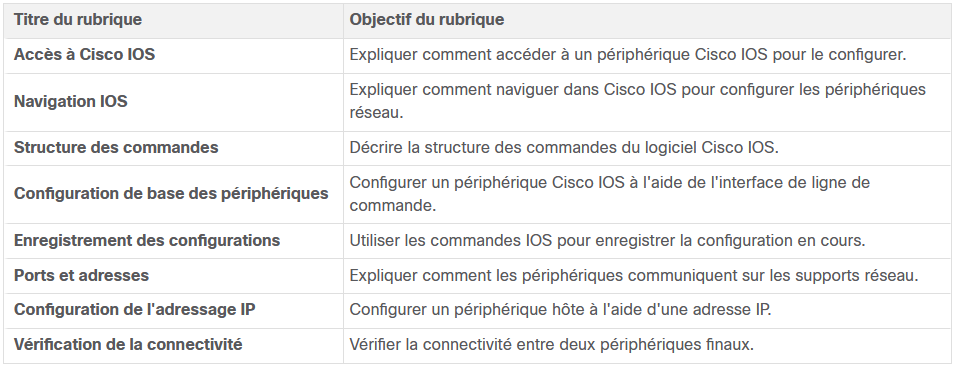
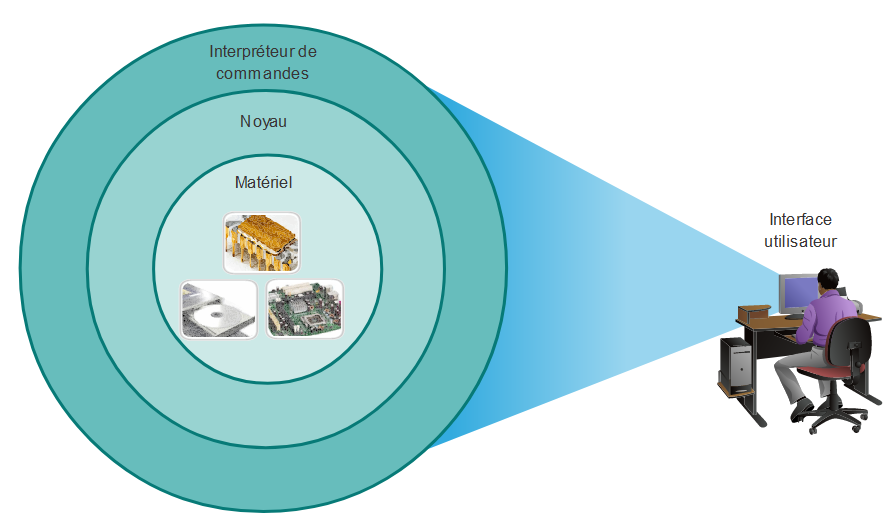
*Cours CISCO et réseaux :*

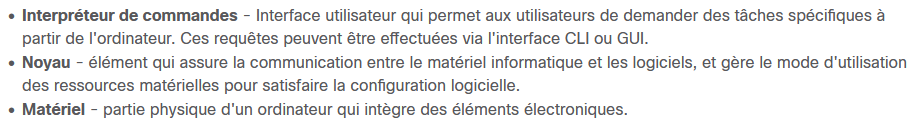
**CHAPITRE 2 - Configuration de base des commutateurs et des périphériques finaux**



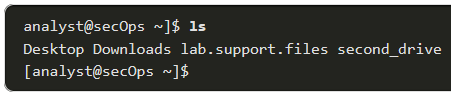
**Systèmes d'exploitation**

Tous les périphériques finaux et réseau requièrent un système d'exploitation (SE). Comme le montre la figure, la partie du OS 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 de commande sous-jacente qui contrôle le système.



## Interface utilisateur

Une interface utilisateur graphique (GUI) telle que Windows, macOS, Linux KDE, 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'exemple d'interface utilisateur graphique (GUI) de la figure est plus convivial 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 (GUI).

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 (IOS). Cisco IOS est utilisé par la plupart des routeurs et des commutateurs Cisco, quels que soient leur taille et leur type. Chaque routeur de périphérique ou type de commutateur utilise une version différente de Cisco IOS. Les autres systèmes d'exploitation Cisco incluent IOS XE, IOS XR et NX-OS.

**Note**: 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.

## Objectif d'un OS

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

* 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'effectuer les étapes suivantes :

* 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.

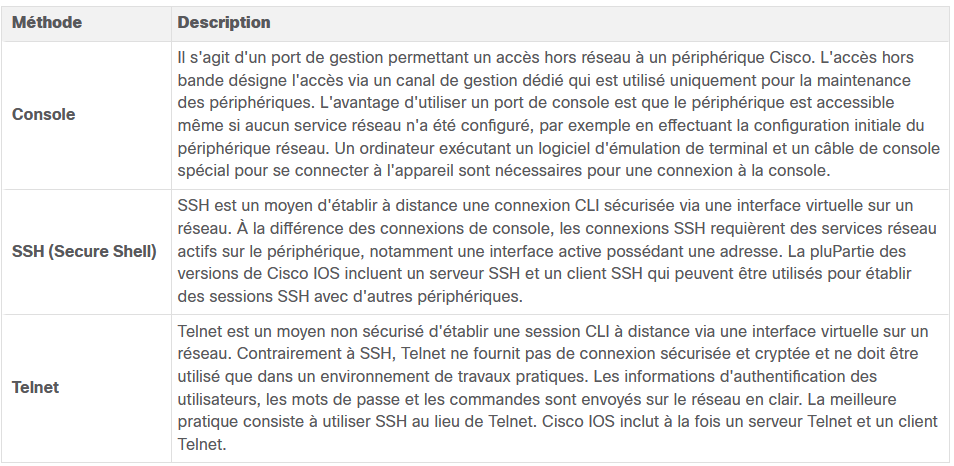
Les périphériques réseau exécutent des versions spécifiques de Cisco IOS. La version de l'IOS dépend du type de périphérique utilisé et des fonctions nécessaires. Alors que tous les périphériques possèdent un IOS et un ensemble de fonctionnalités par défaut, il est possible de mettre à niveau l'IOS ou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

La figure répertorie les versions logicielles d'IOS disponibles pour un commutateur Cisco Catalyst 2960.

## Méthodes d'accès

Un commutateur transmet le trafic par défaut et n'a pas besoin d'être explicitement configuré pour fonctionner. Par exemple, deux hôtes configurés connectés au même nouveau commutateur seraient en mesure de communiquer.

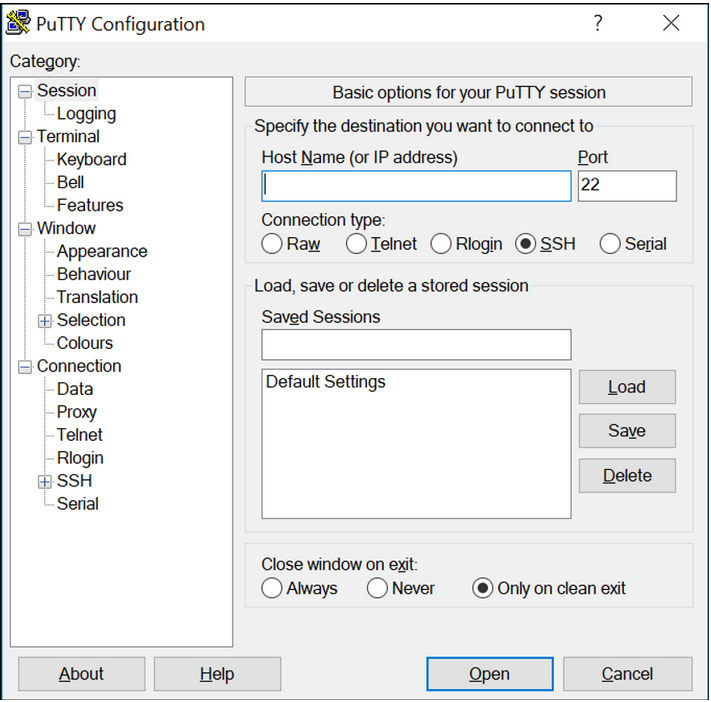
Quel que soit le comportement par défaut d'un nouveau commutateur, tous les commutateurs doivent être configurés et sécurisés.



**Remarque:** Certains périphériques tels que les routeurs peuvent également prendre en charge un port auxiliaire ancien qui était utilisé auparavant pour établir une session CLI à distance à l'aide d'un modem. Tout comme une connexion console, le port AUX est hors réseau et ne nécessite pas de service réseau pour être configuré ou disponible.

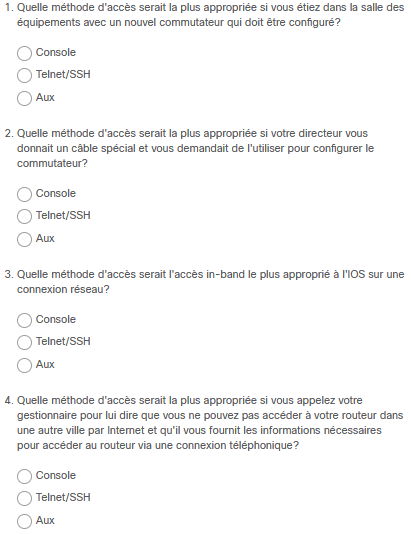
## Programmes d'émulation de terminal

## Il existe d'excellents programmes d'émulation de terminal permettant de se connecter à un périphérique réseau via une connexion série sur un port de console ou via une connexion SSH ou Telnet. Ces programmes vous permettent d'améliorer votre productivité grâce à différentes fonctionnalités comme la personnalisation de la taille des fenêtres, de la taille des polices ou des jeux de couleurs.



## Ex d’émulateur de terminal :

## Vérifiez votre compréhension - Accès à Cisco IOS



## NAVIGATION IOS

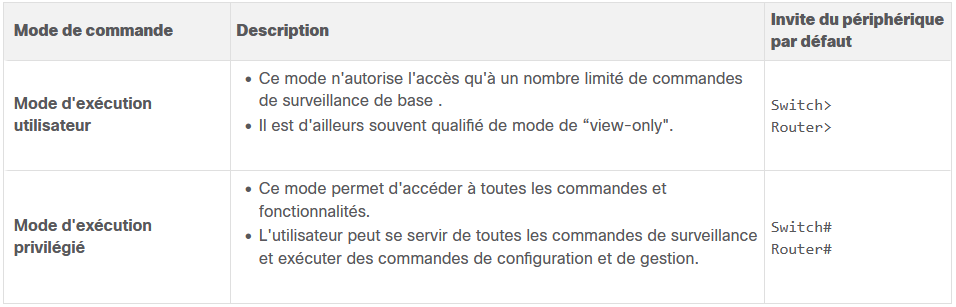
## Modes de commande principaux

Dans la rubrique précédente, vous avez appris que tous les périphériques réseau nécessitent un système d'exploitation et qu'ils peuvent être configurés à l'aide de l'interface de ligne de commande ou d'une interface graphique. L'utilisation de l'interface de ligne de commande peut fournir à l'administrateur réseau un contrôle et une flexibilité plus précis que l'utilisation de l'interface graphique. Cette rubrique présente l'utilisation du CLI pour naviguer dans l'IOS de Cisco.

Par mesure de sécurité, le logiciel Cisco IOS sépare l'accès à la gestion en deux modes de commande:

* **Mode d'exécution utilisateur** - ce mode offre des fonctionnalités limitées, mais s'avère utile pour les opérations de base. Il autorise seulement un nombre limité de commandes de surveillance de base, mais il n'autorise aucune commande susceptible de modifier la configuration du périphérique. Le mode d'exécution utilisateur se reconnaît à l'invite CLI qui se termine par le symbole >.
* **Mode d'exécution privilégié** - pour exécuter les commandes de configuration, un administrateur réseau doit accéder au mode d'exécution privilégié. Pour accéder aux modes de configuration supérieurs, comme celui de configuration globale, il est nécessaire de passer par le mode d'exécution privilégié. Le mode d'exécution privilégié se reconnaît à l'invite qui se termine par le symbole # .

Le tableau résume les deux modes et affiche les invites de l'interface de ligne de commande par défaut d'un commutateur et d'un routeur Cisco.



## Mode de configuration et sous-modes de configuration

Pour configurer le périphérique, l'utilisateur doit passer en mode de configuration globale, appelé généralement mode de config. globale.

Les modifications de la configuration effectuées dans l'interface de ligne de commande en mode de config. globale affectent le fonctionnement du périphérique dans son ensemble. Le mode de configuration globale se reconnaît à l'invite se terminant par (config)# après le nom de l'appareil, comme **Switch(config)#**.

L'accès au mode de configuration globale se fait avant les autres modes de configuration spécifiques. À partir du mode de config. globale, l'utilisateur peut accéder à différents sous-modes de configuration. Chacun de ces modes permet de configurer une partie ou une fonction spéciale du périphérique IOS. Les deux sous-modes de configuration les plus courants sont les suivants:

* **Mode de configuration de ligne -** utilisé pour configurer l'accès par la console, par SSH, par Telnet, ou l'accès AUX.
* **Mode de configuration d'interface -** utilisé pour configurer l'interface réseau d'un port de commutateur ou d'un routeur.

Lors l'utilisation de CLI, le mode dans lequel vous travaillez est reconnaissable à son invite de commandes unique. Par défaut, toute invite commence par le nom du périphérique. Après le nom du périphérique, le reste de l'invite précise le mode. Par exemple, l'invite par défaut pour le mode de configuration de ligne est **Switch(config-line)#** et l'invite par défaut pour le mode de configuration d'interface est **Switch(config-if)#**.

## Naviguer entre les différents modes IOS

Différentes commandes sont utilisées pour entrer et sortir des invites de commandes. Pour passer du mode utilisateur au mode privilégié, utilisez la commande **enable** . Utilisez la commande **disable** du mode d'exécution privilégié pour retourner au mode d'exécution utilisateur.

**Remarque**: le mode d'exécution privilégié est parfois appelé mode actif.

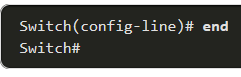
Pour passer en mode de configuration globale et le quitter, utilisez la commande de mode d'exécution privilégié **configure terminal** . Pour repasser en mode d'exécution privilégié, entrez la commande de mode de config. globale **exit** .

Il existe de nombreux sous-modes de configuration différents. Par exemple, pour passer en sous-mode de configuration de ligne, utilisez la commande **line** suivie du type et du numéro de la ligne de gestion à laquelle vous souhaitez accéder. Pour quitter un sous-mode de configuration et retourner au mode de configuration globale, utilisez la commande **exit** .

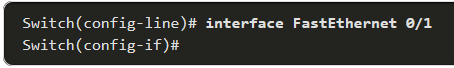
## 

Pour passer de n'importe quel sous-mode de configuration du mode de configuration globale au mode situé un niveau plus haut dans la hiérarchie des modes, saisissez la commande **exit** .

Pour passer de n'importe quel sous-mode de configuration au mode d'exécution privilégié, entrez la commande **end** ou utilisez la combinaison de touches **Ctrl+Z** .



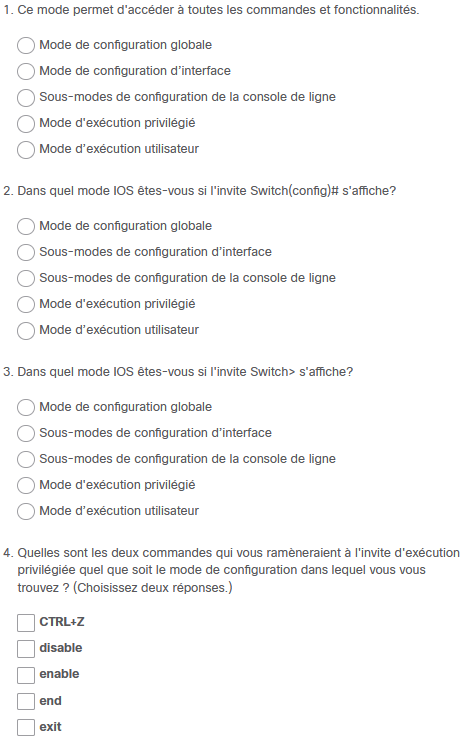
Vous pouvez aussi passer directement d'un sous-mode de configuration à un autre. Notez qu'après avoir sélectionné une interface, l'invite de commande change de **(config-line)#** to **(config-if)#**.



## Remarque sur les activités du contrôleur de syntaxe

Lorsque vous apprenez à modifier les configurations de périphériques, vous pouvez commencer dans un environnement sûr et non productif avant de l'essayer sur un équipement réel. NetaCAD vous offre différents outils de simulation pour vous aider à développer vos compétences de configuration et de dépannage. Comme il s'agit d'outils de simulation, ils n'ont généralement pas toutes les fonctionnalités de l'équipement réel. Un de ces outils est le contrôleur de syntaxe. Dans chaque contrôleur de syntaxe, on vous donne un ensemble d'instructions pour saisir un ensemble spécifique de commandes. Vous ne pouvez pas progresser dans le contrôleur de syntaxe sauf si la commande exacte et complète est entrée comme spécifié. Des outils de simulation plus avancés, tels que le Packet Tracer, vous permettent de saisir des commandes abrégées, comme vous l'appliquerez sur un équipement réel.

## Vérifiez votre compréhension - Navigation d'IOS

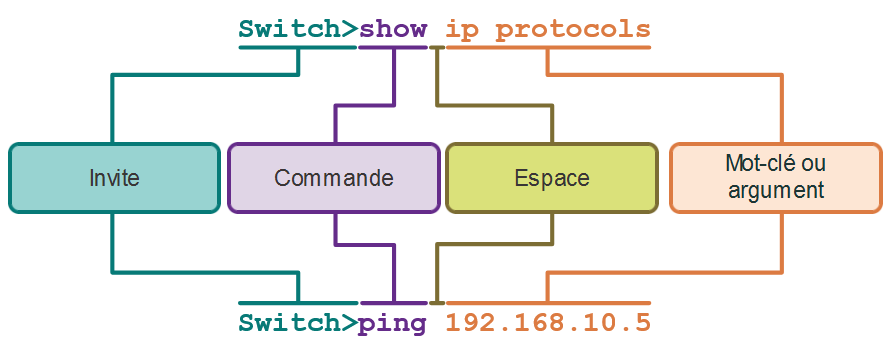


# **Structure des commandes**

## Structure des commandes IOS de base

Cette rubrique couvre la structure de base des commandes de Cisco IOS. Un administrateur réseau doit connaître la structure de commande IOS de base pour pouvoir utiliser l'interface de ligne de commande pour la configuration du périphérique.

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. La syntaxe générale d'une commande est constituée de la commande suivie des mots-clés et des arguments appropriés.



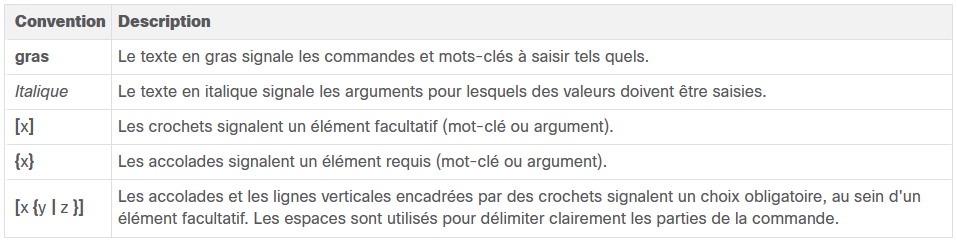
* **Mot-clé** - Il s'agit d'un paramètre spécifique défini dans le système d'exploitation (sur la figure, **ip protocols**).
* **Argument** - Ce n'est pas prédéfini; c'est une valeur ou une variable définie par l'utilisateur (dans la figure **192.168.10.5**)

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

## Vérification de la syntaxe des commandes IOS

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

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



Par exemple, la syntaxe d'utilisation de la commande **description** est **description** *string.* L'argument est une valeur *string* fournie par l'utilisateur. La commande **description** est généralement utilisée pour identifier le rôle d'une interface. Par exemple, la commande **description Connects to the main headquarter office switch** décrit l'endroit où se trouve l'autre périphérique au bout de la connexion.

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

* **ping** *ip-address* - 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** *ip-address* - 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**.

Si une commande est complexe avec plusieurs arguments, vous pouvez la voir représentée comme ceci:



La commande sera généralement suivie une description détaillée de la commande et chaque argument.

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

## Fonctionnalités d'aide d'IOS

L'IOS propose deux formes d'aide: l'aide contextuelle et la vérification de la syntaxe des commandes.

Une aide contextuelle vous permet de trouver rapidement des réponses aux questions suivantes:

* Quelles commandes sont disponibles dans chaque mode de commande?
* Quelles commandes commencent par des caractères spécifiques ou un groupe de caractères?
* Quels arguments et mots clés sont disponibles pour des commandes particulières?

Pour afficher l'aide contextuelle, tapez simplement un point d'interrogation, **?**, dans le CLI.

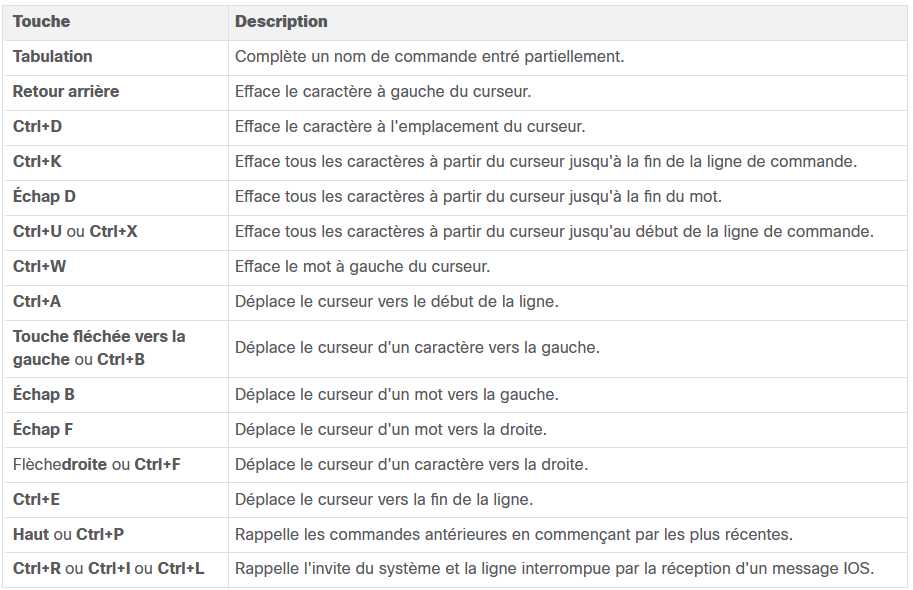
La vérification de la syntaxe des commandes contrôle que l'utilisateur a entré une commande valide. Lorsque vous entrez une commande, l'interpréteur de lignes de commandes analyse la commande de gauche à droite. Si l'interpréteur comprend la commande, IOS exécute l'action demandée et l'invite appropriée reparaît dans l'ILC. Par contre, s'il ne comprend pas la commande entrée, l'interpréteur affiche des commentaires décrivant le problème rencontré.

## Touches d’accès rapide et raccourcis.

Dans le CLI d'IOS, des touches d'accès rapide et des raccourcis facilitent la configuration, la surveillance et le dépannage.

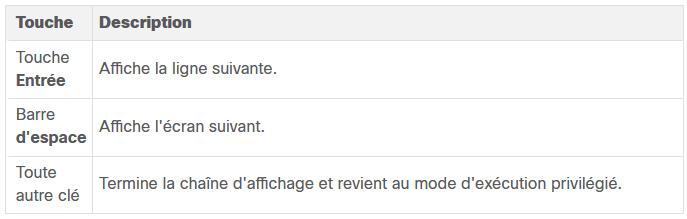
Il est possible de raccourcir les commandes et les mots-clés jusqu'au nombre minimal de caractères qui identifient une sélection unique. Par exemple, vous pouvez raccourcir la commande **configure** en entrant **conf** parce que **configure** est la seule commande qui commence par **conf**. Par contre, la version raccourcie **con**, ne fonctionne pas parce que plusieurs commandes débutent par **con**. Vous pouvez aussi raccourcir les mots clés.

Le tableau répertorie les touches our améliorer l'édition en ligne de commande.

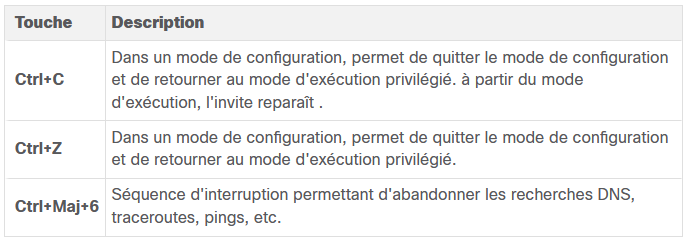


**Remarque**: Bien que la touche **Delete** supprime généralement le caractère à droite de l'invite, la structure de commande IOS ne reconnaît pas la touche Supprimer.

Lorsqu'une sortie de commande produit plus de texte que ce qui peut être affiché dans une fenêtre de terminal, l'IOS affiche une invite **“--More--”** . Le tableau suivant décrit les frappes qui peuvent être utilisées lorsque cette invite est affichée.



Ce tableau répertorie les commandes utilisées pour quitter une opération.



# **Configuration de base des périphériques**

## Noms de périphériques

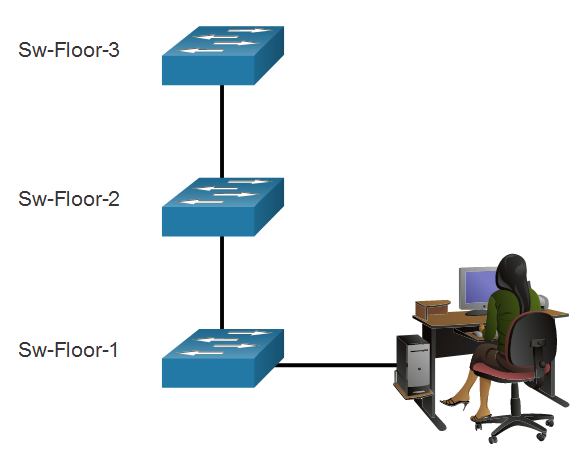
Vous avez beaucoup appris sur le Cisco IOS, la navigation dans l'IOS et la structure de commande. Maintenant, vous êtes prêt à configurer les périphériques! La première commande de configuration sur un périphérique doit être l'attribution d'un nom de périphérique ou un nom d'hôte unique. Par défaut, tous les périphériques se voient attribuer un nom d'usine par défaut. Par exemple, un commutateur Cisco IOS est "Switch".

Si tous les périphériques réseau ont conservé leurs noms par défaut, il sera difficile d'identifier un périphérique spécifique. Par exemple, comment sauriez-vous que vous êtes connecté au bon appareil lorsque vous y accédez à distance à l'aide de SSH? Le nom d'hôte confirme que vous êtes connecté au périphérique approprié.

Le nom par défaut doit être remplacé par quelque chose de plus descriptif. 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 ci-dessous:

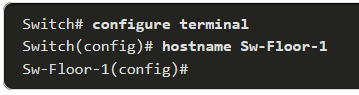
* débutent par une lettre
* Ne contiennent pas d'espaces
* se terminent par une lettre ou un chiffre
* Ne comportent que des lettres, des chiffres et des tirets
* Comportent moins de 64 caractères

Une organisation doit choisir une convention de dénomination qui facilite et intuitif l'identification d'un appareil spécifique. IOS distingue les majuscules des minuscules dans les noms d'hôte utilisés pour les périphériques. Par exemple, dans la figure, 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.



Grâce aux noms il est plus facile d’identifier des périphériques réseau pour les configurer.

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. Comme indiquee dans l'illustration, 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 **Enter**. Remarquez le changement dans le nom de l'invite de commandes.

**Remarque**: Pour renvoyer le commutateur à l'invite par défaut, utilisez la commande de config. globale **no hostname** .

N'oubliez pas de mettre à jour la documentation chaque fois que vous ajoutez ou modifiez un périphérique. Dans la documentation, identifiez les périphériques par leur emplacement, leur rôle et leur adresse.

## Recommandations relatives aux mots de passe forts

L'utilisation de mots de passe faibles ou facilement devinés continue d'être la préoccupation la plus importante des organisations en matière de sécurité. Des mots de passe doivent toujours être configurés pour les périphériques réseau, y compris les routeurs sans fil domestiques, afin de limiter l'accès administratif.

Cisco IOS peut être configuré pour utiliser des mots de passe de mode hiérarchique afin de permettre d'établir différents privilèges d'accès à un périphérique réseau.

Tous les périphériques réseau doivent limiter l'accès administratif en sécurisant les accès d'exécution, d'exécution utilisateur et Telnet à distance avec des mots de passe. En outre, tous les mots de passe doivent être cryptés et des notifications légales doivent être fournies.

Utilisez des mots de passe forts qui ne sont pas faciles à deviner. Pour choisir les mots de passe, respectez les règles suivantes:

* Utilisez des mots de passe de plus de 8 caractères.
* Utilisez une combinaison de lettres majuscules et minuscules, des chiffres, des caractères spéciaux et/ou des séquences de chiffres.
* Évitez d'utiliser le même mot de passe pour tous les périphériques.
* N'utilisez pas des mots courants car ils sont faciles à deviner.

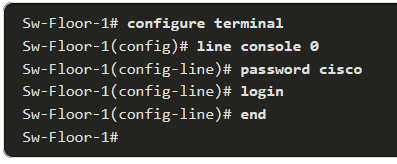
Utilisez une recherche sur Internet pour trouver un générateur de mot de passe. Plusieurs vous permettront de définir la longueur, le jeu de caractères et d'autres paramètres.

Classe de **Remarque:** La plupart des laboratoires de ce cours utilisent des mots de passe simples tels que **cisco** ou \*\*\*\*. Il faut éviter ces mots de passe dans les environnements de production, car ils sont considérés comme faibles et faciles à deviner. Nous n'utilisons ces mots de passe que pour une utilisation dans une salle de cours ou pour illustrer des exemples de configuration.

## Configurer les mots de passe

Lorsque vous vous connectez initialement à un périphérique, vous êtes en mode d'exécution utilisateur. Ce mode est sécurisé à l'aide de la console.

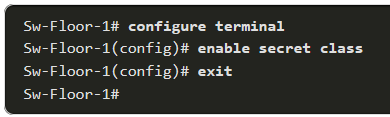
Pour sécuriser l'accès en mode d'exécution utilisateur, entrez le mode de configuration de la console de ligne à l'aide de la commande de configuration globale **line console 0** , comme indiqué dans l'exemple. Le zéro sert à représenter la première (et le plus souvent, la seule) interface de console. Spécifiez ensuite le mot de passe du mode d'exécution utilisateur à l'aide de la commande **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.

Pour disposer d'un accès administrateur à toutes les commandes IOS, y compris la configuration d'un périphérique, vous devez obtenir un accès privilégié en mode d'exécution. C'est la méthode d'accès la plus importante car elle fournit un accès complet à l'appareil.

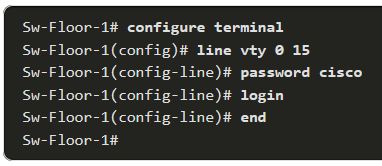
Pour sécuriser l'accès au mode d'exécution privilégié, utilisez la commande de config. globale **enable secret** mot de passe, comme indiqué dans l’illustration.



Les lignes VTY (terminal virtuel) activent l'accès à distance au périphérique en utilisant Telnet ou SSH. Plusieurs commutateurs Cisco prennent en charge jusqu'à 16 lignes VTY, numérotées de 0 à 15.

Pour sécuriser les lignes VTY, entrez le mode VTY ligne à l'aide de la commande de config. globale **line vty 0 15** . Spécifiez ensuite le mot de passe VTY à l'aide de la commande **password** mot de passe . En dernier lieu, activez l'accès VTY à l'aide de la commande **login** .

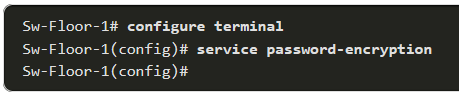
Un exemple de sécurisation des lignes VTY sur un commutateur est illustré.



## Chiffrer les mots de passe

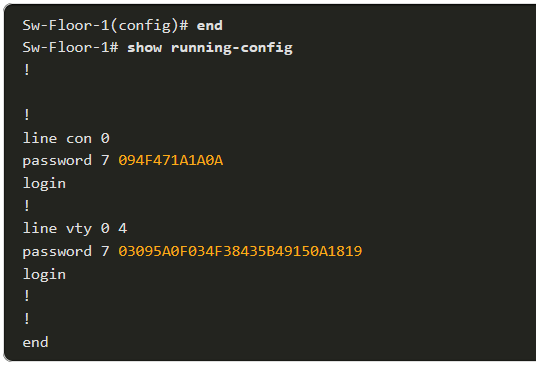
Les fichiers startup-config et running-config affichent la pluPartie des mots de passe en clair. C'est une menace à la sécurité dans la mesure où n'importe quel utilisateur peut voir les mots de passe utilisés s'il a accès à ces fichiers.

Pour chiffrer tous les mots de passe en texte clair, utilisez la commande de config. globale **service password-encryption** comme indiqué dans l’illustration.



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.

Utilisez la commande **show running-config** pour vérifier que les mots de passe sont maintenant chiffrés.

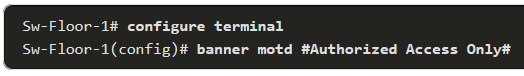


## Messages de bannière

Bien que les mots de passe soient l'un des moyens dont vous disposez pour empêcher l'accès non autorisé à un réseau, il est vital de mettre en place une méthode pour déclarer que l'accès à un périphérique est réservé aux seules personnes autorisées. À cet effet, ajoutez une bannière aux informations affichées par le périphérique. Les bannières peuvent constituer une pièce importante dans un procès intenté à une personne qui aurait accédé illégalement à un périphérique. En effet, dans certains systèmes juridiques, il est impossible de poursuivre des utilisateurs, ni même de les surveiller s'ils n'ont pas reçu de notification appropriée au préalable.

Pour créer une bannière MOTD (Message Of The Day) sur un périphérique réseau, utilisez la commande de config. globale du **banner motd #** du message du jour **#** . Le "#" situé dans la syntaxe de la commande est le caractère de délimitation. Il est placé avant et après le message. Vous pouvez utiliser comme délimiteur tout caractère ne figurant pas dans le message. C'est la raison pour laquelle les symboles tels que "#" sont souvent employés comme délimiteurs. Une fois cette commande exécutée, la bannière s'affiche lors de toutes les tentatives d'accès au périphérique jusqu'à ce que vous la supprimiez.

L'exemple suivant montre les étapes de configuration de la bannière sur Sw-Floor-1.

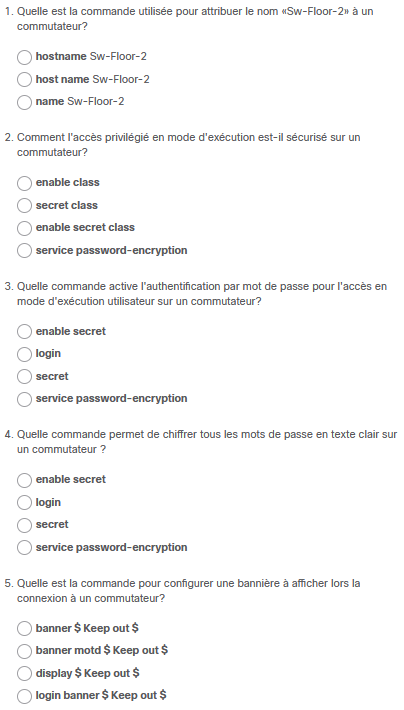


## Contrôleur de syntaxe - Configuration de base du périphérique

Sécuriser l'accès à la gestion d'un commutateur.

* Attribuez un nom de périphérique.
* Sécurisez l'accès au mode d'exécution utilisateur.
* Sécurisez l'accès au mode d'exécution privilégié.
* Sécurisez l'accès VTY.
* Cryptez tous les mots de passe en clair.
* Affichez la bannière

## Vérifiez votre compréhension - Configuration du périphérique de base



# **Enregistrement des configurations**

## Fichiers de configuration

Vous savez maintenant comment effectuer la configuration de base sur un commutateur, y compris les mots de passe et les messages de bannière. Cette rubrique vous montrera comment enregistrer vos configurations.

Deux fichiers système stockent la configuration des périphériques:

* **startup-config** - Ceci est le fichier de configuration enregistré qui est stocké dans NVRAM. Ce fichier stocké dans la mémoire vive non volatile contient toutes les commandes qui seront utilisées 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** - Ceci est stocké dans la mémoire vive (RAM). Il 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.

La commande mode d'exécution privilégié **show running-config** est utilisée pour afficher la configuration en cours d'exécution. Comme indiqué dans l'exemple, la commande répertorie la configuration complète actuellement stockée dans la RAM.

## 

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.

## Modifier la configuration en cours

Si les modifications apportées à la configuration d'exécution n'ont pas l'effet souhaité et que la configuration d'exécution n'a pas encore été enregistrée, vous pouvez restaurer l'appareil dans sa configuration précédente. Supprimez les commandes modifiées individuellement ou rechargez le périphérique à l'aide de la commande en mode d’exécution **reload** privilégié pour restaurer la configuration de démarrage.

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**.

Par ailleurs, 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 **Enter** pour accepter la connexion.

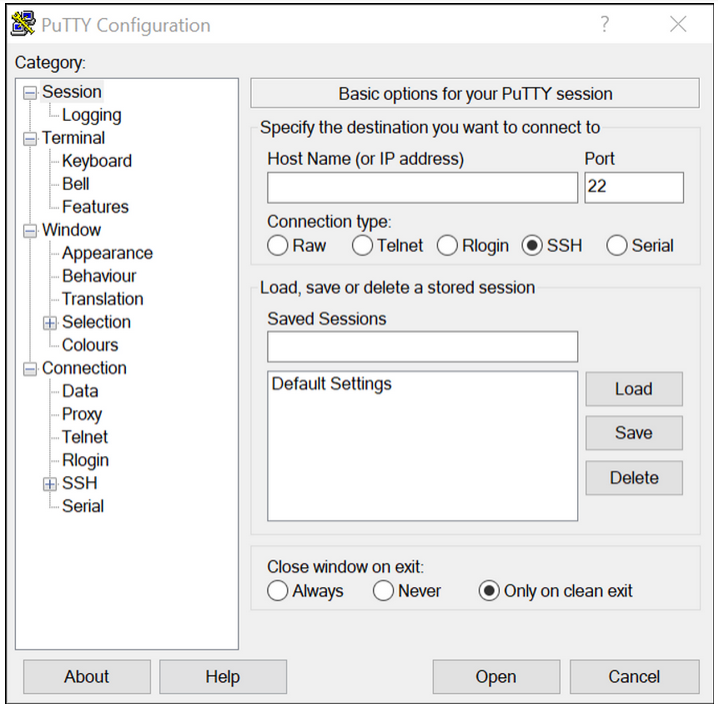
Après avoir supprimé le fichier de configuration initiale de la mémoire NVRAM, rechargez le périphérique pour supprimer le fichier de configuration en cours de la mémoire vive. Lors du rechargement, un commutateur charge la configuration initiale qui était proposée à l'origine avec le périphérique.

## Capturer de la configuration dans un fichier texte

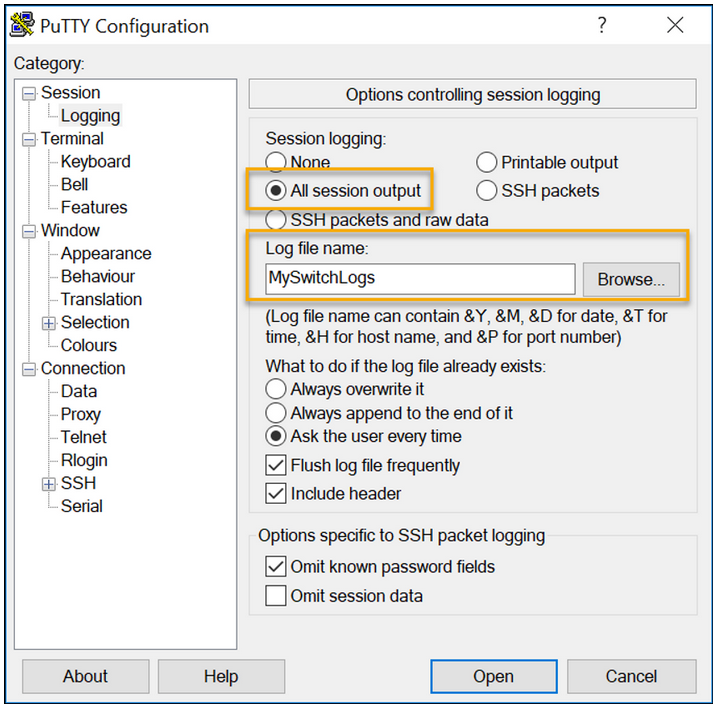
Vous pouvez aussi enregistrer et archiver les fichiers de configuration dans un document texte. Cette procédure permet de vous assurer qu'une copie de travail du fichier de configuration est disponible en vue d'une modification ou d'une réutilisation ultérieure.

Par exemple, supposons qu'un commutateur a été configuré et que la configuration en cours a été enregistrée sur le périphérique.

**Étape 1.** Ouvrez un logiciel d'émulation de terminal, tel que PuTTY ou Tera Term qui est connecté à un commutateur.



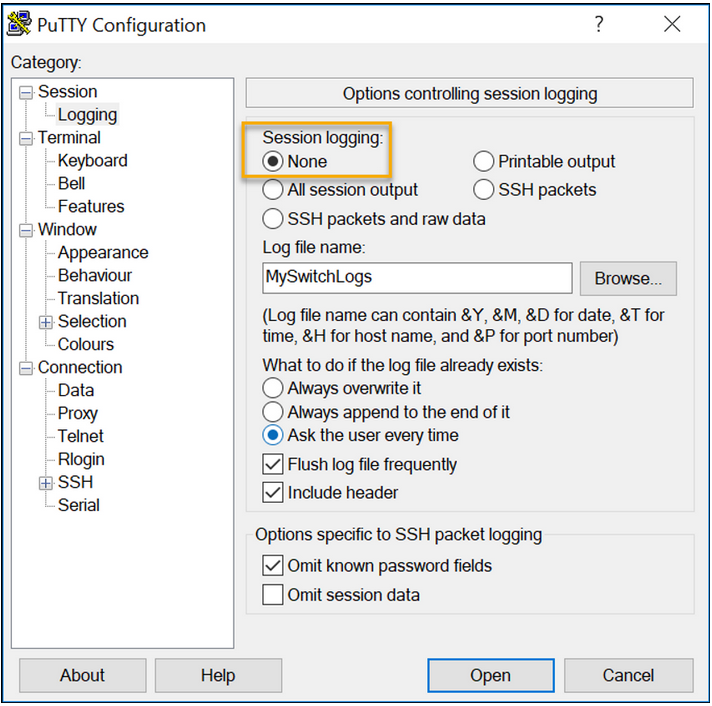
**Étape 2.** Activez l'enregistrement dans le logiciel de terminal, et attribuez un nom et un emplacement de fichier pour enregistrer le fichier journal. La figure indique que **All session output** seront capturés dans le fichier spécifié (c.-à-d., MySwitchLogs).



**Étape 3.** Exécutez la commande **show running-config** ou **show startup-config** à l'invite d'exécution privilégiée. Le texte affiché dans la fenêtre du terminal est alors placé dans le fichier choisi.



**Étape 4.** Désactivez l'enregistrement dans le logiciel de terminal. La figure montre comment désactiver l'enregistrement en choisissant l'option d'ouverture de session **None** (Aucune).



Le fichier texte créé peut être utilisé comme enregistrement de la façon dont le périphérique est actuellement implémenté. Il peut être nécessaire de modifier le fichier avant de l'utiliser afin de restaurer une configuration enregistrée sur un périphérique.

Pour restaurer un fichier de configuration sur un périphérique:

**Étape 1.** passez en mode de configuration globale sur le périphérique;

**Étape 2.** copiez et collez le fichier texte dans la fenêtre du terminal connecté au commutateur.

Le texte contenu dans le fichier est appliqué sous forme de commandes dans l'environnement CLI et devient la configuration en cours du périphérique. Cette méthode s'avère pratique pour configurer manuellement un périphérique.

# **Ports et adresses**

## Adresses IP

Félicitations, vous avez effectué une configuration de base de l'appareil! Bien sûr, le plaisir n'est pas encore terminé. Si vous souhaitez que vos périphériques finaux communiquent entre eux, vous devez vous assurer que chacun d'eux possède une adresse IP appropriée et qu'il est correctement connecté. Vous en apprendrez plus sur les adresses IP, les ports de périphériques et les supports utilisés pour connecter les périphériques dans cette rubrique.

L'utilisation d'adresses IP est le principal moyen permettant aux périphériques de se localiser les uns les autres et d'établir la communication de bout en bout sur Internet. Chaque périphérique final d'un réseau doit être configuré avec une adresse IP. Exemples de périphériques finaux:

* Ordinateurs (stations de travail, ordinateurs portables, serveurs de fichiers, serveurs web)
* Imprimantes réseau
* Téléphones VoIP
* Caméras de surveillance
* Smartphones
* Périphériques portables mobiles (par exemple, lecteurs de codes à barres sans fil)

La structure d'une adresse IPv4 est appelée «notation décimale à point» et est composée de quatre nombres décimaux compris entre 0 et 255. Les adresses IPv4 sont affectées à des périphériques individuels connectés à un réseau.

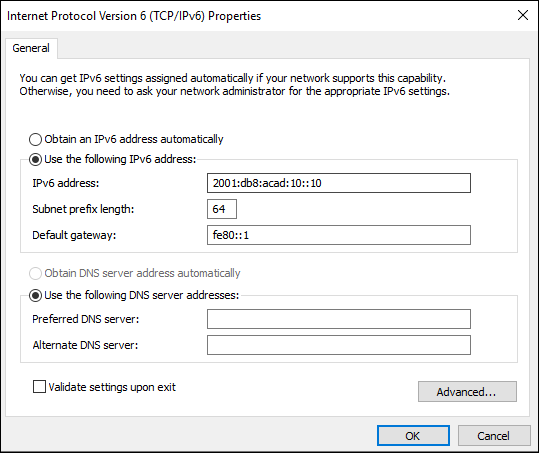
**Remarque**: Dans ce cours, «IP» fait référence aux protocoles IPv4 et IPv6. L'IPv6 est la version la plus récente de l'IP et remplace l'IPv4.

Avec une adresse IPv4, un masque de sous-réseau est également nécessaire. Un masque de sous-réseau IPv4 est une valeur 32 bits qui différencie la partie réseau de l'adresse de la partie hôte. Associé à l'adresse IPv4, le masque de sous-réseau détermine à quel sous-réseau spécifique le périphérique appartient.

L'exemple de la figure montre l'adresse IPv4 (192.168.1.10), le masque de sous-réseau (255.255.255.0) et la passerelle par défaut (192.168.1.1) attribués à un hôte. L'adresse de passerelle par défaut est l'adresse IP du routeur que l'hôte utilisera pour accéder aux réseaux distants, y compris à Internet.

## 

Les adresses IPv6 ont une longueur de 128 bits et sont notées sous forme de chaînes de valeurs hexadécimales. Tous les groupes de 4 bits sont représentés par un caractère hexadécimal unique, pour un total de 32 valeurs hexadécimales. Les groupes de quatre chiffres hexadécimaux sont séparés par un deux-points (:). Les adresses IPv6 ne sont pas sensibles à la casse et peuvent être notées en minuscules ou en majuscules.



## Interfaces et ports

## Les communications réseau dépendent des interfaces des périphériques utilisateur final, des interfaces des périphériques réseau et des câbles de connexion. Chaque interface a des caractéristiques, ou des normes, qui la définissent. Un câble de connexion à l'interface doit donc être adapté aux normes physiques de l'interface. Ces supports de transmission peuvent être des câbles en cuivre à paires torsadées, des câbles à fibres optiques, des câbles coaxiaux ou une liaison sans fil, comme illustré dans la figure.

## 

Les différents types de supports réseau possèdent divers avantages et fonctionnalités. Tous les supports réseau n'ont pas les mêmes caractéristiques. Tous les médias ne sont pas appropriés pour le même objectif Les différences entre les types de supports de transmission incluent, entre autres:

* la distance sur laquelle les supports peuvent transporter correctement un signal
* l'environnement dans lequel les supports doivent être installés
* la quantité de données et le débit de la transmission
* le coût des supports et de l'installation.

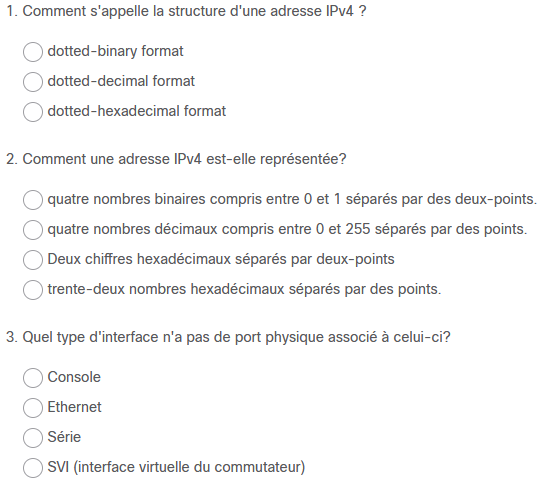
Chaque liaison à Internet requiert un type de support réseau spécifique, ainsi qu'une technologie réseau particulière. Par exemple, l'Ethernet est la technologie de réseau local (LAN) la plus répandue aujourd'hui. Les ports Ethernet sont présents sur les périphériques des utilisateurs finaux, les commutateurs et d'autres périphériques réseau pouvant se connecter physiquement au réseau à l'aide d'un câble.

Les commutateurs Cisco IOS de couche 2 sont équipés de ports physiques pour permettre à des périphériques de s'y connecter. Ces ports ne prennent pas en charge les adresses IP de couche 3. Par conséquent, les commutateurs ont une ou plusieurs interfaces de commutateur virtuelles (SVI). Ces interfaces sont virtuelles car il n'existe aucun matériel sur le périphérique associé. Une interface SVI est créée au niveau logiciel.

L'interface virtuelle est un moyen de gérer à distance un commutateur sur un réseau grâce à l'IPv4 et l'IPv6 Chaque commutateur dispose d'une interface SVI apparaissant dans la configuration par défaut prête à l'emploi. L'interface SVI par défaut est l'interface VLAN1.

**Remarque**: un commutateur de couche 2 ne nécessite pas d'adresse IP. L'adresse IP attribuée à l'interface SVI sert à accéder à distance au commutateur. Une adresse IP n'est pas nécessaire pour permettre au commutateur d'accomplir ses tâches.

## Vérifiez votre compréhension - Ports et adresses



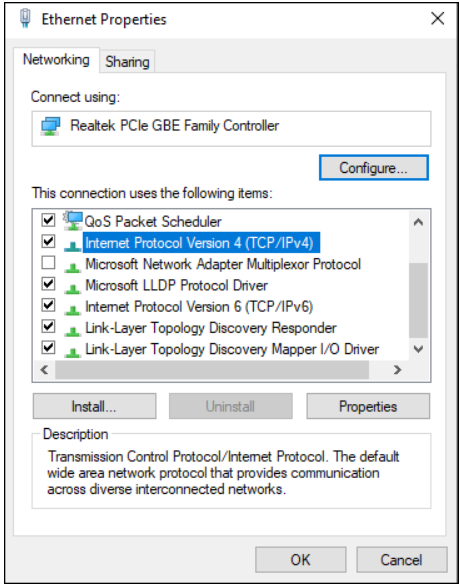
# **Configuration de l'adressage IP**

## Configuration manuelle des adresses IP des périphériques finaux

Tout comme vous avez besoin des numéros de téléphone de vos amis pour les envoyer par SMS ou les appeler, les terminaux de votre réseau ont besoin d'une adresse IP afin qu'ils puissent communiquer avec d'autres appareils de votre réseau. Dans cette rubrique vous mettrez ensuite en œuvre la connectivité de base en configurant l'adressage IP sur les commutateurs et les ordinateurs.

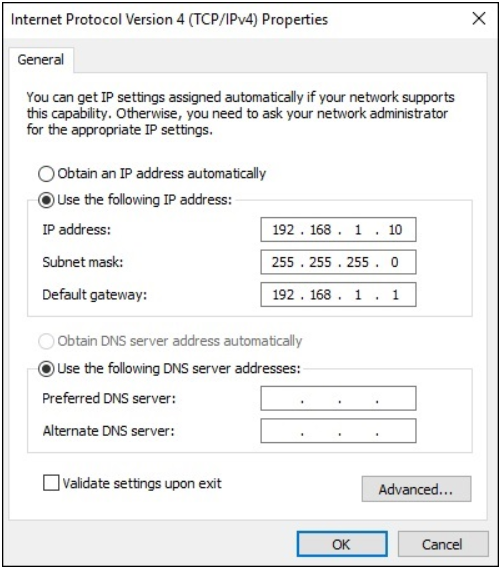
Les informations d'adresse IPv4 peuvent être entrées manuellement sur les périphériques finaux, ou attribuées automatiquement à l'aide du protocole DHCP (Dynamic Host Configuration Protocol).

Pour configurer manuellement une adresse IPv4 sur un hôte Windows, ouvrez **Control Panel > Network Sharing Center > Change adapter settings** et choisissez la carte. Cliquez ensuite avec le bouton droit **Properties** de la souris et sélectionnez pour afficher le **Local Area Connection Properties**, comme indiqué dans la figure.



Surlignez Protocole Internet version 4 (TCP/IPv4) et cliquez sur **Properties** pour ouvrir la fenêtre **Internet Protocol Version 4 (TCP/IPv4) Properties** , illustrée dans la figure. Configurez les informations de l'adresse IPv4 et du masque de sous-réseau, ainsi que la passerelle par défaut.

**Remarque**: Les options d'adressage et de configuration IPv6 sont similaires à IPv4.



**Remarque**: les adresses du serveur DNS sont les adresses IP des serveurs de système de noms de domaine (DNS). Elles sont utilisées pour convertir des adresses IP en noms de domaine.

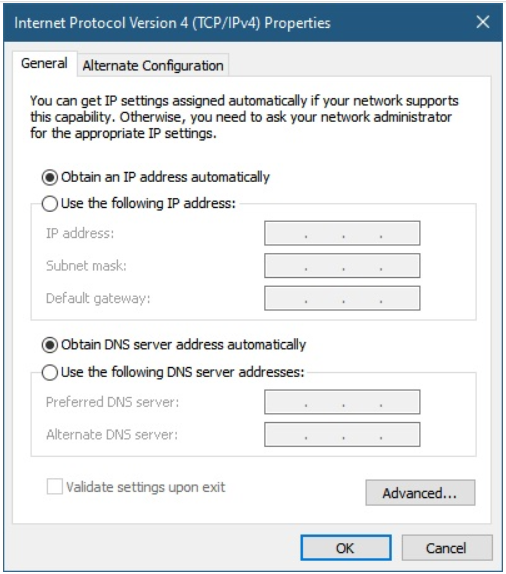
## Configuration automatique des adresses IP des périphériques finaux

Généralement, les périphériques finaux utilisent par défaut le protocole DHCP pour la configuration automatique des adresses IPv4. Le protocole DHCP est une technologie utilisée sur presque tous les réseaux. Le meilleur moyen de comprendre pourquoi le DHCP est tellement répandu est de prendre en compte tout le travail supplémentaire qui doit être effectué sans celui-ci.

Sur un réseau, le protocole DHCP permet la configuration automatique des adresses IPv4 pour chaque périphérique final utilisant DHCP. Imaginez le temps que cela prendrait si chaque fois que vous vous connectez au réseau vous deviez entrer manuellement l'adresse IPv4, le masque de sous-réseau, la passerelle par défaut et le serveur DNS. Multipliez cette opération par le nombre d'utilisateurs et de périphériques d'une entreprise: vous avez saisi le problème. La configuration manuelle augmente également les risques de mauvaise configuration en dupliquant l'adresse IPv4 d'un autre périphérique.

Comme le montre la figure, pour configurer DHCP sur un PC Windows, il vous suffit de sélectionner **Obtain an IP address automatically** et **Obtain DNS server address automatically**. Votre ordinateur recherchera alors un serveur DHCP et se verra affecté les paramètres de l'adresse qui sont nécessaires pour communiquer sur le réseau.

**Remarque**: IPv6 utilise DHCPv6 et SLAAC (configuration automatique d'adresses sans état) pour l'allocation dynamique d'adresses.



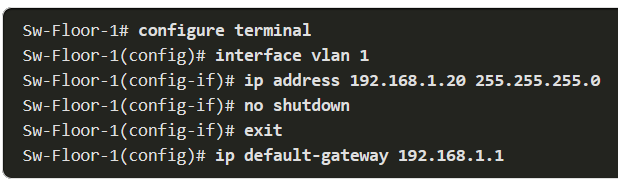
## Contrôleur de syntaxe - Vérification de la configuration IP de Windows PC

Il est possible d'afficher les paramètres de configuration IP d'un ordinateur Windows à l'aide de la commande **ipconfig** depuis l'invite de commandes. Le résultat affiche les informations concernant l'adresse IPv4, le masque de sous-réseau et la passerelle, qui ont été reçues du serveur DHCP.

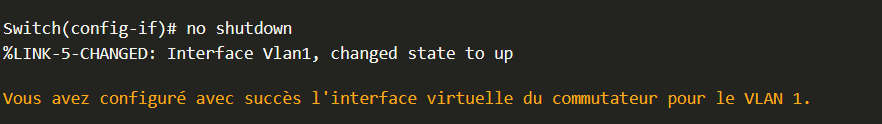
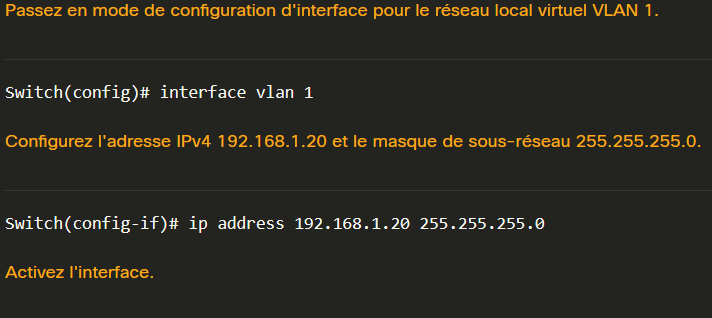
## Configuration de l'interface de commutateur virtuelle

Pour accéder à distance au commutateur, une adresse IP et un masque de sous-réseau doivent être configurés sur l'interface SVI. Pour configurer une SVI sur un commutateur, utilisez la commande de configuration globale **interface vlan 1** . Vlan 1 n'est pas une interface physique réelle mais une interface virtuelle. Attribuez ensuite une adresse IPv4 à l'aide de la commande de configuration d'interface **ip address** ip-address subnet-mask. Enfin, activez l'interface virtuelle à l'aide de la commande de configuration d'interface **no shutdown** .

Une fois ces commandes configurées, le commutateur dispose de tous les éléments IPv4 adaptés pour la communication sur le réseau.



## Contrôleur de syntaxe - Configuration d'une interface de commutateur virtuelle



## Qu'est-ce que j'ai appris dans ce module?

Tous les périphériques finaux et réseau requièrent un système d'exploitation (SE). L'utilisateur peut interagir avec le shell à l'aide d'une interface de ligne de commande (CLI) pour utiliser un clavier pour exécuter des programmes réseau basés sur l'interface utilisateur, utiliser un clavier pour entrer des commandes textuelles et textuelles et afficher la sortie sur un moniteur.

Par mesure de sécurité, le logiciel Cisco IOS sépare l'accès aux fonctionnalités de gestion en deux modes de commande: le mode d'exécution utilisateur et le mode d'exécution privilégié.

L'accès au mode de configuration globale se fait avant les autres modes de configuration spécifiques. À partir du mode de config. globale, l'utilisateur peut accéder à différents sous-modes de configuration. Chacun de ces modes permet de configurer une partie ou une fonction spéciale du périphérique IOS. Deux sous-modes de configuration courants sont: le mode de configuration de ligne et le mode de configuration d'interface. Pour passer en mode de configuration globale et le quitter, utilisez la commande **configure terminal** de mode d'exécution privilégié . Pour repasser en mode d'exécution privilégié, entrez la commande de mode de config. globale **exit** .

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. L'IOS propose deux formes d'aide: l'aide contextuelle et la vérification de la syntaxe des commandes.

La première commande de configuration sur un périphérique doit être l'attribution d'un nom de périphérique ou un nom d'hôte unique. Des mots de passe doivent toujours être configurés pour les périphériques réseau, afin de limiter l'accès administratif. Cisco IOS peut être configuré pour utiliser des mots de passe de mode hiérarchique afin de permettre d'établir différents privilèges d'accès à un périphérique réseau. Configurez et chiffrez tous les mots de passe . Fournir une méthode pour déclarer que seul le personnel autorisé doit tenter d'accéder à l'appareil en ajoutant une bannière à la sortie de l'appareil.

Deux fichiers système stockent la configuration des périphériques: startup-config et running-config. Les fichiers de configuration en cours d'exécution peuvent être modifiés s'ils n'ont pas été enregistrés. Vous pouvez aussi enregistrer et archiver les fichiers de configuration dans un document texte.

La commande IP addresses enable devices permet aux périphériques de se localiser les uns les autres et d'établir la communication de bout en bout sur Internet. Chaque périphérique final d'un réseau doit être configuré avec une adresse IP. La structure d'une adresse IPv4 est appelée «notation décimale à point» et est composée de quatre nombres décimaux compris entre 0 et 255.

Les informations d'adresse IPv4 peuvent être entrées manuellement sur les périphériques finaux, ou attribuées automatiquement à l'aide du protocole DHCP (Dynamic Host Configuration Protocol). Sur un réseau, le protocole DHCP permet la configuration automatique des adresses IPv4 pour chaque périphérique final utilisant DHCP. Pour accéder à distance au commutateur, une adresse IP et un masque de sous-réseau doivent être configurés sur l'interface SVI. Pour configurer une SVI sur un commutateur, utilisez la commande **interface vlan 1 global configuration** . Vlan 1 n'est pas une interface physique réelle mais une interface virtuelle.

Après avoir appris à utiliser des commandes et des utilitaires pour vérifier la configuration réseau de l'hôte PC, vous allez également utiliser des commandes permettant de vérifier les interfaces et les paramètres des adresses des périphériques intermédiaires, tels que les commutateurs et les routeurs. La commande **show ip interface brief** est utile pour vérifier l'état des interfaces des commutateurs. La commande **ping** peut être utilisée pour tester la connectivité vers un autre périphérique sur le réseau, un site web ou Internet.

## Questionnaires de module -Configuration des paramètres de base des commutateurs et des périphériques finaux

