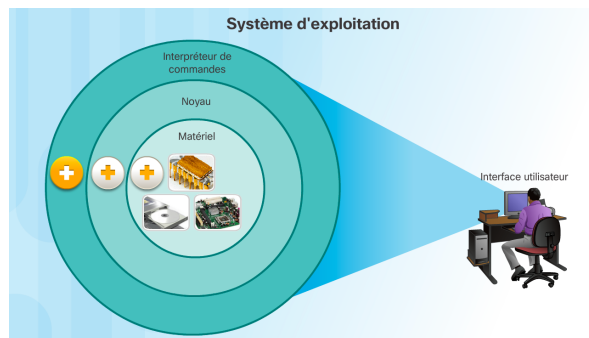


SOMMAIRE

1 Formation intensive à IOS .	2
1.1 Système d'exploitation	2
1.2 Utilité d'un système d'exploitation.	3
1.3 Méthode d'accès	3
1.4 Programme d'émulation de terminal	4
1.5 Connexion au commutateur pour la première fois	5
2 Naviguer dans Cisco IOS	5
2.1 Mode de fonctionnement de Cisco IOS.	5
2.2 Structure des commandes IOS de base.	6
2.3 Syntaxe des commandes IOS	6
2.4 Touche d'accès rapide et raccourcis	7
3 Configuration des périphériques de base	7
3.1 Nom de périphérique	7
3.2 Configurer les noms d'hôte	8
3.3 Configurer les mots de passe	8
3.4 Messages de bannière	9
3.5 Enregistrer le fichier de configuration en cours	10
3.6 Modifier la configuration en cours	11

1. Formation intensive à IOS :

1.1 Système d'exploitation :



Tous les périphériques finaux et réseau requièrent un système d'exploitation (SE). Comme le montre ci-dessus, la partie du SE directement liée au matériel informatique s'appelle le *noyau*. La partie liée aux applications et à l'utilisateur s'appelle l'*interpréteur de commandes*.

L'utilisateur accède à l'interpréteur de commandes à l'aide d'une interface en ligne de commande (CLI) ou d'une interface utilisateur graphique.

Lorsqu'il utilise une interface en ligne de commande, l'utilisateur accède directement au système dans un environnement textuel, en entrant des commandes au clavier dans une invite de commandes. En règle générale, le système exécute la commande en fournissant une sortie textuelle. La CLI nécessite très peu de surcharge pour fonctionner. Cependant, l'utilisateur doit connaître la structure sous-jacente qui contrôle le système.

Une interface utilisateur graphique telle que Windows, OS X, Apple iOS ou Android, permet à l'utilisateur d'interagir avec le système à l'aide d'un environnement utilisant des graphiques, des icônes, des menus et des fenêtres.

L'interface utilisateur graphique est plus conviviale et ne nécessite pas de connaissances approfondies de la structure de commande sous-jacente qui contrôle le système. C'est pour cette raison que de nombreux utilisateurs préfèrent les environnements basés sur une interface utilisateur graphique.

Cependant, les interfaces utilisateur graphiques ne disposent pas toujours de toutes les fonctionnalités disponibles dans la CLI. Elles peuvent également tomber en panne ou simplement ne pas fonctionner correctement. C'est pourquoi l'accès aux périphériques réseau se fait habituellement via une CLI. La CLI demande moins de ressources et offre une grande stabilité par rapport à une interface utilisateur graphique.

Le système d'exploitation réseau utilisé sur les périphériques Cisco est appelé système d'exploitation interréseau Cisco. Cisco IOS est utilisé par la plupart des périphériques Cisco, quels que soient leur taille et leur type.

Remarque : le système d'exploitation des routeurs domestiques est généralement appelé « firmware ». La méthode la plus courante pour configurer un routeur domestique est d'utiliser une interface utilisateur graphique basée sur navigateur web.

1.2 Utilité d'un système d'exploitation :

Les systèmes d'exploitation réseau sont similaires au système d'exploitation d'un ordinateur. Grâce à une interface utilisateur graphique, le système d'exploitation d'un ordinateur permet à l'utilisateur :

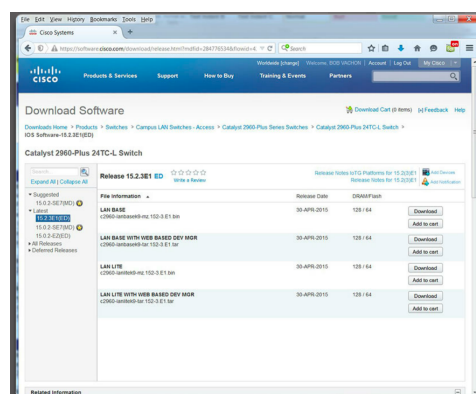
- d'utiliser une souris pour faire des sélections et exécuter des programmes.
- d'entrer des commandes textuelles.
- d'afficher des images sur un écran.

Un système d'exploitation réseau utilisant une CLI, comme Cisco IOS, installé sur un commutateur ou un routeur permet à un technicien réseau :

- d'utiliser un clavier pour exécuter des programmes réseau basés sur CLI.
- d'utiliser un clavier pour entrer des commandes textuelles.
- d'afficher des images sur un écran.

Les périphériques réseau exécutent des versions spécifiques de Cisco IOS. La version de l'IOS dépend du type de périphérique utilisé et des fonctions nécessaires. Alors que tous les périphériques possèdent un IOS et un ensemble de fonctionnalités par défaut, il est possible de mettre à niveau l'IOS ou l'ensemble de fonctionnalités, afin d'obtenir des fonctions supplémentaires.

Dans ce cours, vous vous concentrerez principalement sur Cisco IOS version 15.x. La figure répertorie les versions logicielles d'IOS disponibles pour un commutateur Cisco Catalyst 2960.



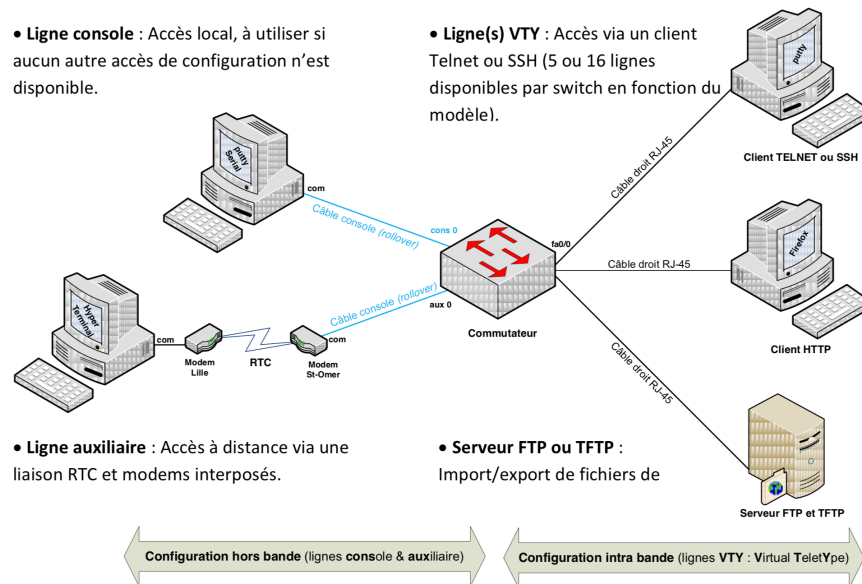
1.3 Méthode d'accès :

Un commutateur Cisco IOS peut être implémenté sans être configuré. Il effectuera tout de même la commutation des données entre les périphériques connectés. Deux PC reliés à un commutateur disposeront immédiatement d'une interconnectivité instantanée.

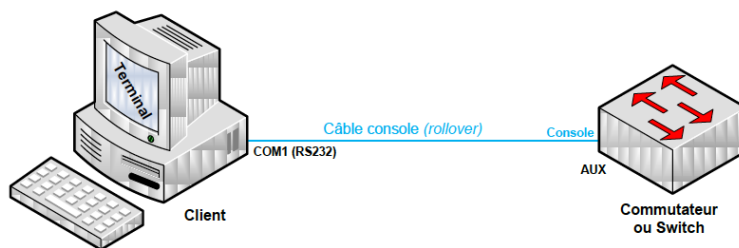
Même si un commutateur Cisco fonctionne toujours immédiatement, il est recommandé de configurer les paramètres initiaux. Il existe plusieurs moyens d'accéder à l'environnement CLI et de configurer le périphérique. Voici les méthodes les plus répandues :

- Console : il s'agit d'un port de gestion permettant un accès hors réseau à un périphérique Cisco. L'accès hors bande désigne l'accès via un canal de gestion dédié qui est utilisé uniquement pour la maintenance des périphériques.

- Secure Shell (SSH) : moyen d'établir à distance une connexion CLI sécurisée via une interface virtuelle sur un réseau. À la différence des connexions de console, les connexions SSH requièrent des services réseau actifs sur le périphérique, notamment une interface active possédant une adresse.
- Telnet : moyen non sécurisé d'établir une session CLI à distance via une interface virtuelle sur un réseau. Contrairement aux connexions SSH, Telnet ne fournit pas de connexion chiffrée de manière sécurisée. L'authentification des utilisateurs, les mots de passe et les commandes sont envoyés en clair sur le réseau.



1.4 Programme d'émulation de terminal :



Sur Ubuntu, on utilisera le terminal.

1. Brancher le port console sur le port USB d'un PC.
2. Rechercher le nom du port en tapant : `sudo dmesg | grep tty`

Vous pouvez par exemple relever `ttyACM0` ou `ttyUSB0`.

3. Saisir ensuite la commande : `sudo screen /dev/ttyACM0 9600` et taper sur entrée

screen est un émulateur de terminal qui peut ouvrir une session série (RS-232/USB-série). C'est l'équivalent de PuTTY ou Tera Term sous Windows, mais en ligne de commande Linux.

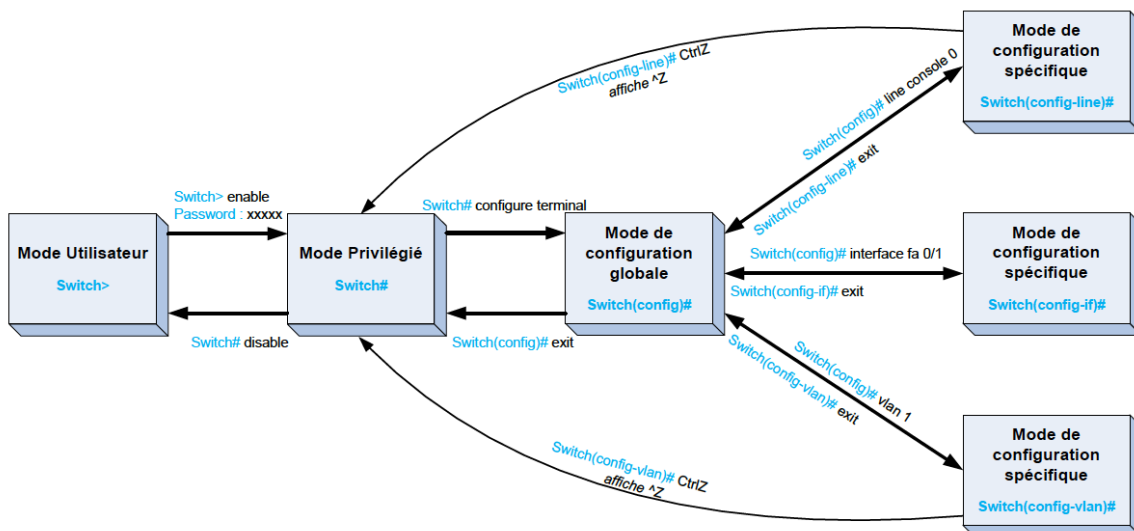
```
user@ubuntu$ sudo dmesg | grep tty
password for user
[ 1748.034719] cdc_acm 3-2.3:1: ttyACM0: USB ACM device
user@ubuntu$
sudo screen screen /dev/ttyACM0 9600
```

2. Naviguer dans Cisco IOS:

2.1 Mode de fonctionnement de Cisco IOS :

Une fois connecté depuis putty, le technicien réseau doit naviguer à travers différents modes de commande dans la CLI de Cisco IOS. Les modes de Cisco IOS utilisent une structure hiérarchique et sont assez similaires sur les commutateurs et les routeurs.

Une fois le commutateur démarré, la console de commande en ligne vous propose une invite ">" signifiant que vous êtes dans le mode utilisateur.



Router > enable (en) :

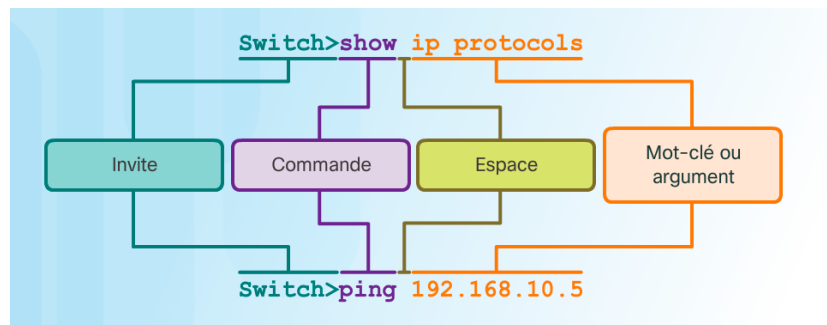
Pour entrer dans le mode commande privilégié permettant la gestion (statistique, debugage,...) du fonctionnement du commutateur. La validation de cette commande entraîne souvent la demande d'un mot de passe. Par la suite pour revenir à ce niveau du mode commande, il suffira de taper « CTRL+Z ».

Router # configure terminal (conf t) :

Pour entrer dans le mode de configuration globale. Ce mode est utilisé sur un commutateur pour appliquer des instructions de configuration qui affectent l'ensemble du système.

A partir du mode ci-dessus, vous pouvez passer dans les modes spécifiques, l'invite du commutateur se transforme et toute modification de la configuration s'appliquera alors uniquement aux interfaces ou aux processus couverts par le mode particulier.

2.2 Structure des commandes IOS de base:



Un périphérique Cisco IOS prend en charge de nombreuses commandes. Chaque commande IOS a un format ou une syntaxe spécifique et ne peut être exécutée que dans le mode approprié. En général, vous entrez une commande en tapant un nom de commande suivi des mots-clés et des arguments appropriés.

- **Mot-clé** : il s'agit d'un paramètre spécifique défini dans le système d'exploitation (dans la figure, **protocoles IP**)
- **Argument** : non prédéfini ; il s'agit d'une valeur ou d'une variable définie par l'utilisateur (dans la figure, **192.168.10.5**)

2.3 Syntaxe des commandes IOS :

Pour décrire l'utilisation des commandes, nous employons généralement ces conventions.	
Convention	Description
gras	Le texte en gras signale les commandes et mots-clés à saisir tels quels.
<i>Italique</i>	Le texte en italique signale les arguments pour lesquels des valeurs doivent être saisies.
[x]	Les crochets signalent un élément facultatif (mot-clé ou argument).
{x}	Les accolades signalent un élément requis (mot-clé ou argument).
[x {y z}]	Les accolades et les lignes verticales encadrées par des crochets signalent un choix obligatoire, au sein d'un élément facultatif.

Une commande peut exiger un ou plusieurs arguments. Pour connaître les mots-clés et arguments requis pour une commande, consultez la section sur la syntaxe des commandes. La syntaxe indique le modèle ou le format devant être utilisé lorsque vous saisissez une commande.

Comme indiqué dans le tableau précédent, le texte en gras indique des commandes et des mots clés que l'utilisateur entre tels quels. Le texte en italique signale un argument dont l'utilisateur fournit la valeur.

Les exemples suivants illustrent les conventions utilisées pour documenter et utiliser les commandes IOS.

- **ping** *adresse-ip* : la commande est **ping** et l'argument défini par l'utilisateur est l'*adresse IP* du périphérique de destination. Par exemple, **ping 10.10.10.5**.
- **traceroute** *adresse-ip* : la commande est **traceroute** et l'argument défini par l'utilisateur est l'*adresse IP* du périphérique de destination. Par exemple, **traceroute 192.168.254.254**.

La référence des commandes Cisco IOS est la meilleure source d'informations pour une commande IOS spécifique.

2.4 Touches d'accès rapide et raccourcis :

Dans l'interface CLI de Cisco IOS, des touches d'accès rapide et des raccourcis facilitent la configuration, la surveillance et le dépannage, comme illustré dans le tableau suivant : Il est possible de raccourcir les commandes et les mots-clés jusqu'au nombre minimal de caractères qui identifient une sélection unique. Par exemple, vous pouvez raccourcir la commande **configure** en entrant **conf** parce que **configure** est la seule commande qui commence par **conf**. Par contre, la version raccourcie **con** ne fonctionne pas parce que plusieurs commandes débutent par **con**. Vous pouvez aussi raccourcir les mots clés.

(REMARQUE : la touche « Suppr », qui efface le caractère à droite du curseur, n'est pas reconnue par les programmes d'émulation de terminal.)

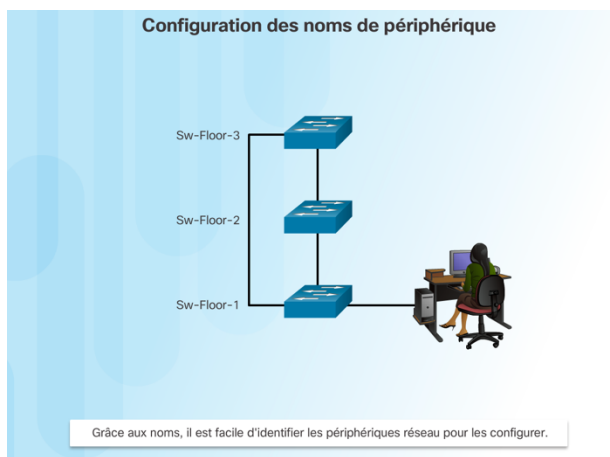
En cas d'invite « -----More----- »	
Touche Entrée	Affiche la ligne suivante.
Barre d'espace	Affiche l'écran suivant.
Autres touches	Termine la chaîne d'affichage et revient au mode d'exécution privilégié.

Touches de pause	
Ctrl+C	Dans un mode de configuration, permet de quitter le mode de configuration et de retourner au mode d'exécution privilégié. à partir du mode d'exécution, l'invite reparait.
Ctrl+Z	Dans un mode de configuration, permet de quitter le mode de configuration et de retourner au mode d'exécution privilégié.
Ctrl+Maj+6	Séquence d'interruption permettant d'abandonner les recherches DNS et les commandes <code>traceroute</code> et <code>ping</code> .

REMARQUE : combinaisons avec **Ctrl** - En maintenant enfoncée la touche , appuyez sur la touche de la lettre indiquée. Séquences d'**échappement** - Appuyez sur la touche puis relâchez-la, avant d'appuyer sur la touche de la lettre indiquée.

3. Configuration des périphériques de base :

3.1 Nom de périphérique :



Les noms d'hôte :

- débutent par une lettre.
- ne contiennent pas d'espaces.
- se terminent par une lettre ou un chiffre.
- ne comportent que des lettres, des chiffres et des tirets.
- comportent moins de 64 caractères.

Lors de la configuration d'un périphérique réseau, l'une des premières étapes est la configuration d'un nom de périphérique ou d'hôte unique. Les noms d'hôte qui apparaissent dans les invites de la CLI peuvent être utilisés dans différents processus d'authentification entre les périphériques et doivent être utilisés dans les bases de données topologiques.

Si le nom du périphérique n'est pas explicitement configuré, un nom par défaut est utilisé par Cisco IOS. Le nom par défaut d'un commutateur Cisco IOS est « Switch » (Commutateur). Si tous les périphériques réseau ont conservé leurs noms par défaut, il sera difficile d'identifier un périphérique spécifique. Par exemple, en accédant à un périphérique distant avec une

connexion SSH, il est important de vous assurer que vous êtes connecté au périphérique approprié.

En revanche, si vous les choisissez intelligemment, vous n'aurez aucune peine à mémoriser, décrire et utiliser les noms des périphériques réseau. Les directives pour la configuration des noms d'hôte sont répertoriées précédemment.

IOS distingue les majuscules des minuscules dans les noms d'hôte utilisés pour les périphériques. Vous pouvez donc utiliser des majuscules comme vous le feriez normalement pour un nom. Contrairement à IOS, la plupart des systèmes d'attribution de noms Internet ne font aucune distinction entre majuscules et minuscules.

Par exemple, trois commutateurs couvrant trois étages différents sont interconnectés sur un réseau. La convention d'attribution de noms utilisée a pris en compte l'emplacement et le rôle que joue chaque périphérique. La documentation réseau doit expliquer comment ces noms ont été choisis afin que des périphériques supplémentaires puissent être nommés en conséquence.

3.2 Configurer les noms d'hôtes :

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

Une fois la convention d'attribution de noms établie, l'étape suivante consiste à associer ces noms aux périphériques à l'aide de la CLI.

Depuis le mode d'exécution privilégié, accédez au mode de configuration globale en entrant la commande **configure terminal**. Remarquez le changement dans l'invite de commandes.

Depuis le mode de configuration globale, entrez la commande **hostname** suivie du nom du commutateur, puis appuyez sur Entrée. Remarquez le changement dans le nom de l'invite de commandes.

Remarque : pour supprimer le nom d'hôte configuré et renvoyer le commutateur à l'invite par défaut, utilisez la commande de config. globale **no hostname**.

3.3 Configurer les mots de passe :

Des mots de passe sont nécessaires pour les accès suivant :

- Sécuriser l'accès au mode d'exécution privilégié.
- Sécuriser l'accès au mode d'exécution utilisateur avec un mot de passe
- Sécuriser l'accès au mode Telnet à distance avec un mot de passe

Il est également nécessaire de chiffrer tous les mots de passe

Le mot de passe le plus important à configurer est celui permettant d'accéder au mode d'exécution privilégié. Pour sécuriser l'accès au mode d'exécution privilégié, utilisez la commande de config. globale **enable secret mot de passe**.

Pour sécuriser l'accès au mode d'exécution utilisateur, le port de console doit être configuré. Passez en mode de configuration de console de ligne à l'aide de la commande de

configuration globale **line console 0**. Le zéro sert à représenter la première (et le plus souvent, la seule) interface de console. Spécifiez ensuite le mot de passe du mode d'exécution utilisateur à l'aide de la commande de mot de passe **password mot de passe**.

Enfin, activez l'accès d'exécution utilisateur à l'aide de la commande **login**. La console d'accès requiert à présent un mot de passe avant d'accéder au mode d'exécution utilisateur. Les lignes VTY (terminal virtuel) activent l'accès à distance au périphérique. Pour sécuriser les lignes VTY utilisées pour SSH et Telnet, passez en mode ligne VTY à l'aide de la

commande de config. globale **line vty 0 15**, comme illustré à la figure 3. De nombreux commutateurs Cisco prennent en charge jusqu'à 16 lignes VTY, numérotées de 0 à 15. Spécifiez ensuite le mot de passe VTY à l'aide de la commande **password**. En dernier lieu, activez l'accès VTY à l'aide de la commande **login**.

Exemple de mot de passe d'exécution privilégié

```
Sw-Floor-1>enable
Sw-Floor-1#
Sw-Floor-1#conf terminal
Sw-Floor-1(config)#enable secret class
Sw-Floor-1(config)#exit
Sw-Floor-1#
Sw-Floor-1#disable
Sw-Floor-1>enable
Password: ← Class
Sw-Floor-1#
```

Exemple de mot de passe d'exécution utilisateur

```
Sw-Floor-1(config)#line console 0
Sw-Floor-1(config-line)#password cisco
Sw-Floor-1(config-line)#login
Sw-Floor-1(config-line)#exit
Sw-Floor-1(config)#
```

Exemple de mot de passe de ligne VTY

```
Sw-Floor-1(config)#line vty 0 15
Sw-Floor-1(config-line)#password cisco
Sw-Floor-1(config-line)#login
Sw-Floor-1(config-line)#
```

Les fichiers startup-config et running-config affichent la plupart des mots de passe en clair. C'est une menace à la sécurité dans la mesure où n'importe quel utilisateur peut voir les mots de passe utilisés s'il a accès à ces fichiers.

Pour chiffrer les mots de passe, utilisez la commande de configuration globale **service password-encryption**. La commande applique un chiffrement simple à tous les mots de passe non chiffrés. Ce chiffrement ne s'applique qu'aux mots de passe du fichier de configuration ; il ne s'applique pas lorsque les mots de passe sont transmis sur le réseau. Le but de cette commande est d'empêcher les personnes non autorisées de lire les mots de passe dans le fichier de configuration.

3.4 Messages de bannière :

L'IOS supporte 3 bannières : • La bannière **motd** (Message du jour ou d'accueil),
• La bannière **login** est utilisée pour afficher un message d'avertissement,
• La bannière **exec** permet l'affichage une fois la session ouverte.

Le message peut occuper plusieurs lignes, on doit pour cela choisir un caractère de début et de fin de message : **#**

Ajouter ces lignes à l'ILC du switch :

```
S2960-Newton (config)# banner motd # Avertissement ! Acces aux seules personnes autorisees ! #
```

```
S2960-Newton (config)# banner login
```

#

***** **Avertissement ! Accès aux seules personnes autorisées !** *****
***** **Vos activités au cours de cette session sont susceptibles** *****
***** **d'être enregistrées. Toute activité illicite fera** *****
***** **l'objet d'un recours en justice** *****

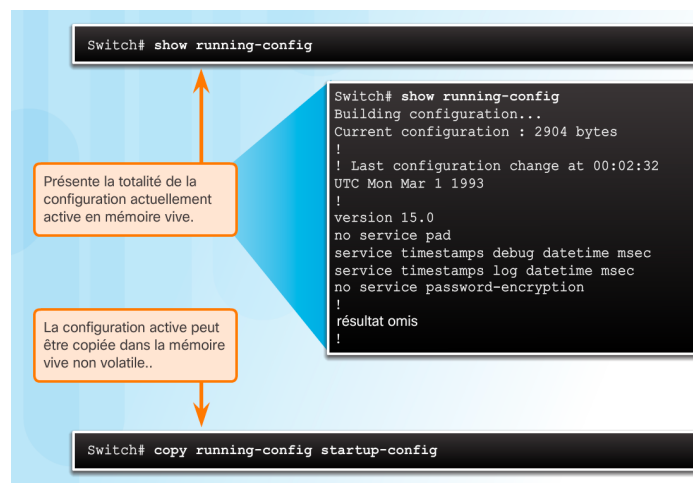
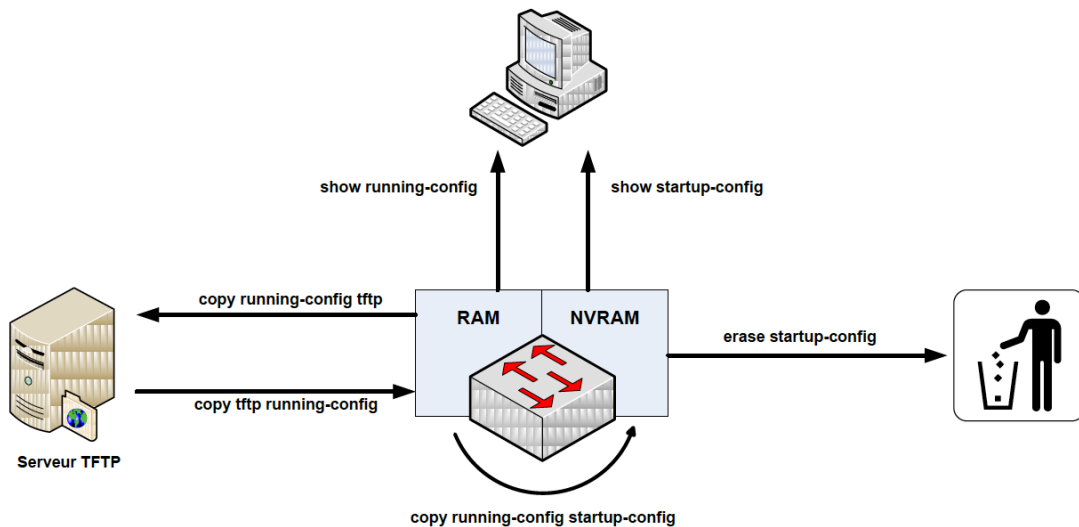
#

S2960-Newton (config)# banner exec

Bienvenue, vous venez de vous connecter au commutateur \$(hostname)
depuis la ligne \$(line), via l'interface \$(line-desc)

#

3.5 Enregistrer le fichier de configuration en cours :



Deux fichiers système stockent la configuration des périphériques :

- **startup-config** : il s'agit du fichier stocké dans la mémoire vive non volatile (NVRAM) qui contient toutes les commandes qui seront utilisées par le périphérique au démarrage ou au redémarrage. La mémoire vive non volatile ne perd pas son contenu lors de la mise hors tension du périphérique.
- **running-config** : il s'agit du fichier stocké dans la mémoire vive (RAM) et qui reflète la configuration actuelle. Modifier une configuration en cours affecte immédiatement le fonctionnement d'un périphérique Cisco. La RAM est une mémoire volatile. Elle perd tout son contenu lorsque le périphérique est mis hors tension ou redémarré.

Comme le montre la figure, vous pouvez entrer la commande du mode d'exécution privilégié **show running-config** pour afficher le fichier de configuration en cours. Pour afficher le fichier de configuration initiale, lancez la commande **show startup-config** du mode d'exécution privilégié.

En cas de panne de courant ou de redémarrage du périphérique, toutes les modifications de la configuration que vous n'avez pas enregistrées sont perdues. Pour enregistrer les modifications apportées à la configuration en cours dans le fichier de configuration initiale, utilisez la commande **copy running-config startup-config** du mode d'exécution privilégié.

3.6 Modifier la configuration en cours :

Si les modifications apportées à la configuration en cours n'ont pas l'effet souhaité et que le fichier running-config n'a pas encore été enregistré, vous pouvez revenir à la configuration antérieure du périphérique en supprimant les commandes modifiées individuellement ou recharger le périphérique à l'aide de la commande **reload** du mode d'exécution privilégié afin de restaurer startup-config.

L'inconvénient de l'utilisation de la commande reload pour supprimer une configuration en cours non enregistrée est le court délai durant lequel le périphérique est hors ligne, entraînant une panne de réseau.

Quand il reçoit une commande de rechargement, IOS vérifie si la configuration en cours comporte des modifications qui n'ont pas été enregistrées dans la configuration initiale. Dans l'affirmative, IOS affiche une invite vous demandant s'il doit enregistrer les modifications. Pour abandonner les modifications, entrez **n** ou **no**.

Sinon, si des modifications indésirables ont été enregistrées dans la configuration initiale, il peut s'avérer nécessaire de supprimer toutes les configurations. Pour ce faire, vous devez effacer la configuration initiale et redémarrer le périphérique. La commande **erase startup-config** du mode d'exécution privilégié permet de supprimer la configuration initiale. Quand vous entrez cette commande, le commutateur vous demande de la confirmer. Appuyez sur **Entrée** pour accepter par défaut.

Après avoir supprimé le fichier de configuration initiale de la mémoire NVRAM, rechargez le périphérique pour supprimer le fichier de configuration en cours de la mémoire vive. Lors du rechargement, un commutateur charge la configuration initiale qui était proposée à l'origine avec le périphérique.