(config)#line vty 0 15
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config-line)#
```

Chiffrement de l'affichage des mots de passe

Bien que les mots de passe soient configurés, ces derniers sont accessibles en clair dans les fichiers de configuration du dispositif (sauf le mot de passe d'accès privilégié) :

```
Switch>enable
Switch#show running-config
...
line con 0
 password cisco
 login
!
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
```

Il faut donc activer les services de chiffrements des mots de passe. Ces services empêchent que les mots de passe soient indiqués en clair dans les informations de configuration.

L'annulation du service de chiffrement ne supprime pas ce chiffrement.

```
Switch#configure terminal
Switch(config)#service password-encryption
Switch(config)#exit

Switch#show running-config
...
line con 0
 password 7 0822455D0A16
 login
```

Revenons-en au TP.

1. Attribuer `cisco` comme mot de passe de console, puis activer la connexion
2. **Question :** Quelles commandes avez-vous tapées ? Parmi ces commandes, laquelle permet d'activer la connexion ?
3. **Question :** Comment pourrait-on vérifier que le mot de passe est bien mis ?
4. Utiliser `class` comme mot de passe pour le mode d'exécution privilégié chiffré
5. **Question :** Quelles commandes avez-vous tapées ?
6. **Question :** Comment pourrait-on vérifier que le mot de passe est bien mis ?
7. Utiliser `passtelnet` comme mot de passe pour l'accès Telnet
8. **Question :** Quelles commandes avez-vous tapées ?
9. **Question :** Comment pourrait-on vérifier que le mot de passe est bien mis ?
10. **Question :** Montrer que les mots de passe mis sont écrits en clair dans les fichiers de configurations
11. Régler ce problème
12. **Question :** Quelles commandes avez-vous tapées ?

III/3.c Configurer une bannière `MOTD`

Les bannières peuvent constituer une pièce importante en cas de poursuite contre une personne ayant accédé sans autorisation à un périphérique. En effet, dans certains systèmes juridiques, il n'est pas possible de poursuivre des utilisateurs ni même de les surveiller, sauf s'ils ont reçu une notification appropriée. Voici quelques exemples d'informations à inclure dans la bannière :

— « L'utilisation du périphérique est strictement réservée au personnel autorisé »
— « Vos interactions avec le périphérique peuvent faire l'objet d'une surveillance »
— « Toute utilisation non autorisée fera l'objet de poursuite judiciaire »

IOS fournit plusieurs types de bannières. L'un des plus communs est le message du jour (`MOTD`). Pour configurer le `MOTD`, on utilise la commande `banner motd` dans le mode de configuration globale.

```
Switch>enable
Switch#configure terminal
Switch(config)#banner motd "L'utilisation de cet appareil est reservee"
Switch(config)#exit
Switch#exit

Switch con0 is now available
Press RETURN to get started.
L'utilisation de cet appareil est reservee
Switch>
```

L'objectif ici est de configurer une bannière `MOTD` pour afficher un avertissement d'accès non autorisé. Voici un exemple de texte : « Accès autorisé uniquement. Tout contrevenant sera poursuivi conformément à la loi. »

1. Fixer le message exemple en tant que bannière `MOTD`. Attention, les accents ne sont pas pris en compte
2. **Question :** Quelles commandes avez-vous tapées ?
3. **Question :** Comment pourrait-on vérifier que la bannière est bien mise ?

III/3.d Enregistrer le fichier de configuration dans la mémoire `NVRAM`

Le fichier de configuration en cours reflète la configuration actuelle appliquée à un périphérique *Cisco IOS*. Il contient les commandes utilisées pour déterminer comment le périphérique fonctionne sur le réseau. Modifier une configuration en cours affecte immédiatement le fonctionnement d'un périphérique *Cisco*.

En cas de panne de courant ou de redémarrage, toutes les modifications de la configuration qui n'ont pas été enregistrées seront perdues. Après avoir apporté des modifications à un fichier de configuration en cours, 3 possibilités s'offrent à nous :

— adopter la configuration modifiée comme configuration initiale : `copy running-config startup-config`

— restaurer la configuration initiale : `reload` (en mode d'exécution privilégié)

— supprimer toutes les configuration : `erase startup-config`

Pour cette dernière option, il est à noter que sur les commutateurs, il faudra également entrer la commande `delete vlan.dat`.

Exemple de restauration de la configuration intiale

```
S1(config)#enable secret cisco
S1(config)#exit

S1#disable
S1>enable
Password:
S1#reload
System configuration has been modified. Save? [yes/no]:n
Proceed with reload? [confirm]
...
Press RETURN to get started!

Switch>enable
Switch#
```

Exemple de changement de configuration initiale

```
S1(config)#enable secret cisco
S1(config)#exit

S1#disable
S1>enable
Password:
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#reload
Proceed with reload? [confirm]
...
Press RETURN to get started!
S1>enable
Password:
S1#
```

1. Passer en mode d'exécution privilégié
2. Utiliser la commande appropriée pour copier la configuration actuelle dans la configuration de démarrage
3. **Question :** Quelle commande avez-vous tapée ? D'autres validation ont été nécessaires afin de réaliser cette copie ? Si oui, lesquelles.

III/4 Configuration de S2

Appliquer le paramétrage de S1 à S2. Il est rappelé que vous devez utiliser un ordinateur pour effectuer la configuration de S2.

III/5 Configurer les ordinateurs

III/5.a Configurer les deux ordinateurs avec des adresses IP

1. Configurer l'adresse IP de PC1 et PC2. Vous utiliserez `192.168.1.1/24` pour PC1 et `192.168.1.2/24` pour PC2
2. **Question :** Justifier les changements faits avec le résultat de la commande `ipconfig`
3. **Question :** PC1 et PC2 font-ils partis du même réseau ? Justifier.
4. Depuis le PC1, faire un ping à PC2
5. **Question :** Le ping a-t-il abouti ? Est-ce normal ?
6. Depuis le PC2, faire un ping à PC1
7. **Question :** Le ping a-t-il abouti ? Est-ce normal ?