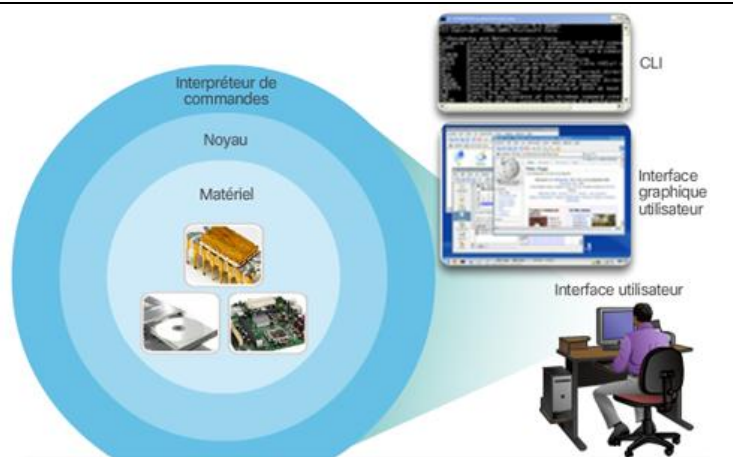


Chapitre 2 : Configuration d'un système d'exploitation réseau

Chaque machine nécessite un système d'exploitation pour fonctionner y compris les machines réseau. Nous allons voir ici les systèmes d'exploitation réseau Cisco appelés aussi IOS.

Système d'exploitation

Le système d'exploitation fait le lien entre l'utilisateur et le matériel. Il est composé d'une interface pouvant être graphique (basé sur des fenêtres) ou en ligne de commandes (interpréteur de commande). Et d'un noyau qui fait le lien entre l'interface et le matériel.



Les systèmes d'exploitation des PC permettent à l'utilisateur d'effectuer les tâches suivantes :

- Utiliser une souris pour faire des sélections et exécuter des programmes
- Saisir du texte et des commandes textuelles
- Afficher les sorties sur un écran
-

Cisco IOS permet à un technicien réseau d'effectuer les tâches suivantes :

- Utiliser un clavier pour exécuter des programmes réseau basés sur une CLI
- Utiliser un clavier pour saisir du texte et des commandes textuelles
- Afficher les sorties sur un écran

Tous les périphériques réseau sont livrés avec un IOS par défaut. Il est possible de mettre à niveau la version ou un ensemble de fonctionnalités de l'IOS.

IOS

Accès

Pour accéder au système IOS, on peut utiliser plusieurs méthodes ayant chacune ses avantages et ses inconvénients.

- **Console** Un port physique de gestion d'un système pouvant être accédé hors réseau et utile pour la maintenance du périphérique, il utilise un câble (**bleu**) spécifique
- **SSH (secure shell)** permettant de se connecter à distance au système
- **Telnet** Méthode non sécurisée d'accès, tous les mots de passe et les commandes sont transmis en clair
- **AUX** Ancien port utilisant une connexion téléphonique et un modem pour être administré

	Console	Telnet/SSH	AUX
1.Vous êtes dans le local technique et un nouveau commutateur doit être configuré.	✓		
2.Votre responsable vous donne un câble spécial et vous demande de l'utiliser pour configurer le commutateur.	✓		
3.Vous accédez à l'IOS à l'aide d'un autre périphérique intermédiaire via une connexion réseau.		✓	
4.Vous appelez votre responsable pour lui indiquer que vous ne pouvez pas accéder au routeur via Internet depuis une autre ville. Il vous fournit des informations pour accéder au commutateur par une connexion téléphonique.			✓

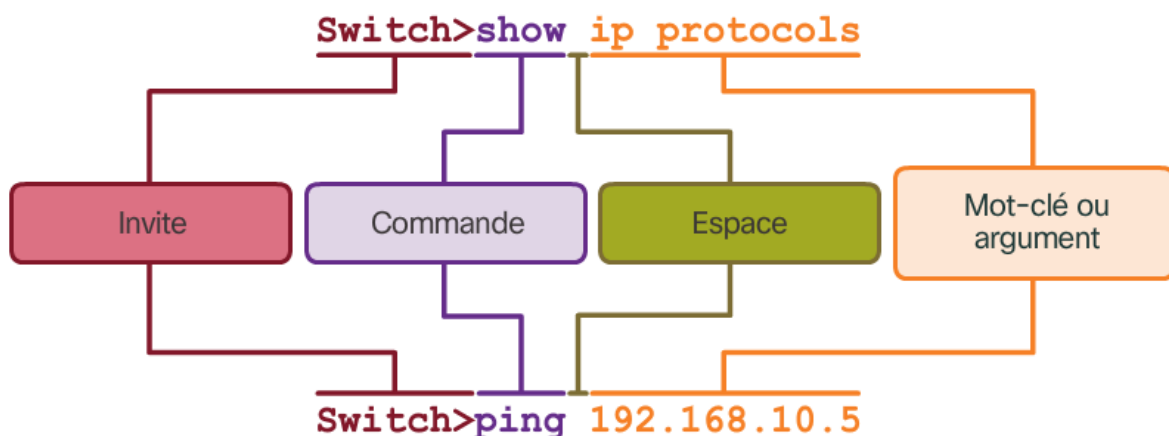
Modes de commande

Il existe deux grands modes de commande permettant à l'utilisateur de faire plus ou moins d'actions.

- **Mode utilisateur** visible par le prompt `>`, permet des actions limitées de monitoring mais empêche toute modification de la configuration.
- **Mode privilégié** visible par le prompt `#`, permet d'exécuter des opérations de maintenance et de configuration du routeur. On entre dans ce mode par la commande `enable` depuis le mode utilisateur.
- **Mode de configuration** visible par le prompt `(config)#` et accessible par l'intermédiaire du mode privilégié, on peut y modifier la configuration du périphérique. On entre dans ce mode avec la commande `configure terminal`
- **Mode de configuration de ligne** visible par le prompt `(config-line)#` et accessible par le mode de configuration, il permet de modifier la configuration des accès console, ssh ou telnet. On entre dans ce mode avec la commande `line`
- **Mode de configuration d'interface** visible par le prompt `(config-if)#` et accessible depuis le mode de configuration, il permet de modifier la configuration relative aux interfaces réseau. On entre dans ce mode avec la commande `interface`.

Structure des commandes

Une commandes IOS est constituée de plusieurs éléments :



IOS implémente des fonctionnalités d'aide accessible par la commande `?` à tout instant. De plus entrer une syntaxe incorrecte vous sera informé dans l'invite.

Après avoir tapé une commande complète suivie des mots-clés et des arguments adéquats, appuyez sur la touche Entrée pour la soumettre à l'interpréteur de commandes.

Raccourcis clavier : Lors de l'Édition d'une commande

Touche	Description	Touche	Description
Tab	Complète le nom de la commande	CTRL+E	Déplace le curseur à la fin de la ligne
CTRL+D	Efface le caractère à l'emplacement du curseur	Esc+B	Déplace le curseur d'un mot vers la gauche
CTRL+K	Efface tous les caractères jusqu'à la fin de la ligne	Esc+F	Déplace le curseur d'un mot vers la droite
Esc+D	Efface tous les caractères du curseur jusqu'à la fin du mot	CTRL+R	Rappelle l'invité de commande
CTRL+U CTRL+X	Efface tous les caractères jusqu'au début de la ligne	CTRL+C	Quitte le mode configuration
CTRL+W	Efface le mot à gauche du curseur	CTRL+MAJ+6	Interrompt une commande de recherche DNS, traceroute ou ping
CTRL+A	Déplace le curseur au début de la ligne	CTRL+Z	Quitte le mode configuration, retourne au mode privilégié

Lors d'un invité "More"

Entrée Avance d'une ligne

Espace Avance d'une page

Autre chose Quitte l'affichage "More"

Nom de périphérique

Le nom de périphérique permet de reconnaître un périphérique sur le réseau. Ce nom doit :

- Débuter par une lettre
- Ne pas contenir d'espace
- Se terminer par une lettre ou un chiffre
- Ne peut comporter des lettres, des chiffres et des tirets
- Comporter moins de 64 caractères

Pour configurer le nom de périphérique (nom d'hôte), dans le mode de configuration, on doit utiliser la commande **hostname** suivi du nouveau nom du périphérique.

Exemple :

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

On peut annuler les changements en utilisant **no hostname**

Sécurité

Les systèmes IOS permettent, pour sécuriser le matériel, les actions suivantes :

- Ajouter un mot de passe au mode d'exécution privilégié
- Ajouter un mot de passe au mode utilisateur
- Ajouter un mot de passe lors de l'accès à distance
- Chiffrer les mots de passe
- Ajouter une notification légale

Mots de passe

On ajoute un mot de passe lors de l'accès au mode d'exécution privilégié avec la commande **enable secret** suivi du mot de passe. Cette commande doit être exécutée dans le mode de configuration globale. On ajoute un mot de passe lors de l'accès utilisateur avec la commande **password** suivi du mot de passe. Cette commande doit être exécutée dans le mode de configuration en ligne (**line console 0**). On active ensuite l'authentification avec la commande **login** (on peut la désactiver avec **no login**).

On peut en faire de même pour les accès distants via telnet ou **SSH** en utilisant les mêmes commandes que précédemment mais dans le mode de configuration **vtty** (**line vty 0 15**).

Les mots de passe sont alors écrits en clair dans les fichiers startup-config et running-config ce qui peut représenter un problème de sécurité. Pour activer le chiffrement des mots de passe on peut utiliser la commande **service password-encryption** dans le mode de configuration global.

Message légal

Pour prévenir de l'aspect privé du matériel on peut mettre en place une bannière qui s'affichera à chaque connexion. Pour se faire on utilise la commande **banner motd** **#<message>#**. On écrit alors le message entre les #.

Fichiers de configuration

Il existe deux fichiers de configuration sur le système IOS:

- **startup-config** La configuration dans la mémoire vive et non volatile qui lui permet d'être conservée malgré l'arrêt du système.
- **running-config** Une copie de startup-config utilisée par le système. Cette configuration est réinitialisée lors du redémarrage de la machine.
-

Pour afficher une des deux configurations on utilise la commande **show** suivi du nom de la configuration à afficher.

Pour enregistrer la configuration courante dans la mémoire et ainsi persister cette configuration on utilise la commande **copy running-config startup-config**.

Si une configuration non voulue vient à être ajoutée on peut ainsi utiliser la commande **reload** pour recharger le périphérique et ainsi revenir à la configuration startup-config. Dans le pire des cas on peut supprimer la configuration initiale avec **erase startup-config**. Cela aura pour effet de réinitialiser la configuration à son état original au prochain rechargement.

Adresse IP

Une adresse IP est le principal outil permettant aux périphériques de se localiser entre eux. Une adresse IP est composée de 4 nombres de 0 à 255 séparés par des points.

Une adresse IP peut être attribuée à chaque port physique et aux interfaces virtuelles d'appareils Cisco.

Interface

Une interface est la jonction entre le matériel de la machine et le support réseau. On représente souvent une interface comme un port physique Ethernet est la technologie de réseau local (LAN) la plus répandue aujourd'hui, mais il existe bien d'autres types de ports qui dépendent de :

- La distance sur laquelle le support peut transmettre l'information
- L'environnement dans lequel les supports sont installés
- Le débit
- Le coût d'installation

Interface virtuelle

Une interface virtuelle (nommée SVI) est, dans les systèmes Cisco de couche 3 et plus, un moyen de gérer à distance **un commutateur de couche 2** et dispose d'une adresse IP. L'interface virtuelle par défaut est Vlan1

Pour configurer une interface virtuelle, il faut entrer dans le mode de configuration d'interface en donnant le nom de l'interface. Par défaut l'interface virtuelle est vlan1 on entre donc dans ce mode avec `interface vlan 1` depuis le mode d'exécution privilégié. On peut alors configurer son adresse IP à l'aide de la commande `ip address <adresse ip> <masque>`. On doit alors redémarrer l'interface avec la commande `no shutdown`.

Exemple

```
Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.10.2 255.255.255.0
Switch(config-if)# no shutdown
```

Configuration IP

La configuration de l'adresse IP peut se faire manuellement en spécifiant l'adresse et le masque dans les paramètres du système.

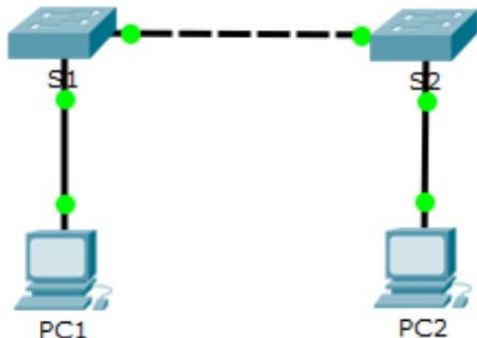
Mais il peut aussi s'effectuer automatiquement en suivant le protocole DHCP permettant de demander à un serveur spécialisé une adresse IP et un masque.

Tests et monitoring

Sur une machine Cisco, on peut exécuter diverses commandes permettant de tester ou de monitorer les interfaces. Pour afficher l'IP d'une interface on utilisera `show ip interface brief` depuis le mode d'exécution privilégié. Cette commande affiche l'état des interfaces de la machine et diverses informations à son sujet

Pour tester la connexion d'une machine à une autre on utilisera la commande `ping` permettant de demander une réponse à la machine distante.

Exemple 2.3.2.5 Packet Tracer - Mise en œuvre de la connectivité de base.

Topologie	Table d'adressage			
	Appareil	Interface	Adresse IP	Masque de sous-réseau
	S1	VLAN 1	192.168.1.253	255.255.255.0
	S2	VLAN 1	192.168.1.254	255.255.255.0
	PC1	Carte réseau	192.168.1.1	255.255.255.0
	PC2	Carte réseau	192.168.1.2	255.255.255.0

Effectuer une configuration de base sur S1 et S2 (Exemple pour le Switch S1)

<pre>Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#hostname S1 S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#enable secret class S1(config)#banner motd "Acces autoris uniquement. Violators will be prosecuted to the full extent of the law." S1(config)#exit S1# %SYS-5-CONFIG_I: Configured from console by console S1#copy running-config startup- config Destination filename [startup- config]? Building configuration... [OK] S1# S1#exit Acces autorise uniquement. Violators will be prosecuted to the full extent of the law.</pre>	<pre>User Access Verification Password: cisco S1>enable Password: class S1#conf t Enter configuration commands, one per line. End with CNTL/Z. S1(config)#interface vlan 1 S1(config-if)#ip address 192.168.1.253 255.255.255.0 S1(config-if)#no shutdown S1(config-if)# %LINK-5-CHANGED: Interface Vlan1, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up S1(config-if)#exit S1(config)#exit S1# S1#copy running-config startup-config Destination filename [startup- config]? Building configuration... [OK] S1#</pre>
--	---

Utilisez la commande **show ip interface brief** pour afficher l'adresse IP et l'état de tous les ports et interfaces des commutateurs. Vous pouvez également utiliser la commande **show running-config**. Vérifier la connectivité entre le PC et le switch grâce à la commande **ping** depuis le switch ou le PC dans l'invite de commande.