# Configuration des périphériques réseau

## 1 Configuration initiale d'un routeur à services intégrés (ISR)

### *1.1 ISR*

Le routeur à services intégrés (ISR) Cisco est l'un des périphériques réseau les plus populaires conçus pour répondre aux besoins croissants des entreprises en termes de communication. La technologie ISR réunit dans un seul périphérique plusieurs fonctionnalités telles que des fonctions de routage et de commutation du réseau local (LAN), de sécurité, vocales, ainsi que des fonctions de connectivité de réseau étendu (WAN). Le routeur ISR est ainsi idéal pour les petites et moyennes entreprises, ainsi que pour les clients des FAI.

Le module de commutation intégré facultatif permet aux petites entreprises de connecter des périphériques LAN directement au routeur ISR 1841. Grâce au module de commutation intégré, si le nombre d'hôtes du réseau local est supérieur au nombre de ports de commutation, des commutateurs ou concentrateurs supplémentaires peuvent être connectés en chaîne pour augmenter le nombre de ports LAN disponibles. Si le module de commutation n'est pas inclus, des commutateurs externes sont connectés aux interfaces du routeur ISR.

La fonction de routage de l'ISR permet de subdiviser un réseau en de nombreux sous-réseaux locaux et prend en charge la connexion des périphériques LAN internes à Internet ou au réseau étendu (WAN).

La gamme de routeurs à services intégrés (ISR) Cisco

Routeur à services intégrés de la gamme Cisco 800

Routeur à services intégrés de la gamme Cisco 3800

Routeur à services intégrés de la gamme Cisco 1800

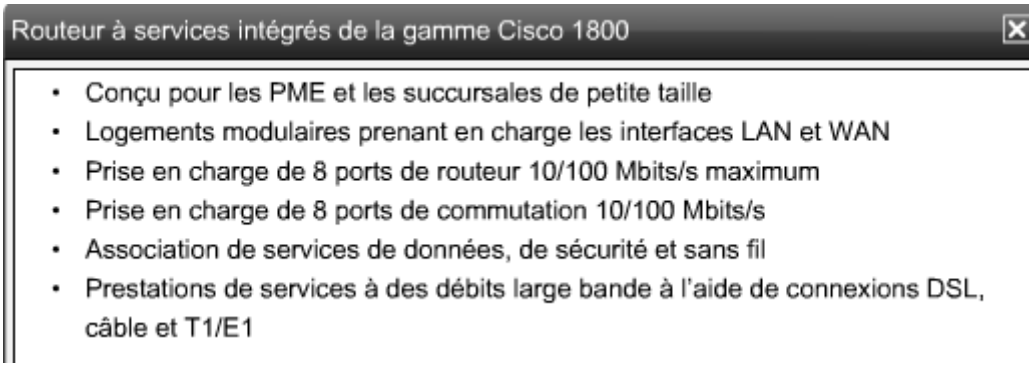
Routeur à services intégrés de la gamme Cisco 2800

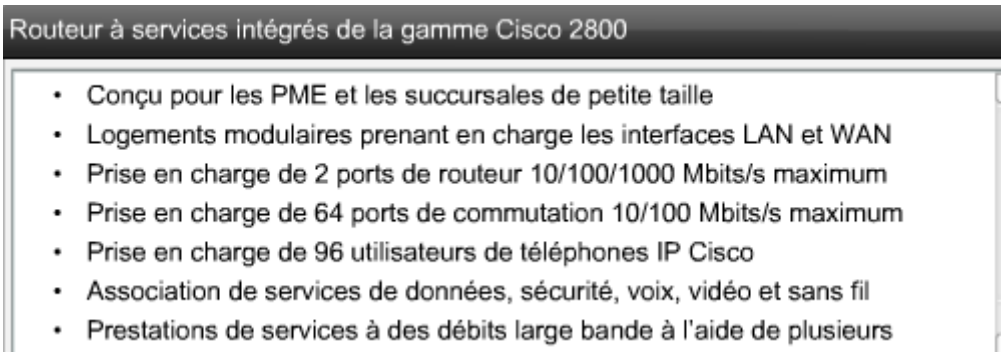
**Routeur à services intégrés de la gamme Cisco 800**

- Conçu pour les utilisateurs à domicile et dans les petits bureaux
- Prise en charge d'1 connexion WAN
- Prise en charge de 4 ports 10/100 Mbits/s
- Association de services de données, de sécurité et sans fil
- Prestations de services à des débits large bande

**Routeur à services intégrés de la gamme Cisco 3800**

- Conçu pour les PME et les succursales de petite taille
- Logements modulaires prenant en charge les interfaces LAN et WAN
- Prise en charge de 2 ports de routeur 10/100/1000 Mbits/s maximum
- Prise en charge de 112 ports de commutation 10/100 Mbits/s maximum
- Prise en charge de 240 utilisateurs de téléphones IP Cisco
- Association de services de données, sécurité, voix, vidéo et sans fil
- Prestations de services à des débits large bande à l'aide de connexions DSL,



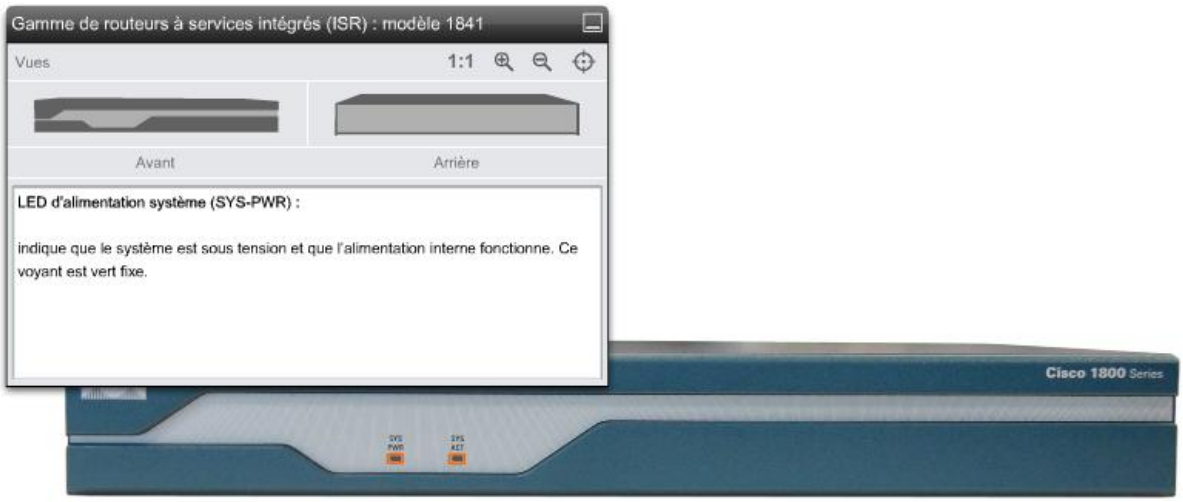

Le logiciel Cisco IOS (Internetwork Operating System) fournit des fonctionnalités qui permettent à un périphérique Cisco d'envoyer et de recevoir du trafic réseau à l'aide d'un réseau filaire ou sans fil. Le logiciel Cisco IOS est proposé aux clients sous la forme de modules appelés images. Ces images prennent en charge diverses fonctionnalités pour des organisations de toutes tailles.

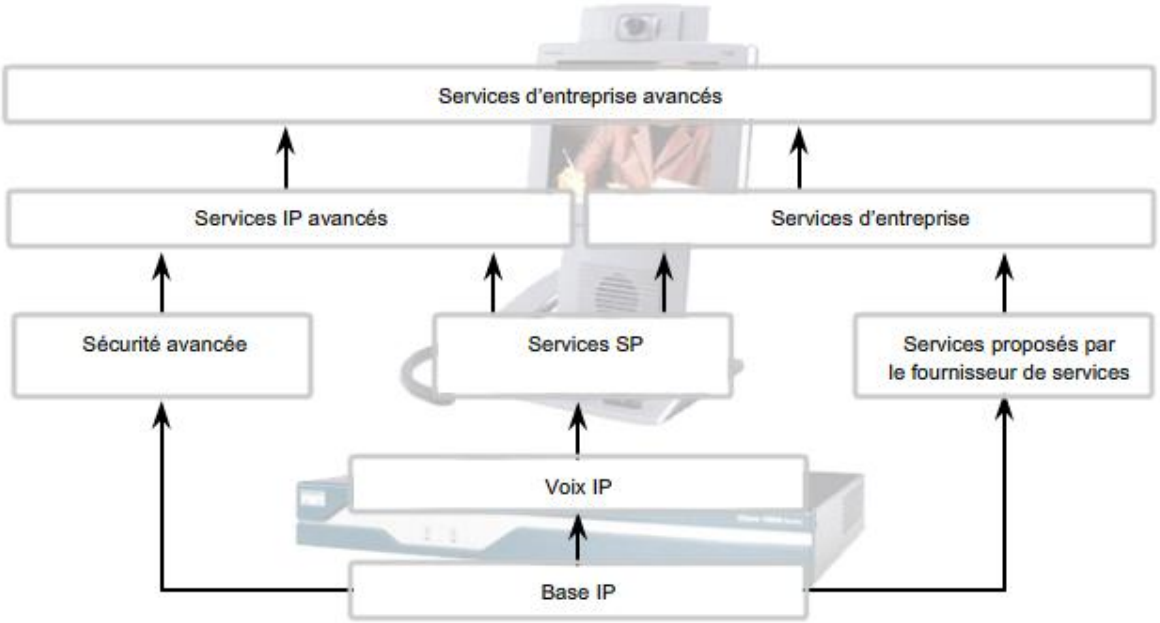
L'image logicielle Cisco IOS de base est appelée l'image de base IP. Le logiciel de base IP Cisco IOS prend en charge les petites et moyennes entreprises, ainsi que le routage entre réseaux.

D'autres images logicielles Cisco IOS ajoutent des services à l'image de base IP. Par exemple, l'image Advanced Security offre des fonctionnalités de sécurité avancée, telles que la création de réseaux privés et les pare-feu.

Un grand nombre de types et de versions d'images Cisco IOS sont disponibles. Ces images sont conçues pour fonctionner sur des modèles spécifiques de routeurs, de commutateurs et d'ISR.

Il est important de savoir quelle image et quelle version sont chargées sur un périphérique avant de commencer le processus de configuration.




## *1.2 <u>Configuration physique du routeur ISR</u>*

Chaque routeur ISR est fourni avec les câbles et la documentation nécessaires pour le mettre sous tension et commencer l'installation. À la réception d'un nouveau périphérique, il est nécessaire de le déballer et de vérifier que l'ensemble du matériel et de l'équipement est inclus.

Accessoires fournis avec chaque nouveau routeur à services intégrés Cisco 1841 :

- un câble console RJ-45 vers DB-9 ;
- un adaptateur modem DB-9 vers DB-25 ;
- un cordon d'alimentation ;
- la carte d'enregistrement du produit, appelée carte Cisco.com ;

- des informations de sécurité et de conformité aux réglementations (Regulatory Compliance and Safety Information) pour les routeurs Cisco 1841 ;
- un guide de démarrage rapide pour le gestionnaire SDM (Router and Security Device Manager) ;
- un guide de démarrage rapide (modulaire) pour les routeurs ISR de la gamme Cisco 1800.

L'installation d'un nouveau routeur ISR Cisco 1841 nécessite des outils et un équipement spéciaux que la plupart des FAI et ateliers techniques possèdent. Les éventuels équipements spécifiques supplémentaires requis dépendent du modèle du périphérique et le cas échéant des équipements optionnels commandés.

En général, les outils requis pour l'installation d'un nouveau périphérique sont les suivants :

- un PC avec un programme d'émulation de terminal, tel que HyperTerminal ;
- des attaches de câble et un tournevis cruciforme n° 2 ;
- des câbles pour les interfaces WAN, LAN et USB.

Vous devrez peut-être également disposer de l'équipement et des périphériques requis pour les réseaux WAN et les services de communication large bande, tels qu'un modem. En outre, vous devrez peut-être utiliser des commutateurs Ethernet pour connecter des périphériques LAN ou étendre la connectivité LAN, selon la disponibilité du module de commutateur intégré et le nombre de ports LAN requis.

Avant de procéder à l'installation d'un équipement, il est important de lire le guide de démarrage rapide du périphérique, ainsi que toute documentation fournie avec celui-ci. La documentation contient des informations importantes sur la sécurité et les procédures à suivre, qui permettent d'éviter tout dommage accidentel à l'équipement lors de l'installation

Pour mettre sous tension un routeur ISR 1841, procédez comme suit.

1. Fixez solidement le châssis ou le boîtier du périphérique et reliez-le à la terre.

**Étape 1 : montage et mise à la terre du châssis du périphérique de façon sécurisée**

Les routeurs et les routeurs à services intégrés de Cisco peuvent être fixés à un mur, placés sur une étagère ou un bureau, ou installés dans une armoire.

2. Mettez en place la carte Compact Flash externe.


**Étape 2 : insertion de la mémoire Compact Flash externe**

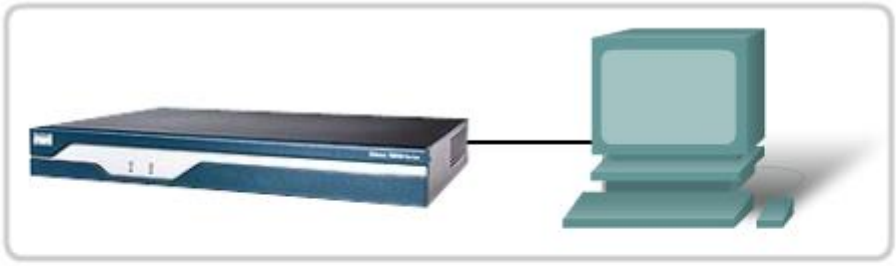
Introduisez la carte de mémoire Compact Flash externe dans son logement. Assurez-vous qu'elle est bien enfoncée et vérifiez que le bouton d'éjection est en positionnement correct. Le bouton d'éjection se trouve habituellement à gauche du logement.

3. Branchez le cordon d'alimentation.


**Étape 3 : connexion du câble d'alimentation**

Connectez le câble d'alimentation au périphérique, puis à une source d'alimentation fiable. Les routeurs et les périphériques réseau se connectent généralement à un système d'alimentation sans coupure équipé d'une batterie. Ceci permet d'éviter que le périphérique s'arrête en cas de panne de courant inopinée.

4. Configurez le logiciel d'émulation de terminal sur l'ordinateur et connectez ce dernier au port de console.



**Étape 4 : configuration du logiciel d'émulation de terminal et connexion de l'ordinateur au port de console**

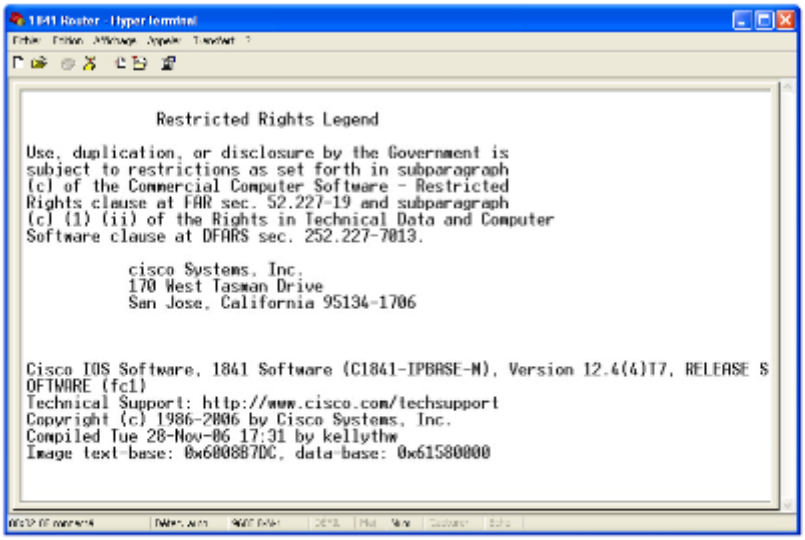
Sur un ordinateur, configurez les paramètres du logiciel d'émulation de terminal nécessaires pour communiquer avec un routeur Cisco. Connectez l'ordinateur qui exécute le programme d'émulation au port de console du routeur à services intégrés à l'aide du câble console fourni avec le périphérique.

5. Mettez le routeur sous tension.


**Étape 5 : mise sous tension du routeur**

Allumez le routeur à services intégrés à l'aide de l'interrupteur d'alimentation situé à l'arrière du périphérique.

6. Examinez les messages affichés sur l'ordinateur lors du démarrage du routeur.




**Étape 6 : examen des messages de démarrage**

Examinez les messages de démarrage qui s'affichent dans la fenêtre du programme d'émulation de terminal. Ces messages sont générés par le système d'exploitation du routeur.

### *1.3 Processus de démarrage*

Le processus de démarrage du routeur se compose de trois étapes :

1. Exécution du test automatique de mise sous tension (POST) et chargement du programme d'amorçage

Le test POST est un processus exécuté sur pratiquement tous les ordinateurs lors du démarrage. Il est utilisé pour tester le matériel du routeur. Une fois le test POST terminé, le programme d'amorçage est chargé.

2. Localisation et chargement du logiciel Cisco IOS

Le programme d'amorçage recherche le logiciel Cisco IOS et le charge dans la mémoire vive. Les fichiers Cisco IOS peuvent être situés à l'un des trois emplacements suivants : dans la mémoire flash, sur un serveur TFTP ou à un autre emplacement indiqué dans le fichier de configuration initiale.

**TFTP**

Trivial File Transfer Protocol

Norme qui permet de transférer des fichiers d'un ordinateur à un autre sur un réseau, généralement sans l'autorisation du client. Le protocole TFTP est la version simplifiée du protocole FTP.

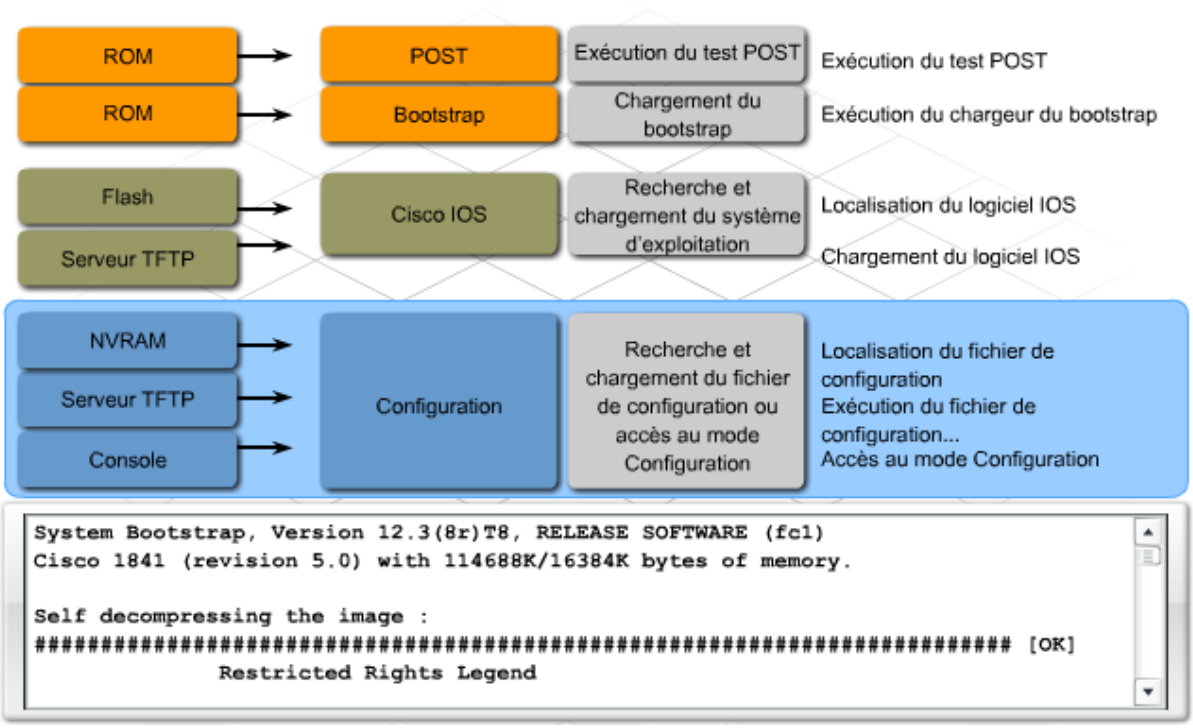
Par défaut, le logiciel Cisco IOS est chargé à partir de la mémoire flash. Vous devez modifier les paramètres de configuration pour le charger à partir d'un autre emplacement.

3. Localisation et exécution du fichier de configuration initiale ou passage en mode Configuration

Après le chargement du logiciel Cisco IOS, le programme d'amorçage recherche le fichier de configuration initiale dans la mémoire vive non volatile. Ce fichier contient les commandes et paramètres de configuration précédemment enregistrés, y compris les adresses d'interface, les informations de routage, les mots de passe et d'autres paramètres de configuration.

Si aucun fichier de configuration n'est détecté, le routeur invite l'utilisateur à passer en mode Configuration pour commencer le processus de configuration.

S'il détecte un fichier de configuration, le routeur le copie dans la mémoire vive et affiche une invite contenant le nom d'hôte. L'invite indique que le routeur a chargé correctement le logiciel Cisco IOS et le fichier de configuration.




Pour éviter toute perte de données, il est important de bien comprendre la différence entre le fichier de configuration initiale et le fichier de configuration en cours.

**Fichier de configuration initiale**

Le fichier de configuration initiale est le fichier de configuration enregistré qui définit les propriétés du périphérique à chaque mise sous tension de l'appareil. Ce fichier est stocké dans la mémoire vive non volatile (NVRAM), ce qui signifie qu'il est enregistré même lorsque le périphérique est éteint.

Lorsqu'un routeur Cisco est mis sous tension, il charge le logiciel Cisco IOS dans la mémoire de travail, c'est-à-dire la mémoire vive (RAM). Le fichier de configuration initiale est ensuite copié de la mémoire vive non volatile vers la mémoire vive. Lorsque le fichier de configuration initiale est chargé dans la mémoire vive, il devient alors la configuration en cours initiale.

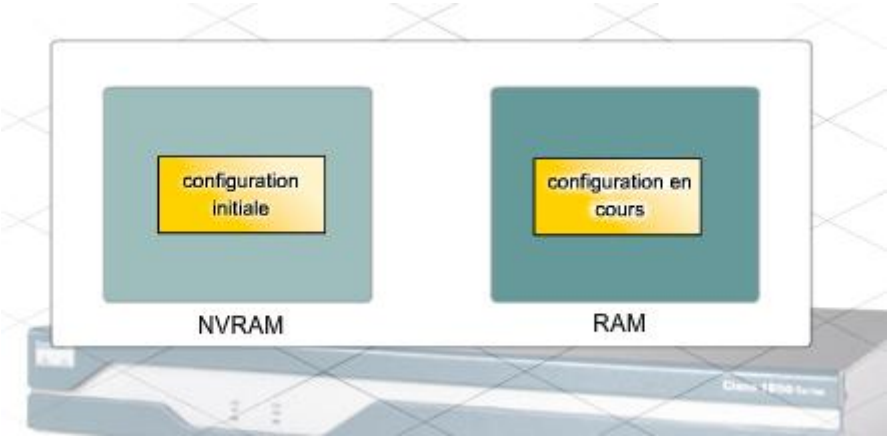
**Fichier de configuration en cours**

L'expression « configuration en cours » fait référence à la configuration actuelle en cours d'exécution dans la mémoire vive du périphérique. Ce fichier contient les commandes utilisées pour déterminer comment le périphérique fonctionne sur le réseau.

Le fichier de configuration en cours est stocké dans la mémoire vive du périphérique. Vous pouvez apporter des modifications à la configuration et aux divers paramètres du périphérique lorsque le fichier est dans la mémoire vive. Toutefois, la configuration en cours est perdue chaque fois que le périphérique est éteint, à moins de l'enregistrer dans le fichier de configuration initiale.

Les modifications apportées à la configuration en cours ne sont pas automatiquement enregistrées dans le fichier de configuration initiale. Vous devez copier manuellement la configuration en cours dans le fichier de configuration initiale.

Lorsque vous configurez un périphérique par le biais de l'interface de ligne de commande (ILC) Cisco, utilisez la commande **copy running-config startup-config**, ou sa version abréviée **copy run start**, pour enregistrer la configuration en cours dans le fichier de configuration initiale. Lorsque vous configurez un périphérique par le biais de l'interface graphique utilisateur du gestionnaire Cisco SDM, le gestionnaire offre l'option d'enregistrer la configuration en cours du routeur dans le fichier de configuration initiale à chaque exécution d'une commande.

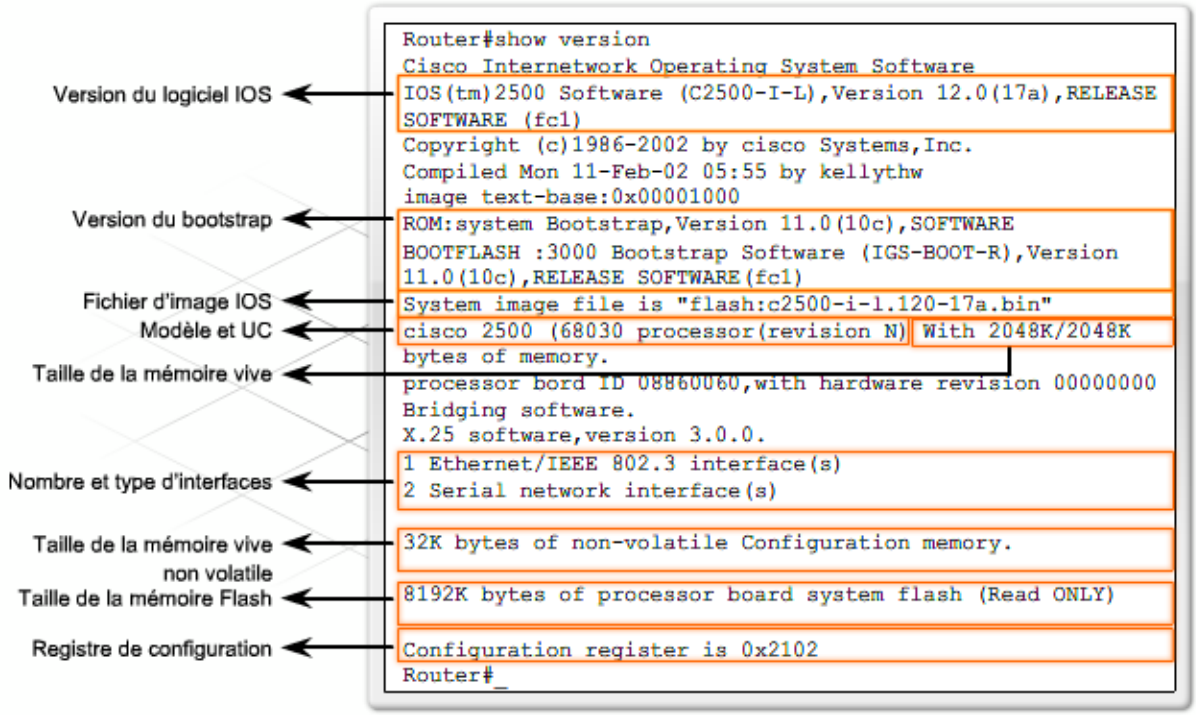



Une fois le fichier de configuration initiale chargé et le routeur démarré correctement, vous pouvez utiliser la commande **show version** pour vérifier et dépanner certains composants matériels et logiciels de base utilisés au cours du processus de démarrage. Les résultats de la commande **show version** comprennent les éléments suivants :

- la version du logiciel Cisco IOS utilisé ;

- la version du logiciel d'amorçage système stocké dans la mémoire ROM qui a été utilisé pour démarrer le routeur ;
- le nom de fichier complet de l'image Cisco IOS et l'emplacement auquel le programme d'amorçage l'a recherchée ;
- le type d'UC utilisée sur le routeur et la taille de la mémoire vive. Vous devrez peut-être mettre à niveau la taille de la mémoire vive lors de la mise à niveau du logiciel Cisco IOS ;
- le nombre et le type d'interfaces physiques sur le routeur ;
- la taille de la mémoire vive non volatile (NVRAM). Celle-ci est utilisée pour stocker le fichier de configuration initiale ;
- la taille de la mémoire flash du routeur. La mémoire flash est utilisée pour stocker l'image Cisco IOS de façon permanente. Vous devrez peut-être mettre à niveau la taille de la mémoire flash lors de la mise à niveau du logiciel Cisco IOS ;
- la valeur configurée actuelle du registre de configuration du logiciel, en nombres hexadécimaux.

Le registre de configuration indique au routeur comment démarrer. Par exemple, le paramètre d'usine par défaut pour le registre de configuration est 0x2102. Cette valeur indique que le routeur tente de charger une image du logiciel Cisco IOS à partir de la mémoire flash et essaie de charger le fichier de configuration initiale à partir de la mémoire vive non volatile. Il est possible de modifier le registre de configuration et, par conséquent, de modifier l'emplacement auquel le routeur recherche l'image Cisco IOS et le fichier de configuration initiale au cours du processus de démarrage. S'il existe une deuxième valeur entre parenthèses, celle-ci indique la valeur du registre de configuration à utiliser au cours du prochain rechargement du routeur.




Dans certains cas, le routeur ne démarre pas correctement. Ceci peut être dû à plusieurs facteurs, notamment un fichier Cisco IOS manquant ou endommagé, un emplacement incorrect de l'image Cisco IOS spécifié par le registre de configuration ou une mémoire insuffisante pour charger une nouvelle image Cisco IOS. Si le routeur ne peut pas démarrer le

logiciel IOS, il démarre en mode ROM monitor (ROMmon). Le logiciel ROMmon est un simple jeu de commandes stocké en mémoire morte (ROM) qui peut être utilisé pour résoudre les erreurs de démarrage et récupérer le routeur lorsque le logiciel IOS n'est pas disponible.

Lorsque le routeur démarre en mode ROMmon, l'une des premières procédures de dépannage consiste à examiner la mémoire flash pour rechercher une image valide à l'aide de la commande **dir flash:** . Si la commande trouve une image, tentez de démarrer cette dernière à l'aide de la commande **boot flash:**.

rommon 1>**boot flash:c2600-is-mz.121-5**

Si le routeur démarre correctement avec cette commande, il existe deux raisons possibles pour lesquelles l'image Cisco IOS ne s'est pas chargée initialement à partir de la mémoire flash. Tout d'abord, utilisez la commande **show version** pour vérifier le registre de configuration afin de vous assurer qu'il est configuré pour la séquence de démarrage par défaut. Si la valeur du registre de configuration est correcte, utilisez la commande **show startup-config** pour vérifier s'il existe une commande **bootsystem** indiquant au routeur d'utiliser un autre emplacement pour l'image Cisco IOS.

```
router#show startup-config
Building configuration...

Current configuration : 1450 bytes
!
version 12.4
!
hostname router
!
boot-start-marker
boot system flash 1841-advipservicesk9-mz.124-10b.bin
boot system tftp 1841-advipservicesk9-mz.124-10b.bin 192.168.1.1
boot system rom
boot-end-marker
!
<résultat omis>
```

**Travaux pratiques** : Mettez sous tension un routeur ISR et affichez les fichiers système et de configuration du routeur à l'aide de commandes show.

### *1.4 Programmes Cisco IOS*

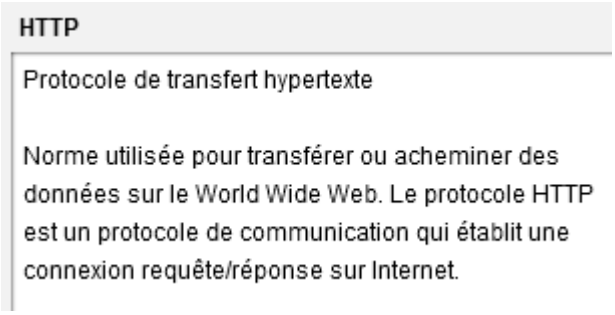
Deux méthodes sont possibles pour connecter un PC à un périphérique réseau en vue d'effectuer des tâches de configuration et de surveillance : la gestion hors bande et intrabande.

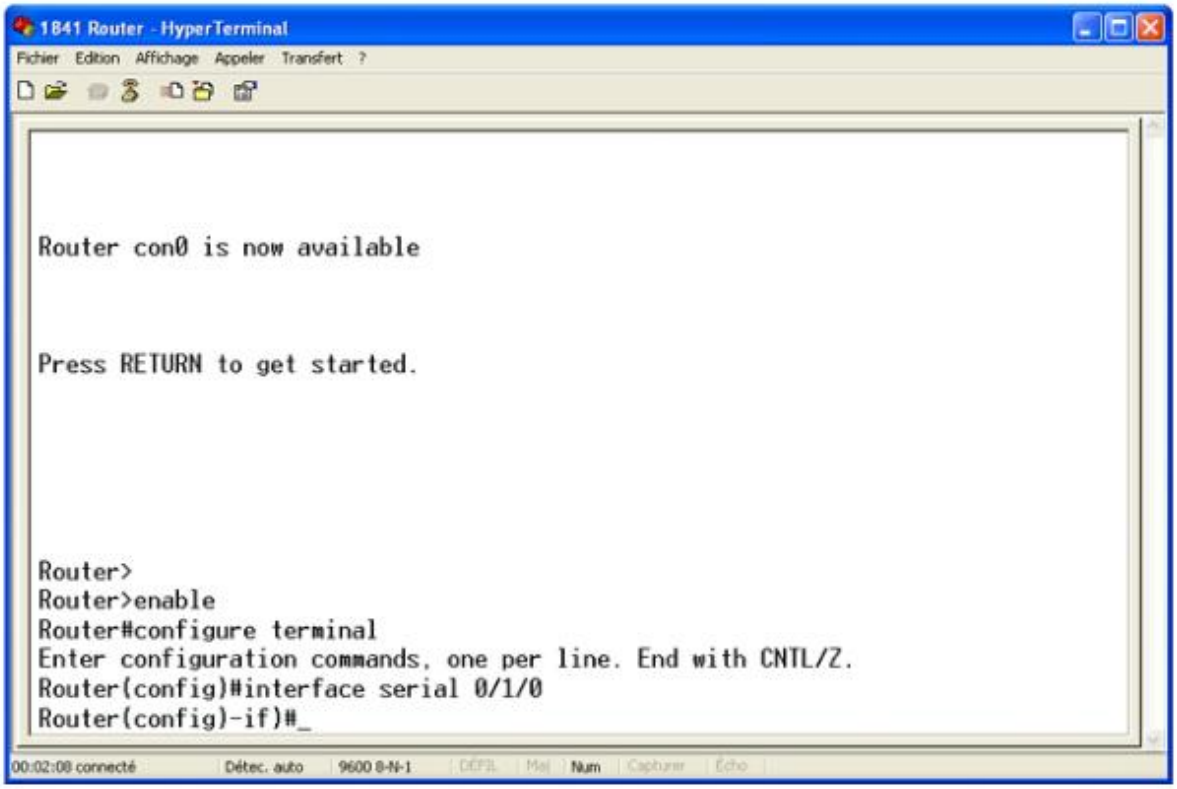
**Gestion hors bande**

Pour la gestion hors bande, un ordinateur doit être directement connecté au port de console ou au port auxiliaire (AUX) du périphérique réseau à configurer. Ce type de connexion ne nécessite pas que les connexions de réseau local sur le périphérique soient actives. Les techniciens utilisent la gestion hors bande pour la configuration initiale d'un périphérique réseau car, tant que celui-ci n'est pas correctement configuré, il ne peut pas prendre part au réseau. La gestion hors bande est également utile lorsque la connectivité réseau ne fonctionne pas correctement et qu'il est impossible d'accéder au périphérique sur le réseau. L'exécution de tâches de gestion hors bande nécessite un client d'émulation de terminal installé sur le PC.

**Gestion intrabande**

La gestion intrabande permet de surveiller un périphérique réseau sur une connexion réseau et d'en modifier la configuration. Pour qu'un ordinateur soit connecté au périphérique et en mesure de réaliser des tâches de gestion intrabande, au moins une interface réseau sur le périphérique doit être connectée au réseau et fonctionner correctement. Vous pouvez utiliser Telnet, HTTP ou SSH pour accéder à un périphérique Cisco pour la gestion intrabande. Un navigateur Web ou un programme client Telnet peuvent être utilisés pour surveiller le périphérique réseau ou modifier sa configuration.






L'interface de ligne de commande (ILC) Cisco IOS est un programme de type texte qui permet d'entrer et d'exécuter des commandes Cisco IOS pour configurer, surveiller et maintenir les périphériques Cisco. L'interface de ligne de commande Cisco peut être utilisée pour les tâches de gestion intrabande ou hors bande.

Utilisez les commandes de l'ILC pour modifier la configuration du périphérique et afficher l'état actuel des processus sur le routeur. Pour les utilisateurs expérimentés, l'ILC offre de nombreuses fonctionnalités permettant d'économiser du temps lors de la création de configurations tant simples que complexes. Pratiquement tous les périphériques réseau Cisco utilisent la même interface de ligne de commande. À la fin de la séquence de mise sous tension du routeur, lorsque l'invite Router> s'affiche, vous pouvez utiliser l'ILC pour entrer des commandes Cisco IOS.

Les techniciens qui maîtrisent les commandes et le fonctionnement de l'ILC peuvent surveiller et configurer facilement un vaste éventail de périphériques réseau. L'ILC comprend un système d'aide détaillé offrant aux utilisateurs une assistance lors de la configuration et de la surveillance des périphériques.


Outre l'interface de ligne de commande Cisco IOS, divers outils sont disponibles pour aider à la configuration d'un routeur ou d'un routeur à services intégrés (ISR) Cisco. Le gestionnaire SDM (Security Device Manager) est un outil Web de gestion des périphériques offrant une interface graphique utilisateur. Contrairement à l'interface de ligne de commande, le gestionnaire SDM peut être utilisé uniquement pour les tâches de gestion intrabande.

Le gestionnaire SDM Express simplifie la configuration initiale du routeur. Il adopte une approche pas à pas pour créer, rapidement et facilement, une configuration de base de routeur.

La version complète du gestionnaire SDM offre des options plus avancées, telles que :

- configuration de connexions LAN et WAN supplémentaires ;
- création de pare-feu ;
- configuration de connexions VPN ;
- exécution de tâches de sécurité.

Le gestionnaire SDM prend en charge la plupart des versions du logiciel Cisco IOS et est disponible gratuitement sur de nombreux routeurs Cisco. Il est préinstallé sur la mémoire Flash du routeur à services intégrés de la gamme Cisco 1800. Si le gestionnaire SDM est installé sur le routeur, il est recommandé de l'utiliser pour effectuer la configuration initiale du routeur. Celle-ci est effectuée en accédant au routeur via un port réseau prédéfini sur le routeur.

| | ICL Cisco IOS | Cisco SDM |
|---|---|---|
| Interface utilisateur | • Logiciel d'émulation de terminal<br>• Session Telnet | Navigateur Web |
| Méthode de configuration de routeur | Commandes texte Cisco | Boutons et zones de texte de l'interface graphique utilisateur |
| Expertise en configuration de périphériques Cisco | En fonction de la tâche de configuration | Aucune connaissance des commandes ILC requise |
| Fonctions d'aide | À invite de commandes | Aide et didacticiels en ligne avec interface graphique utilisateur |
| Configuration requise pour la mémoire Flash du routeur | Couvert par l'image IOS | 6 Mo de mémoire disponible |
| Disponibilité | Tous périphériques Cisco | Gammes Cisco 830 à Cisco 7301 |
| En utilisation | • Cisco SDM non pris en charge par le périphérique Cisco<br>• Tâche de configuration non prise en charge par Cisco SDM | • Exécution de la configuration initiale sur un périphérique équipé de SDM<br>• Configuration des périphériques pas à pas sans connaissance préalable nécessaire de l'ILC |

Les périphériques Cisco ne prennent pas tous en charge le gestionnaire SDM. Par ailleurs, SDM ne prend pas en charge toutes les commandes disponibles via l'interface de ligne de commande. En conséquence, il est parfois nécessaire d'utiliser l'ILC pour terminer la configuration d'un périphérique que vous avez commencée à l'aide du gestionnaire SDM. Il est essentiel de se familiariser avec les deux méthodes afin d'assurer une prise en charge efficace des périphériques Cisco.

**Exercice**

Déterminez quand utiliser l'interface de ligne de commande (ILC) ou le gestionnaire SDM.

Selon la description, cochez ILC ou SDM.

| | ILC | SDM |
|---|---|---|
| 1. Pour configurer un routeur Cisco avec la gestion intrabande et la gestion hors bande | | |
| 2. Pour la configuration initiale d'un routeur Cisco au moyen d'une interface graphique utilisateur basée sur le Web | | |
| 3. Pour configurer un routeur Cisco sans bien connaître les commandes IOS | | |
| 4. Pris en charge par défaut sur tous les routeurs Cisco IOS | | |

Corrigé

| | ILC | SDM |
|---|---|---|
| 1. Pour configurer un routeur Cisco avec la gestion intrabande et la gestion hors bande | ✓ | |
| 2. Pour la configuration initiale d'un routeur Cisco au moyen d'une interface graphique utilisateur basée sur le Web | | ✓ |
| 3. Pour configurer un routeur Cisco sans bien connaître les commandes IOS | | ✓ |
| 4. Pris en charge par défaut sur tous les routeurs Cisco IOS | ✓ | |

# 2 Utilisation de Cisco SDM Express et SDM

## *2.1 Cisco SDM Express*

Lors de l'ajout d'un nouveau périphérique à un réseau, il est essentiel de vérifier que le périphérique fonctionne correctement. L'ajout d'un périphérique mal configuré peut provoquer la défaillance du réseau entier.

La configuration d'un périphérique réseau tel qu'un routeur peut être une tâche complexe, quel que soit l'outil utilisé pour définir la configuration. Par conséquent, respectez toujours les méthodes recommandées pour l'installation d'un nouveau périphérique afin de garantir que tous ses paramètres sont correctement configurés et documentés.

| Méthode recommandée | Détails |
|---|---|
| 1. Procurez-vous puis documentez toutes les informations avant de commencer la configuration. | • Nom affecté au périphérique<br>• Emplacement où il sera installé<br>• Noms d'utilisateur et mots de passe<br>• Type des connexions requises (réseaux local et étendu)<br>• Informations d'adresse IP pour toutes les interfaces du réseau, à savoir adresse IP, masque de sous-réseau et passerelle par défaut<br>• Paramètres DHCP du réseau<br>• Paramètres de traduction d'adresses de réseau (NAT)<br>• Paramètres du pare-feu |
| 2. Créez un schéma de réseau montrant le branchement des câbles. | • Indiquez dans le schéma les désignations des interfaces et les informations d'adresses. |
| 3. Créez une liste de contrôle des étapes de configuration. | • Cochez chaque étape lorsqu'elle a été correctement exécutée. |
| 4. Vérifiez la configuration à l'aide d'un simulateur de réseau. | • Faites un test avant le placement sur le réseau en production. |
| 5. Actualisez la documentation du réseau, puis conservez-en un exemplaire en lieu sûr. | • Enregistrement sur un serveur<br>• Impression et conservation dans un classeur |

Le gestionnaire Cisco SDM Express est un outil intégré à l'outil Cisco Router and Security Device Manager (SDM) pour faciliter la création d'une configuration de routeur de base. Pour utiliser SDM Express, commencez par connecter par câble Ethernet la carte réseau de l'ordinateur au port Ethernet spécifié dans le guide de démarrage du routeur ou du routeur à services intégrés à configurer.

SDM Express utilise les huit écrans de configuration suivants pour faciliter la création d'une configuration de routeur de base :

- Overview (Vue d'ensemble)
- Basic Configuration (Configuration de base)
- LAN IP Address (Adresse IP du réseau local)
- DHCP
- Internet (WAN)
- Firewall (Pare-feu)
- Security Settings (Paramètres de sécurité)
- Summary (Résumé)

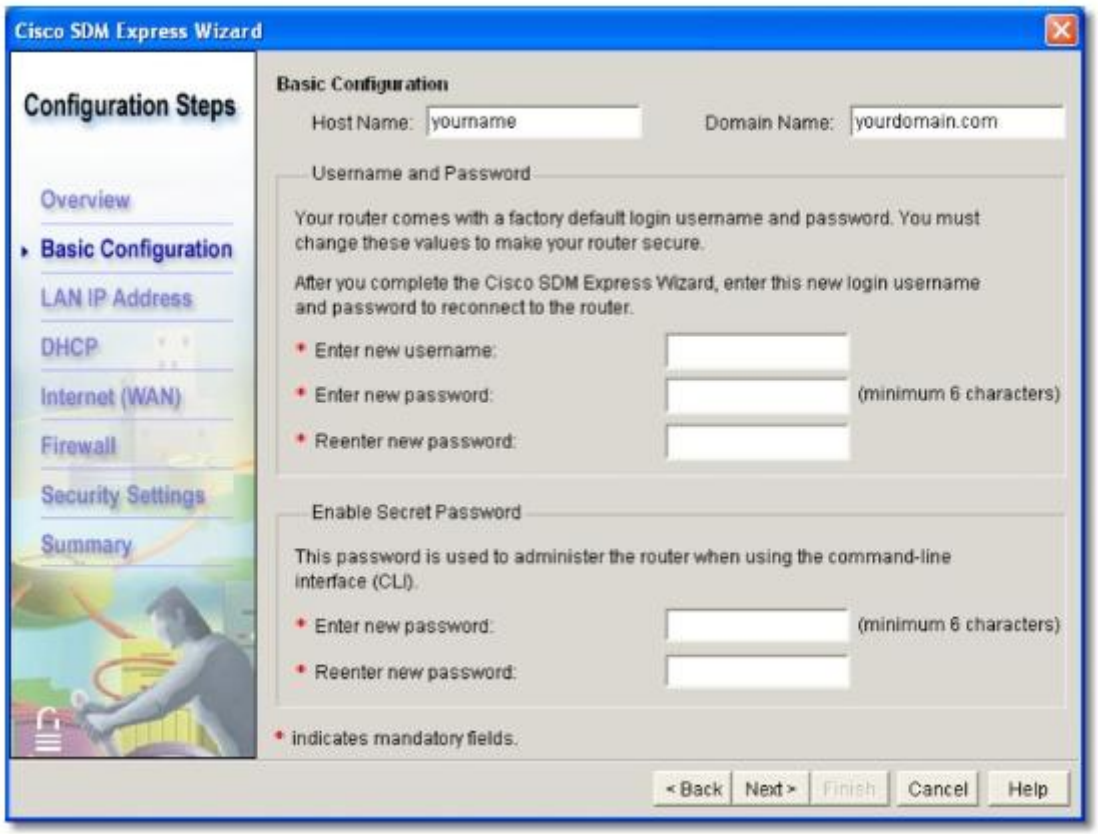
L'interface graphique utilisateur SDM Express fournit des instructions pas à pas pour créer la configuration initiale du routeur. Une fois la configuration initiale terminée, le routeur est disponible sur le réseau local. La configuration du routeur peut également comprendre une

connexion de réseau étendu (WAN), un pare-feu et jusqu'à 30 fonctionnalités améliorées de sécurité.

## *2.2 Options de configuration du gestionnaire SDM Express*

L'écran de configuration de base SDM Express comprend des paramètres de base pour le routeur à configurer. Les informations suivantes sont requises :

- **Host name** - Nom d'hôte attribué au routeur à configurer.
- **Domain Name** - Nom de domaine de l'organisation ; cisco.com est un exemple de nom de domaine, mais les noms de domaine peuvent se terminer par un autre suffixe, comme .org ou .net.
- **Username and Password** - Nom d'utilisateur et mot de passe utilisés pour accéder au gestionnaire SDM Express afin de configurer et de surveiller le routeur. Le mot de passe doit contenir au moins six caractères.
- **Enable Secret Password** - Mot de passe secret actif ; il contrôle l'accès utilisateur au routeur, qui permet de modifier la configuration à l'aide de l'interface de ligne de commande, de Telnet ou de ports de console. Le mot de passe doit contenir au moins six caractères.

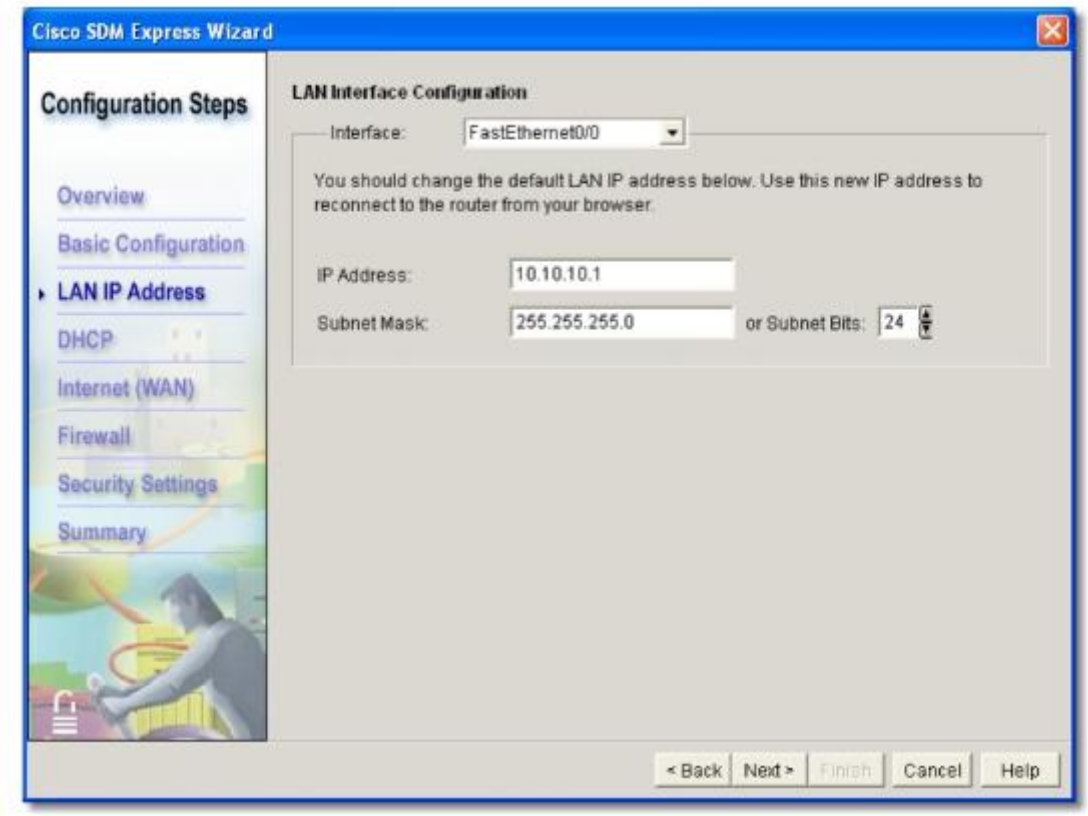



Les paramètres de configuration LAN permettent à l'interface du routeur de prendre part au réseau local connecté.

- **IP address** - Adresse IP de l'interface LAN au format décimal avec points de séparation. Il peut s'agir d'une adresse IP privée si le périphérique est installé sur un réseau qui utilise la traduction d'adresses de réseau (NAT) ou la traduction d'adresses de port (PAT).

Il est important de noter cette adresse car lors du redémarrage du routeur, c'est cette adresse, et non celle fournie dans le guide de démarrage rapide, qui est utilisée pour accéder au gestionnaire SDM Express.

- **Subnet mask** - Masque de sous-réseau, qui identifie la partie réseau de l'adresse IP.
- **Subnet bits** - Bits de sous-réseau : nombre de bits utilisés pour définir la partie réseau de l'adresse IP. Le nombre de bits peut être utilisé à la place du masque de sous-réseau.
- **Wireless parameters** - Paramètres sans fil (facultatifs) : ils s'affichent si le routeur a une interface sans fil et que l'option Yes (Oui) a été sélectionnée dans la fenêtre de configuration de cette interface. Ils spécifient le SSID du réseau sans fil.




Le protocole DHCP constitue une méthode simple d'affecter des adresses IP à des périphériques hôtes. Ce protocole affecte dynamiquement une adresse IP à un hôte du réseau lors de sa mise sous tension et la récupère ensuite à sa mise hors tension. Ceci permet de réutiliser les adresses lorsque les hôtes n'en ont plus besoin. À l'aide de SDM Express, vous pouvez configurer un routeur comme serveur DHCP pour affecter des adresses à des périphériques tels que des PC sur le réseau local interne.

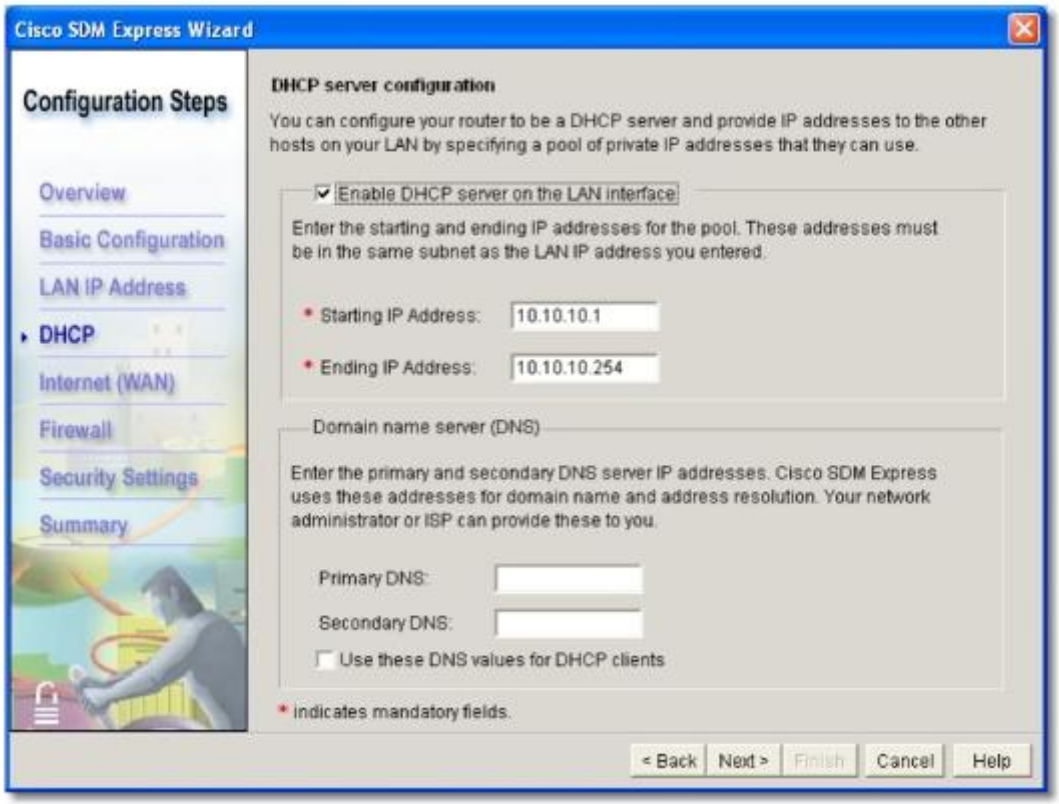
Pour configurer un périphérique pour le protocole DHCP, activez la case à cocher **Enable DHCP Server on the LAN Interface**. L'activation de cette case à cocher permet au routeur

d'affecter des adresses IP privées à des périphériques sur le réseau local. Les adresses IP sont louées aux hôtes pour une durée d'un jour.

Le protocole DHCP utilise une plage d'adresses IP autorisées. Par défaut, la plage d'adresses valides est basée sur l'adresse IP et le masque de sous-réseau entrés pour l'interface LAN.

L'adresse IP de départ (Starting IP Address) est l'adresse la moins élevée de la page d'adresses IP. L'adresse IP de départ peut être modifiée, mais elle doit être sur le même réseau ou sous-réseau que l'interface de réseau local.

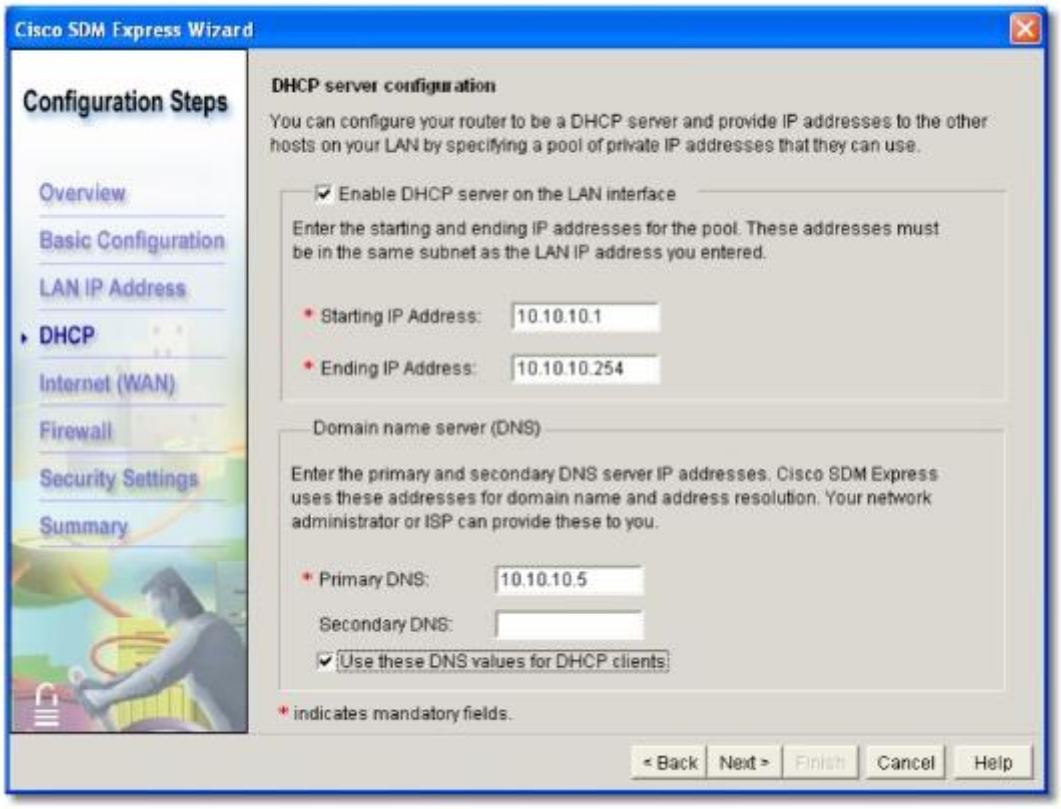
L'adresse IP la plus élevée (Ending IP Address) peut être modifiée pour réduire la taille du pool. Elle doit être sur le même réseau que l'adresse IP de départ.




Les paramètres de configuration DHCP supplémentaires comprennent :

- **Domain name** - Nom de domaine de l'organisation, attribué aux hôtes dans le cadre de la configuration DHCP.
- **Primary DNS** - Adresse IP du serveur DNS principal, utilisée pour résoudre les URL et les noms sur le réseau.
- **Secondary DNS** - Adresse IP d'un serveur DNS secondaire, si elle est disponible. Cette adresse est utilisée si le serveur DNS principal ne répond pas.

L'activation de la case à cocher **Use these DNS values for DHCP clients** permet au serveur DHCP d'attribuer les paramètres DNS configurés aux clients DHCP. Cette option est disponible si un serveur DHCP a été activé sur l'interface de réseau local.




Exercice

Identifiez les paramètres de configuration dans SDM Express.

Faites glisser le paramètre de configuration vers l'information à saisir.

Adresse IP de départ

Nom d'hôte

Nom de domaine

Mot de passe secret actif

Adresse du serveur DNS secondaire

Bits de sous-réseau

Adresse du serveur DNS principal

| Paramètre | Information |
|---|---|
| | Adresse IP du serveur à utiliser pour résoudre le nom si le premier serveur configuré n'est pas disponible |
| | Nom enregistré attribué à l'entreprise, par exemple cisco.com. |
| | Nom attribué à un périphérique par un administrateur. |
| | Contrôle l'accès des utilisateurs pour toute modification de la configuration via Telnet ou la console. |
| | Adresse IP du premier serveur que les hôtes peuvent utiliser pour résoudre les noms. |
| | Première adresse IP de la plage affectée aux hôtes par le serveur DHCP. |
| | Désigne la portion de l'adresse IP qui représente le réseau et le sous-réseau. |

## Corrigé

| Paramètre | Information |
|---|---|
| Adresse du serveur DNS secondaire | Adresse IP du serveur à utiliser pour résoudre le nom si le premier serveur configuré n'est pas disponible |
| Nom de domaine | Nom enregistré attribué à l'entreprise, par exemple cisco.com. |
| Nom d'hôte | Nom attribué à un périphérique par un administrateur. |
| Mot de passe secret actif | Contrôle l'accès des utilisateurs pour toute modification de la configuration via Telnet ou la console. |
| Adresse du serveur DNS principal | Adresse IP du premier serveur que les hôtes peuvent utiliser pour résoudre les noms. |
| Adresse IP de départ | Première adresse IP de la plage affectée aux hôtes par le serveur DHCP. |
| Bits de sous-réseau | Désigne la portion de l'adresse IP qui représente le réseau et le sous-réseau. |

## *2.3 Configuration des connexions WAN à l'aide de SDM Express*

### Configuration d'une connexion Internet (WAN)

Vous pouvez utiliser une connexion série pour relier des réseaux géographiquement éloignés. Ces interconnexions de réseaux étendus (WAN) requièrent un fournisseur de services de télécommunications (FST).

Les connexions série sont généralement des liaisons à plus faible débit que les liaisons Ethernet et nécessitent une configuration supplémentaire. Avant de configurer la connexion, déterminez le type de connexion et d'encapsulation de protocole requis.

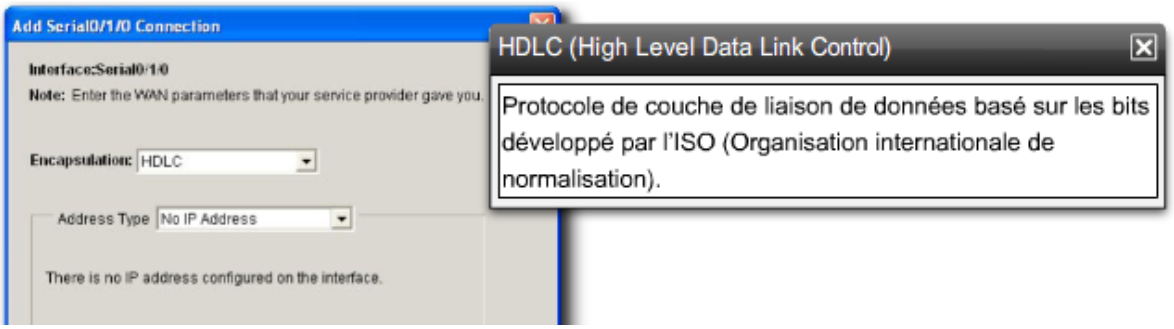
**encapsulation**

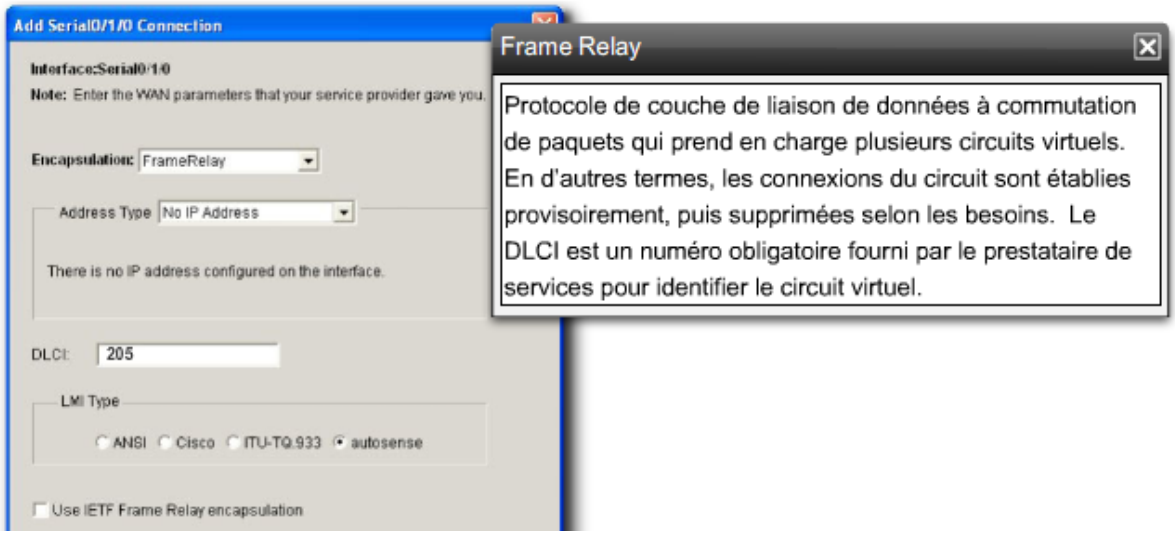
Transmission d'un protocole réseau au sein d'un autre protocole. Avec la transmission tunnel, un paquet de données est encapsulé dans un nouveau paquet conforme aux protocoles utilisés sur les réseaux intermédiaires. La transmission tunnel est la base de systèmes de sécurité IP tels qu'IPsec sur les réseaux privés virtuels.

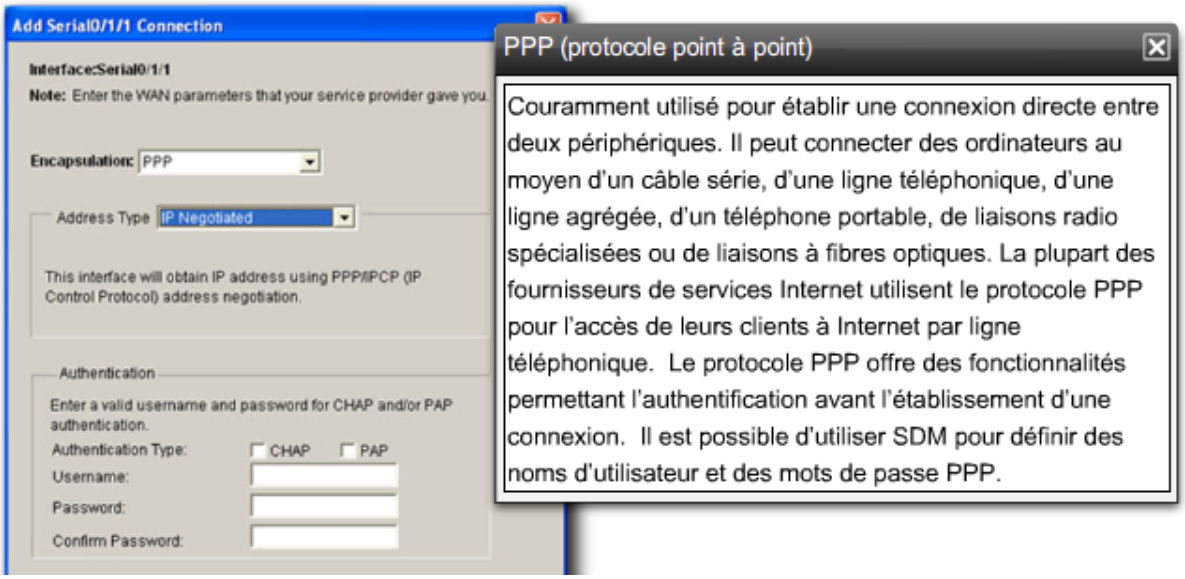
L'encapsulation de protocole doit être identique des deux côtés d'une connexion série. Pour être configurés, certains types d'encapsulation nécessitent des paramètres d'authentification, tels que le nom d'utilisateur et le mot de passe. Les types d'encapsulation incluent :

- HDLC (High Level Data Link Control)

- Frame Relay
- PPP (protocole point à point)



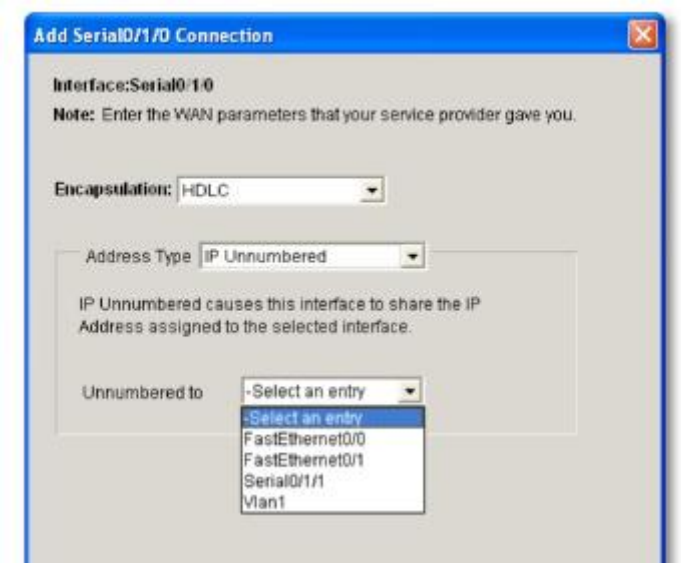




La fenêtre de configuration WAN contient des paramètres WAN supplémentaires.

**Address Type (Liste de types d'adresses)**

Selon le type d'encapsulation sélectionné, différentes méthodes sont disponibles pour obtenir une adresse IP pour l'interface série :

- **Static IP address** - Adresse IP statique, disponible avec les types d'encapsulation Frame Relay, PPP et HDLC. Pour configurer une adresse IP statique, entrez l'adresse IP et le masque de sous-réseau.
- **IP Unnumbered** - Adresse IP non numérotée : définit l'adresse de l'interface série pour correspondre à l'adresse IP de l'une des autres interfaces fonctionnelles du routeur. Disponible avec les types d'encapsulation Frame Relay, PPP et HDLC.
- **IP Negotiated** - Adresse IP négociée : le routeur obtient une adresse IP automatiquement par le biais du protocole PPP.
- **Easy IP (IP Negotiated)** - Adresse IP négociée : le routeur obtient une adresse IP automatiquement par le biais du protocole PPP.




# **Travaux pratiques** : Configuration d'un routeur ISR à l'aide de Cisco SDM Express

## *2.4 Configuration de la fonction NAT à l'aide de Cisco SDM*

Vous pouvez utiliser Cisco SDM Express ou Cisco SDM pour configurer un routeur.

Le gestionnaire SDM prend en charge un grand nombre des fonctionnalités prises en charge par SDM Express, mais il offre en outre d'autres options de configuration avancées. Pour cette raison, de nombreux utilisateurs font appel au gestionnaire SDM une fois la configuration de base du routeur effectuée à l'aide de SDM Express. Par exemple, vous devez utiliser le gestionnaire SDM pour activer la traduction d'adresses de réseau (NAT).

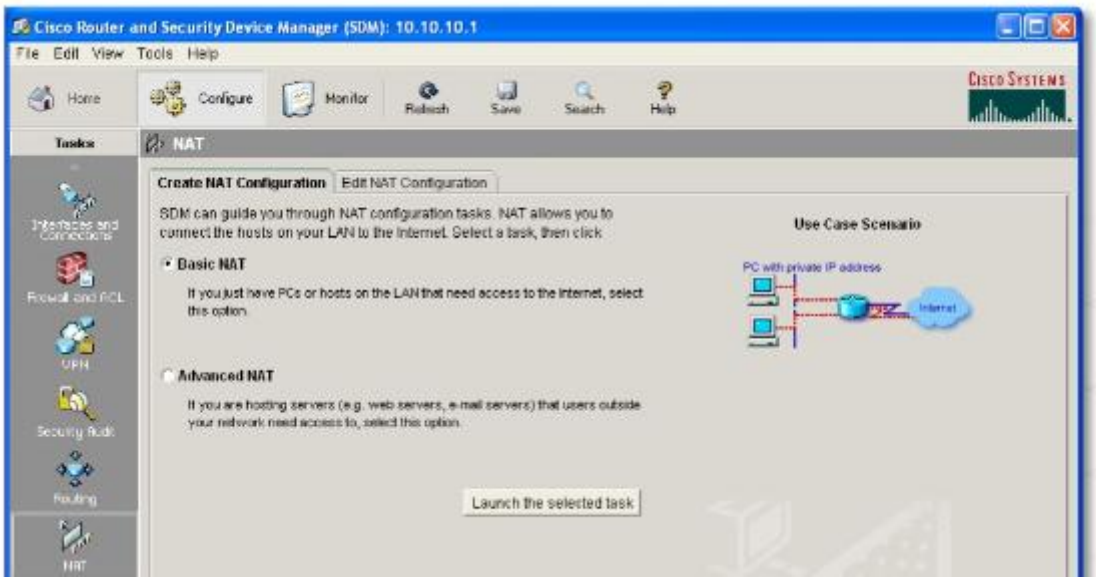
L'assistant Basic NAT Wizard configure la traduction d'adresses de réseau dynamique (Dynamic NAT) avec la traduction d'adresses de port (PAT) par défaut. La fonctionnalité

PAT permet aux hôtes sur le réseau local interne de partager l'adresse IP enregistrée attribuée à l'interface WAN. Ceci permet aux hôtes ayant des adresses privées internes d'avoir accès à Internet.

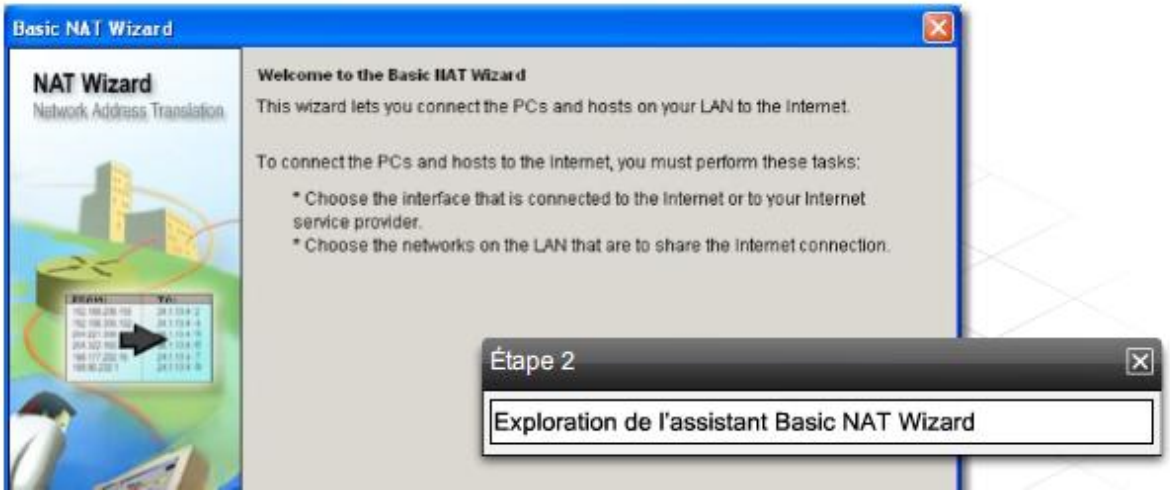
Seules les adresses d'hôtes incluses dans les plages d'adresses internes spécifiées dans la configuration SDM sont traduites. Il est important de vérifier que toutes les plages d'adresses qui nécessitent l'accès Internet sont incluses.

Les étapes de configuration de la fonction NAT comprennent :

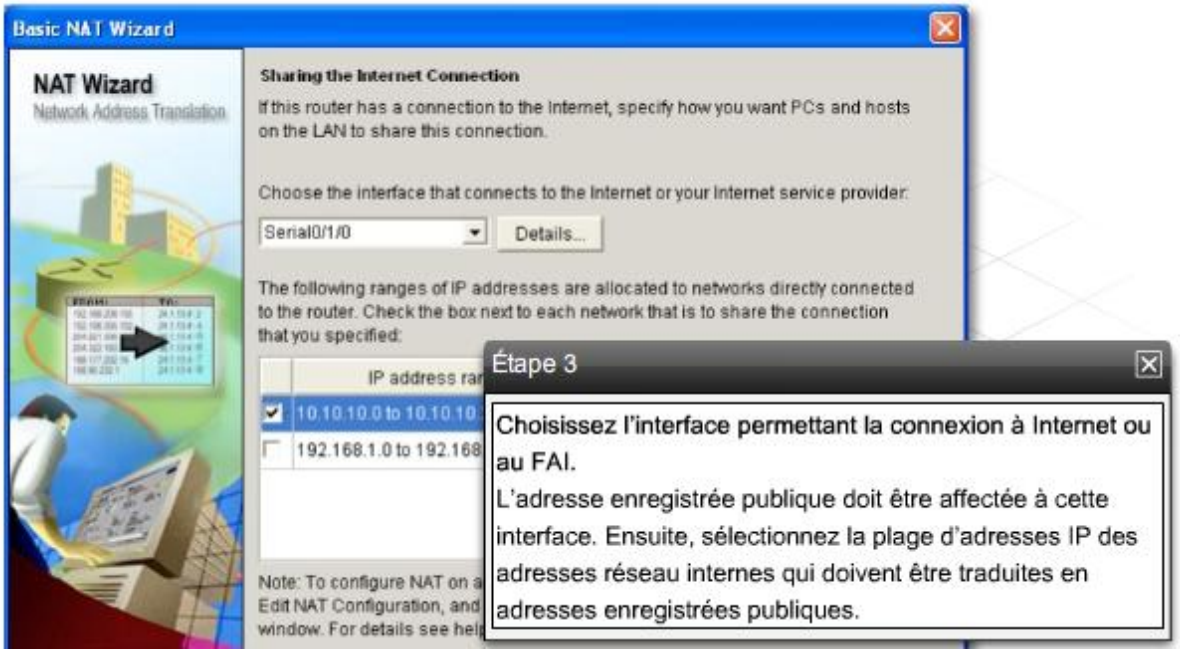
**Étape 1.** Activation de la configuration NAT à l'aide du gestionnaire SDM



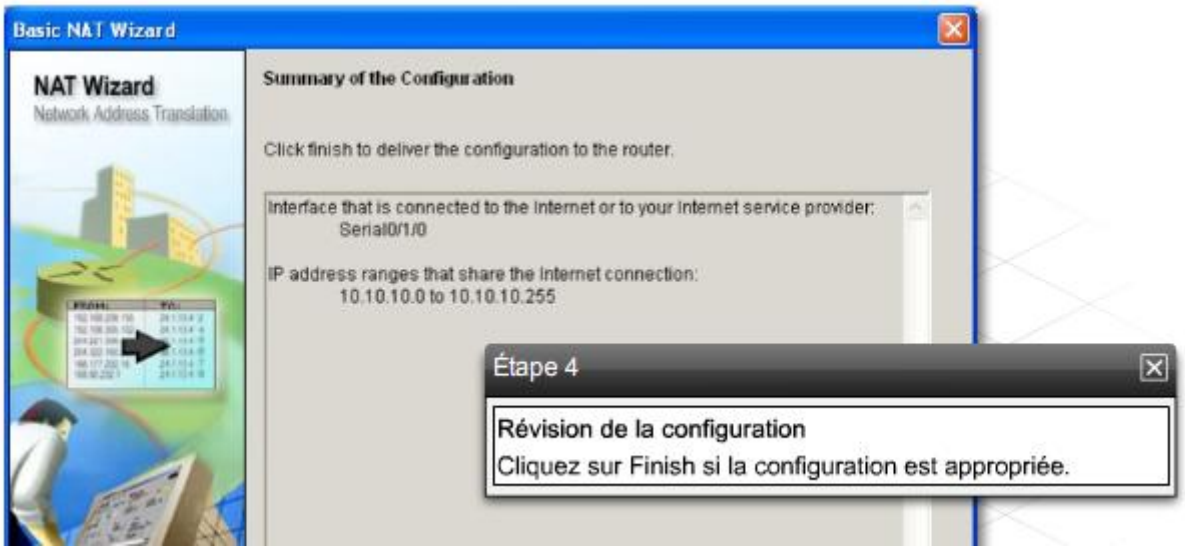

**Étape 2.** Exploration de l'assistant Basic NAT Wizard



**Étape 3.** Sélection de l'interface et définition des plages IP




**Étape 4.** Révision de la configuration




**Travaux pratiques:** Configurez la fonctionnalité NAT dynamique à l'aide de l'assistant Basic NAT Wizard du gestionnaire Cisco SDM.

# 3 Configuration d'un routeur à l'aide de l'interface de ligne de commande IOS

## *3.1 Modes d'interface de ligne de commande*

L'utilisation de l'interface de ligne de commande (ILC) Cisco IOS pour configurer et surveiller un périphérique diffère sensiblement de l'utilisation du gestionnaire SDM. L'ILC ne fournit pas d'assistance pas à pas pour la configuration et requiert par conséquent une planification et une expertise plus étendues.

**Modes de commande de l'ILC**

Le logiciel Cisco IOS prend en charge deux niveaux d'accès à l'interface de ligne de commande : le mode d'exécution utilisateur et le mode d'exécution privilégié.

Lorsqu'un routeur ou tout autre périphérique Cisco IOS est mis sous tension, le niveau d'accès par défaut est le mode d'exécution utilisateur. Ce mode est indiqué par l'invite de ligne de commande suivante :

**Router>**

Les commandes pouvant être exécutées en mode d'exécution utilisateur sont limitées à l'obtention d'informations sur le fonctionnement du périphérique et au dépannage à l'aide de commandes **show** et des utilitaires ping et traceroute.

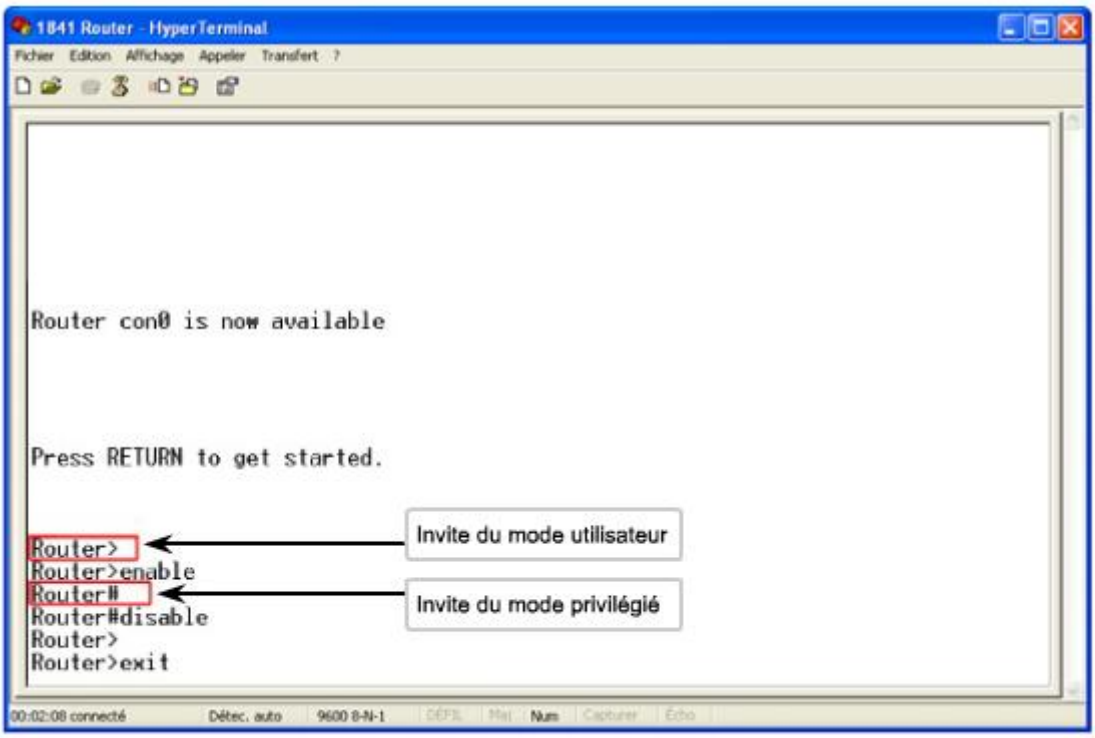
Pour entrer des commandes visant à modifier le fonctionnement du périphérique, vous devez disposer d'un accès de niveau privilégié. Activez le mode d'exécution privilégié en entrant **enable** à l'invite de commandes et en appuyant sur Entrée.

L'invite de ligne de commande change pour refléter le changement de mode d'accès. L'invite du mode d'exécution privilégié est la suivante :

**Router#**

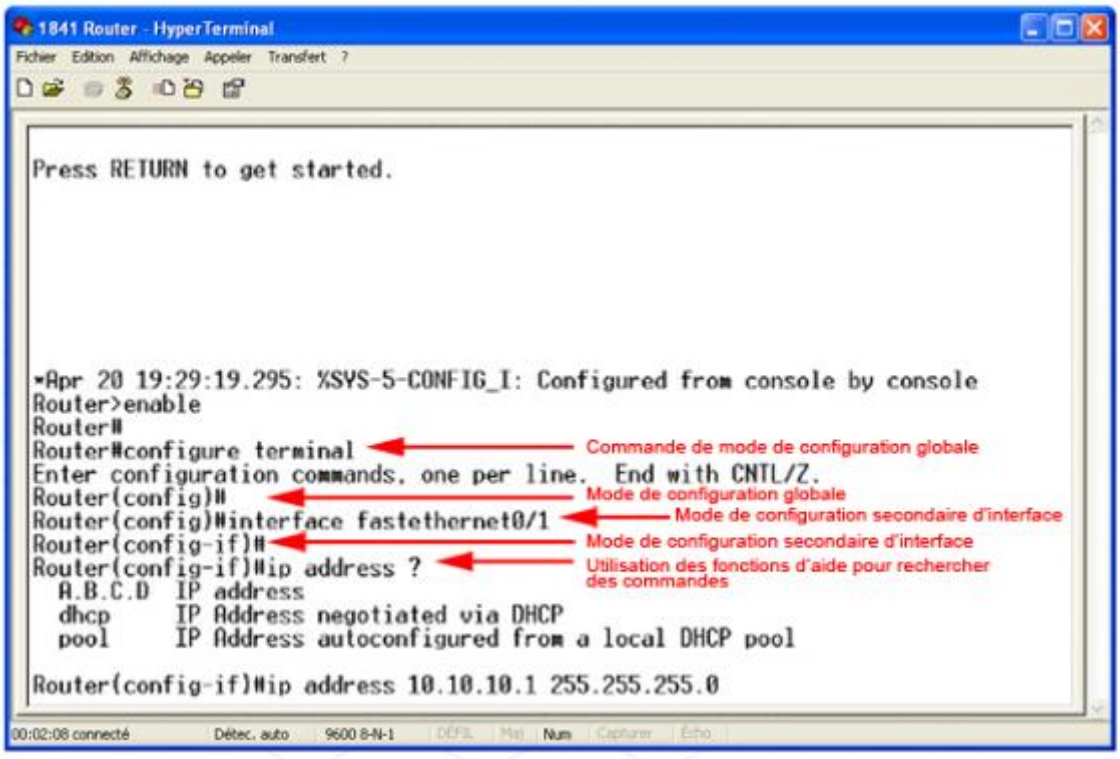
Pour désactiver le mode privilégié et retourner au mode utilisateur, entrez **disable** ou **exit** à l'invite de commandes.

Les deux modes peuvent être protégés par un mot de passe ou une combinaison de nom d'utilisateur et de mot de passe.




Pour configurer un périphérique, vous ferez appel à plusieurs modes de configuration. Pour configurer un périphérique Cisco IOS, vous devez passer en mode d'exécution privilégié. À partir du mode d'exécution privilégié, vous accèderez aux autres modes de configuration.

Dans la plupart des cas, les commandes sont appliquées au fichier de configuration en cours à l'aide d'une connexion de terminal. Pour utiliser ces commandes, vous devez passer en mode de configuration globale.



Pour passer en mode de configuration globale, tapez la commande **configure terminal** ou **config t**. Le mode de configuration globale est indiqué par l'invite de commandes suivante :

**Router(config)#**

Toute commande entrée dans ce mode prend effet immédiatement et peut modifier le fonctionnement du périphérique.

À partir du mode de configuration globale, l'administrateur peut accéder à d'autres sous-modes.

Le mode de configuration d'interface est utilisé pour configurer les interfaces de réseau local (LAN) et étendu (WAN). Pour accéder au mode de configuration d'interface, à partir du mode de configuration globale, tapez la commande **interface [type] [numéro]**. Le mode de configuration d'interface est indiqué par l'invite de commandes suivante :

**Router(config-if)#**

Un autre sous-mode utilisé fréquemment est le sous-mode de configuration du routeur, représenté par l'invite suivante :

**Router(config-router)#**

Ce mode est utilisé pour configurer les paramètres de routage.

**Travaux pratiques en ligne** : À l'aide de l'interface de ligne de commande Cisco, explorez les différents modes de configuration.

### *3.2 Utilisation de l'interface de ligne de commande Cisco IOS*

L'interface de ligne de commande Cisco IOS propose une multitude de fonctionnalités qui facilitent le rappel des commandes nécessaires à la configuration d'un périphérique. Ces fonctionnalités sont l'une des raisons pour lesquelles les techniciens réseau préfèrent utiliser l'ILC Cisco IOS pour configurer des routeurs.

La fonctionnalité d'aide contextuelle est particulièrement utile lors de la configuration d'un périphérique. Entrez **help** ou **?** à l'invite de commandes pour afficher une courte description du système d'aide.

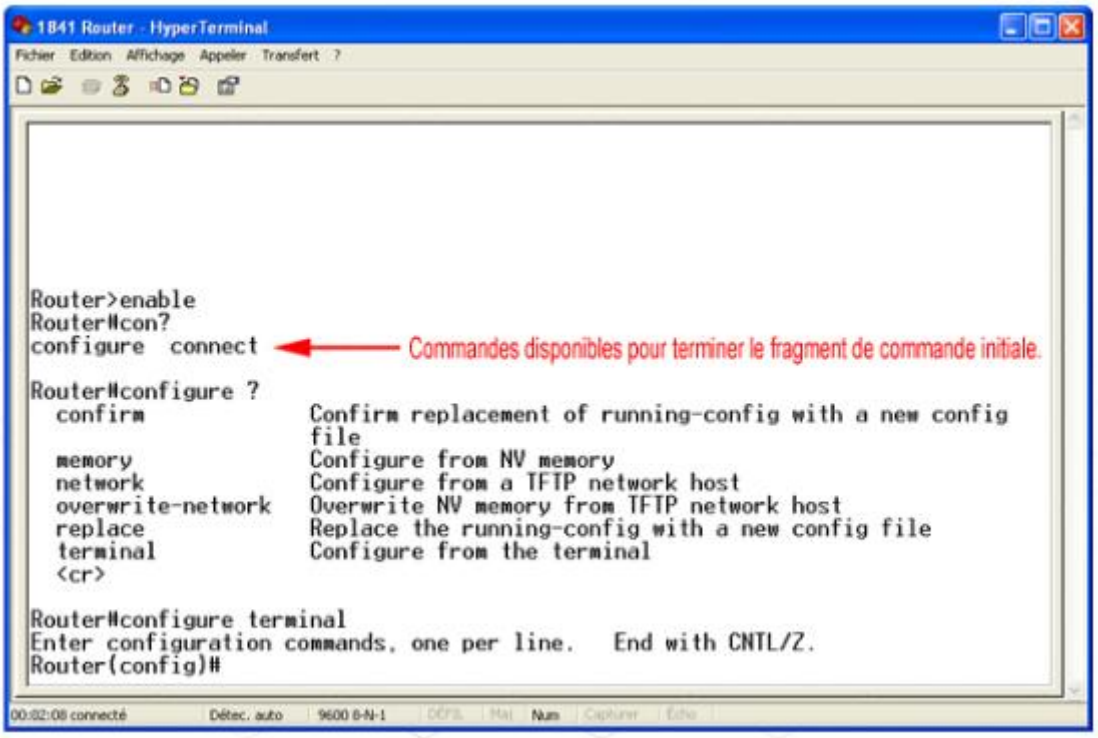
Router# **help**

L'aide contextuelle peut offrir des suggestions pour compléter une commande. Si vous connaissez les premiers caractères d'une commande, sans connaître la commande exacte, entrez la séquence de la commande que vous connaissez suivie d'un point d'interrogation **?**. Notez qu'aucun espace ne doit être inséré entre les caractères de la commande et le ?.

Pour obtenir une liste des options de paramètres pour une commande spécifique, entrez une partie de la commande, suivie d'un espace, puis le point d'interrogation ?. Par exemple, la saisie de la commande **configure** suivie d'un espace et d'un ? affiche une liste de variations

possibles. Choisissez l'une de ces variations pour terminer la chaîne de commande. Une fois la chaîne de commande complétée, un <cr> s'affiche. Appuyez sur Entrée pour exécuter la commande.

Si vous entrez un ? et qu'aucune correspondance n'existe, la liste d'aide qui s'affiche est vide. Ceci indique que la chaîne de commande ne correspond pas à une commande prise en charge.




Les utilisateurs commettent parfois des erreurs en tapant une commande. L'interface de ligne de commande vous indique si une commande entrée n'est pas reconnue ou est incomplète. Le caractère % indique le début d'un message d'erreur. Par exemple, si la commande **interface** est entrée sans autres paramètres, un message d'erreur s'affiche indiquant une commande incomplète :

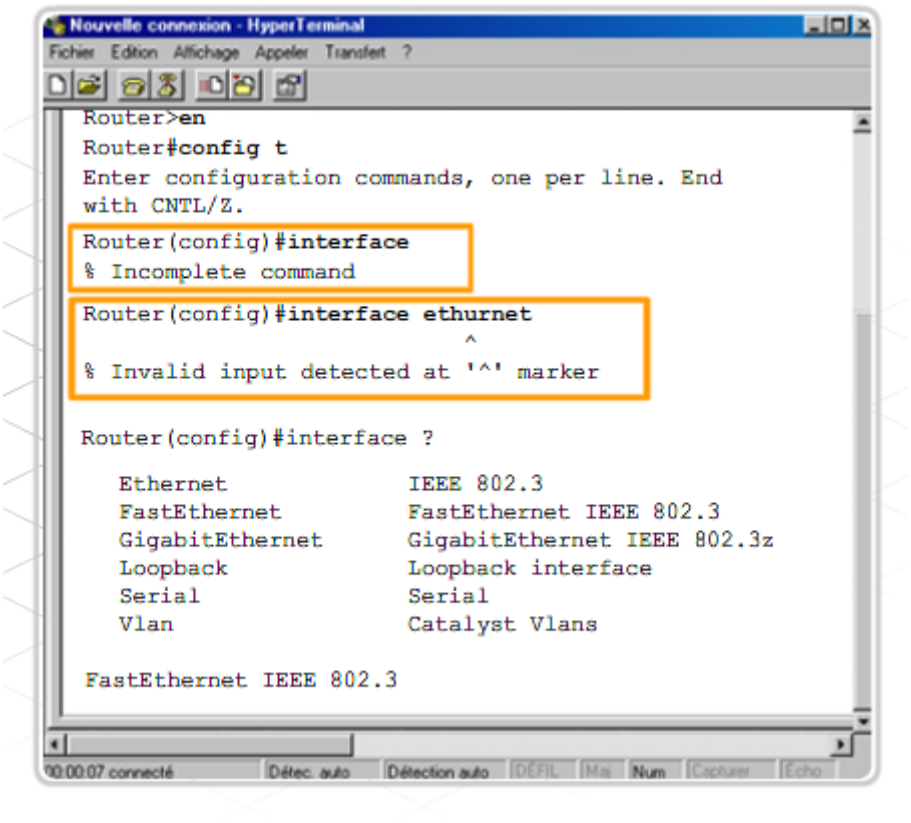
% Incomplete command.

Utilisez le ? pour obtenir une liste des paramètres disponibles.

Si la commande entrée est incorrecte, le message d'erreur suivant s'affiche :

% Invalid input detected

Il est parfois difficile de détecter l'erreur comprise dans une commande entrée de façon incorrecte. Heureusement, l'ILC comprend un indicateur d'erreur. Un accent circonflexe (^) s'affiche à l'emplacement d'un caractère incorrect ou non reconnu dans la chaîne de commande. Il permet ainsi à l'utilisateur de revenir à l'endroit où se trouve l'erreur et d'utiliser la fonction d'aide pour déterminer la commande correcte à utiliser.



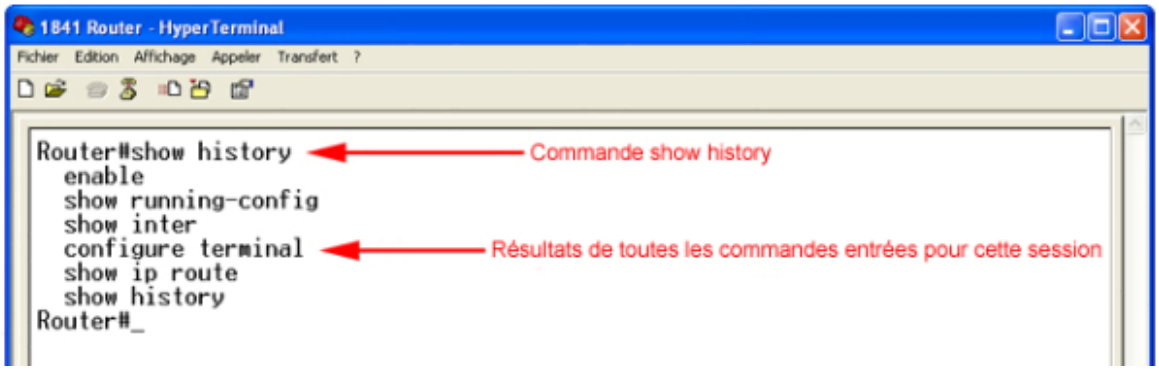

Une autre fonctionnalité de l'interface de ligne de commande Cisco IOS est la possibilité de rappeler des commandes tapées précédemment. Cette fonctionnalité est particulièrement utile pour rappeler des commandes ou des entrées longues ou complexes.

L'historique des commandes est activé par défaut et le système enregistre 10 lignes de commande dans la mémoire tampon d'historique. Pour modifier le nombre de lignes de commandes enregistrées par le système au cours d'une session, utilisez la commande **terminal history size** ou **history size**. Le nombre maximal de lignes de commande est de 256.

Pour rappeler la commande la plus récente dans la mémoire tampon de l'historique, appuyez sur Ctrl-P ou sur la flèche Haut. Appuyez plusieurs fois sur ces touches pour rappeler les commandes plus anciennes. Pour revenir à une commande plus récente dans la mémoire tampon de l'historique, appuyez sur Ctrl-N ou sur la flèche Bas. Appuyez plusieurs fois sur ces touches pour rappeler les commandes plus récentes.

L'interface de ligne de commande reconnaît une commande partiellement tapée en se basant sur ses premiers caractères uniques. Par exemple, tapez « int » au lieu d'« interface ». Si vous appuyez sur la touche Tab après avoir entré une forme abréviée telle que « int », l'ILC complètera l'entrée de la commande en « interface ».

La plupart des ordinateurs offrent des fonctions supplémentaires de sélection et de copie à l'aide de diverses touches de fonctions. Vous pouvez copier une chaîne de commande entrée précédemment et la coller ou l'insérer en tant que commande en cours.




Exercice

Faites correspondre les commandes et leurs fonctions.

Faites glisser la combinaison de touches appropriée sur la définition correcte.

| | |
|---|---|
| **Terminal history** *taille nombre-de-lignes* | |
| **Ctrl-N ou Bas** | |
| **Ctrl-P ou Haut** | |
| **<TAB>** | |
| **Show history** | |

| Touche | Définition |
|---|---|
| | Retour en arrière dans l'historique des commandes |
| | Avance dans l'historique des commandes |
| | Affichage du contenu de la mémoire tampon des commandes |
| | Définition de la taille de la mémoire tampon des commandes |
| | Compléter une saisie de commande |

Corrigé

| Touche | Définition |
|---|---|
| **Ctrl-P ou Haut** | Retour en arrière dans l'historique des commandes |
| **Ctrl-N ou Bas** | Avance dans l'historique des commandes |
| **Show history** | Affichage du contenu de la mémoire tampon des commandes |
| **Terminal history** *taille nombre-de-lignes* | Définition de la taille de la mémoire tampon des commandes |
| **<TAB>** | Compléter une saisie de commande |

**Exercice Packet Tracer:** Explorez les fonctionnalités de l'ILC Cisco IOS.

### *3.3 Utilisation des commandes show*

L’interface de ligne de commande Cisco IOS comprend des commandes show permettant d’afficher les informations appropriées sur la configuration et le fonctionnement du périphérique.

Les techniciens réseau utilisent fréquemment ces commandes pour afficher les fichiers de configuration, vérifier l’état des interfaces et des processus des périphériques et confirmer l’état de fonctionnement du périphérique. Les commandes show sont disponibles que le périphérique soit configuré à l’aide de l’interface de ligne de commande ou du gestionnaire SDM.

Vous pouvez afficher l’état de pratiquement tous les processus ou fonctions du routeur à l’aide d’une commande show. Les commandes show les plus couramment utilisées sont notamment :

- **show running-config**
- **show interfaces**
- **show arp**
- **show ip route**
- **show protocols**
- **show version**

**Travaux pratiques en ligne** : Utilisez les commandes show run et show interface pour répondre aux questions concernant la configuration du routeur.

**Exercice Packet Tracer** : Utilisez des commandes show de Cisco IOS sur un routeur du FAI.

## *3.4 Configuration de base*

La configuration initiale d'un périphérique Cisco IOS requiert la configuration du nom du périphérique, puis des mots de passe utilisés pour contrôler l'accès aux diverses fonctions du périphérique.

L'une des premières tâches de configuration consiste à attribuer au périphérique un nom unique. Cette tâche s'effectue en mode de configuration globale à l'aide de la commande suivante.

Router(config)# **hostname** <*nom*>

Lorsque vous appuyez sur la touche Entrée, l'invite change du nom d'hôte par défaut (Router) au nouveau nom d'hôte configuré.

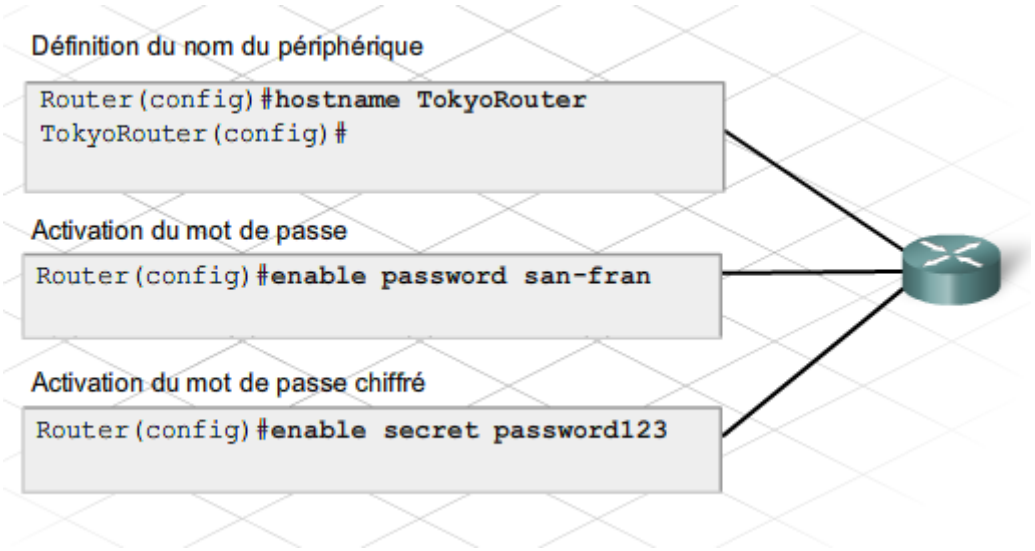
L'étape de configuration suivante consiste à configurer des mots de passe pour empêcher tout accès non autorisé au périphérique.

Les commandes **enable password** et **enable secret** permettent de limiter l'accès au mode d'exécution privilégié uniquement, ce qui empêche tout utilisateur non autorisé de modifier la configuration du routeur.

Router(config)# **enable password** <*mot de passe*>

Router(config)# **enable secret** <*mot de passe*>

La différence entre les deux commandes est que le mot de passe actif défini par la commande enable password n'est pas chiffré par défaut. Si vous utilisez la commande **enable password** pour définir le mot de passe actif, puis la commande **enable secret** pour définir le mot de passe actif secret, celle-ci remplace la première commande.



D’autres configurations de base d’un routeur incluent la configuration d’une bannière, l’activation de l’enregistrement synchrone et la désactivation de la recherche DNS.

**Bannières**

Une bannière est un texte qu’un utilisateur voit lorsqu’il ouvre une session sur le routeur. La configuration d’une bannière appropriée est un élément d’un plan de sécurité efficace. Une bannière doit au moins mettre en garde contre les accès non autorisés. Ne configurez jamais une bannière qui accueille un utilisateur non autorisé.

On distingue deux types de bannières : les messages du jour (MOTD) et les informations d’ouverture de session. L’utilisation de deux types de bannières différents permet de modifier une bannière sans modifier le message entier.

Pour configurer les bannières, utilisez les commandes **banner motd** et **banner login**. Dans les deux types de bannières, un séparateur, tel que le caractère #, est utilisé au début et à la fin du message. Le séparateur permet à l’utilisateur de configurer une bannière comprenant plusieurs lignes.

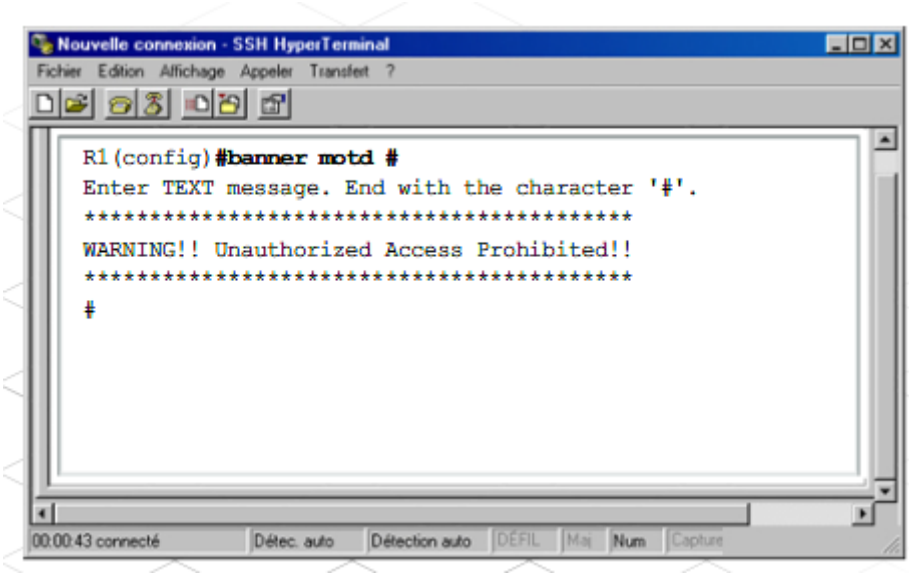
Si les deux bannières sont configurées, la bannière d’ouverture de session apparaît après la bannière MOTD, mais avant les informations d’identification pour l’ouverture de session.

**Enregistrement synchrone**

Le logiciel Cisco IOS envoie fréquemment des messages non sollicités, par exemple pour signaler une modification de l’état d’une interface configurée. Ces messages peuvent parfois s’afficher pendant la saisie d’une commande. Le message n’affecte pas la commande, mais peut être déroutant pour l’utilisateur qui tape la commande. Pour séparer les messages non sollicités des saisies de l’utilisateur, vous pouvez utiliser la commande **logging synchronous** en mode de configuration globale.

**Désactivation de la recherche DNS**

Par défaut, lorsqu’un nom d’hôte est entré en mode actif, le routeur suppose que l’utilisateur tente d’établir une connexion Telnet avec un périphérique. Le routeur tente de résoudre les noms inconnus entrés en mode actif en les envoyant au serveur DNS. Ce processus est appliqué à tous les mots entrés qui ne sont pas reconnus par le routeur, y compris les commandes tapées incorrectement. Si vous ne souhaitez pas appliquer ce processus, la commande **no ip domain-lookup** désactive cette fonctionnalité par défaut.




Pour effectuer des tâches de configuration, vous disposez de plusieurs méthodes d'accès au périphérique. L'une d'elles consiste à utiliser un ordinateur connecté au port de console du périphérique. Ce type de connexion est souvent utilisé pour la configuration initiale du périphérique.

La définition d'un mot de passe pour l'accès à la connexion console est effectuée en mode de configuration globale. Ces commandes empêchent les utilisateurs non autorisés d'accéder au mode utilisateur à partir du port de console.

Route(config)# **line console 0**

Router(config)# **password** <*mot de passe*>

Router(config)# **login**

Lorsque le périphérique est connecté au réseau, il est accessible par le biais de la connexion réseau. Lorsque l'accès au périphérique s'effectue par le réseau, la connexion est considérée comme une connexion vty. Le mot de passe doit être configuré sur le port vty.

Route(config)# **line vty 0 4**

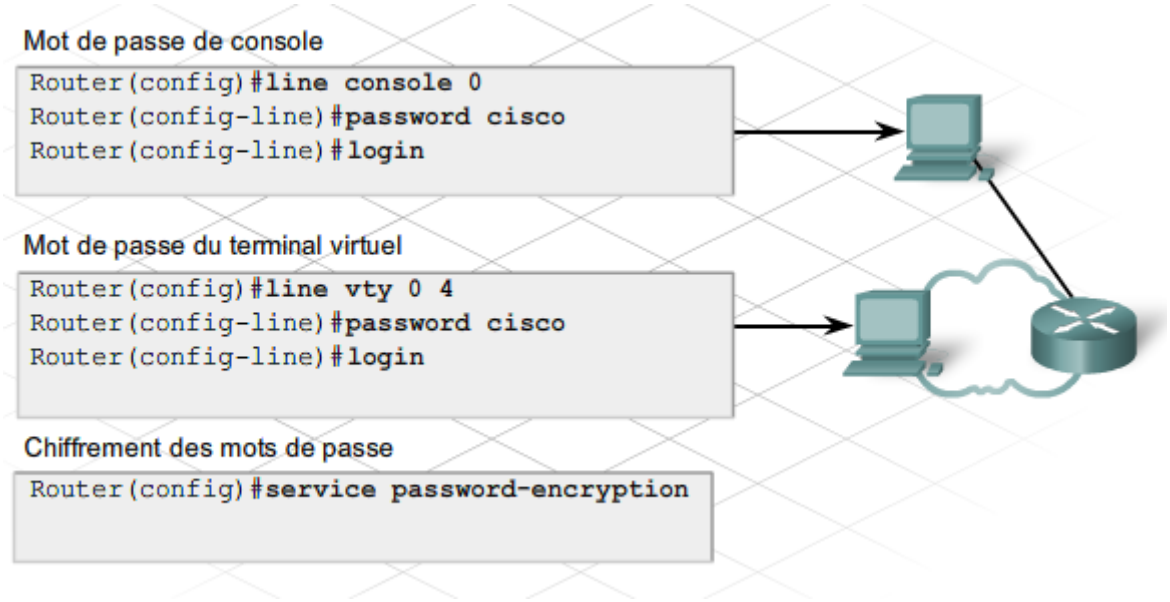
Router(config)# **password** <*mot de passe*>

Router(config)# **login**

0 4 représente 5 connexions intrabande simultanées. Il est possible de définir un mot de passe distinct pour chaque connexion en spécifiant les numéros de connexions de ligne, tels que **line vty 0**.

Pour vérifier que les mots de passe sont définis correctement, utilisez la commande **show running-config**. Ces mots de passe sont stockés dans la configuration en cours en texte clair. Il est possible de chiffrer tous les mots de passe stockés sur le routeur afin d'empêcher leur lecture par des personnes non autorisées. La commande de configuration globale **service password-encryption** permet de chiffrer tous les mots de passe.

N'oubliez pas que si vous modifiez la configuration en cours, vous devez la copier dans le fichier de configuration initiale pour éviter de perdre vos modifications lorsque le périphérique est mis hors tension. Pour copier les modifications apportées à la configuration en cours dans le fichier de configuration initiale enregistré, utilisez la commande **copy run start**.




**Exercice Packet Tracer** : Utilisez l'interface de ligne de commande Cisco IOS pour effectuer une configuration initiale du routeur.

### *3.5 Configuration d'une interface*

Pour diriger du trafic d'un réseau vers un autre, les interfaces sur le routeur doivent être configurées de manière à prendre part à chacun de ces réseaux. Une interface de routeur qui se connecte à un réseau reçoit généralement une adresse IP et un masque de sous-réseau compris dans la plage d'hôtes du réseau connecté.

Il existe différents types d'interfaces sur un routeur. Les interfaces série et Ethernet sont les plus courantes. Les connexions de réseau local (LAN) utilisent des interfaces Ethernet.

Les connexions de réseau étendu (WAN) requièrent une connexion série par le biais d'un FAI. Contrairement aux interfaces Ethernet, les interfaces série nécessitent un signal d'horloge, nommé « fréquence d'horloge », pour contrôler la synchronisation des communications. Dans la plupart des environnements, les périphériques d'équipement de communication de données (DCE), tels qu'un modem ou une unité CSU/DSU, fournissent la fréquence d'horloge.

Pour se connecter au réseau du FAI à l'aide d'une connexion série, un routeur nécessite une unité CSU/DSU si le réseau étendu est digital. S'il est analogique, il requiert un modem. Ces périphériques convertissent les données du routeur en un format acceptable pour la transmission sur le réseau étendu, et ils convertissent d'autre part les données du réseau

étendu en un format acceptable pour le routeur. Par défaut, les routeurs Cisco sont des périphériques d'équipement terminal de traitement de données (ETTD). Étant donné que les périphériques DCE contrôlent la synchronisation de la communication avec le routeur, les périphériques ETTD Cisco acceptent la fréquence d'horloge définie par le périphérique DCE.

Bien que cette procédure ne soit pas courante, il est possible de connecter deux routeurs directement à l'aide d'une connexion série. Dans ce cas, la connexion n'utilise pas d'unité CSU/DSU ni de modem et l'un des routeurs doit être configuré en tant que périphérique DCE pour fournir la synchronisation. Si le routeur est connecté en tant que périphérique DCE, une fréquence d'horloge doit être définie sur l'interface du routeur pour contrôler la synchronisation de la connexion DCE/ETTD.

La configuration d'une interface sur le routeur doit être effectuée en mode de configuration globale. La configuration d'une interface Ethernet est largement similaire à celle d'une interface série. L'une des principales différences est qu'une fréquence d'horloge doit être définie sur l'interface série si celle-ci est configurée comme périphérique DCE.

Les étapes de configuration d'une interface sont les suivantes :

**Étape 1.** Spécification du type d'interface et du numéro de port de l'interface

**Étape 2.** Spécification d'une description de l'interface

**Étape 3.** Configuration de l'adresse IP et du masque de sous-réseau de l'interface

**Étape 4.** Définition de la fréquence d'horloge si vous configurez une interface série en tant que DCE

**Étape 5.** Activation de l'interface

Après avoir activé une interface, vous devrez peut-être la désactiver pour des procédures de maintenance ou de dépannage. Dans ce cas, utilisez la commande shutdown.

Lors de la configuration de l'interface série sur un routeur Cisco 1841, celle-ci est désignée par 3 chiffres, C/S/P, où C=n° de contrôleur, S=n° de logement et P=n° de port. Le Cisco 1841 comporte deux logements modulaires. La désignation Serial0/0/0 indique que le module d'interface série se trouve sur le contrôleur 0, dans le logement 0, et que l'interface à utiliser est la première (0). La deuxième interface est Serial0/0/1. Le module série est normalement installé dans le logement 0, mais peut être installé dans le logement 1. Si c'est le cas, la désignation de la première interface série sera Serial0/1/0 et la deuxième Serial0/1/1.

Pour les ports intégrés, tels que les ports FastEthernet, la désignation est de 2 chiffres, C/P, où C=n° de contrôleur et P=n° de port. La désignation Fa0/0 représente le contrôleur 0 et l'interface 0.

```
Router(config)#interface fastethernet 0/0
Router(config-if)#description connection to Admin LAN
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface serial 0/0/0
Router(config-if)#description connection to Router2
Router(config-if)#ip address 192.168.1.125 255.255.255.0
Router(config-if)#clock rate 64000
Router(config-if)#no shutdown
```

**Travaux pratiques en ligne** : Configurez les interfaces série sur deux routeurs.

**Exercice Packet Tracer** : Configurez les interfaces Ethernet et série d'un routeur.

**Travaux pratiques** : Configurez les paramètres de base d'un routeur à l'aide de l'interface de ligne de commande Cisco IOS.

### *3.6 Configuration d'une route par défaut*

Un routeur transfère des paquets d'un réseau à un autre en fonction de l'adresse IP de destination spécifiée dans le paquet. Il examine la table de routage pour déterminer où transférer le paquet pour qu'il atteigne le réseau de destination. Si le routeur ne dispose pas dans sa table de routage de route vers un réseau spécifique, une route par défaut peut être configurée pour indiquer au routeur comment transférer le paquet. Le routeur n'utilise la route par défaut que s'il ne sait pas où envoyer un paquet.

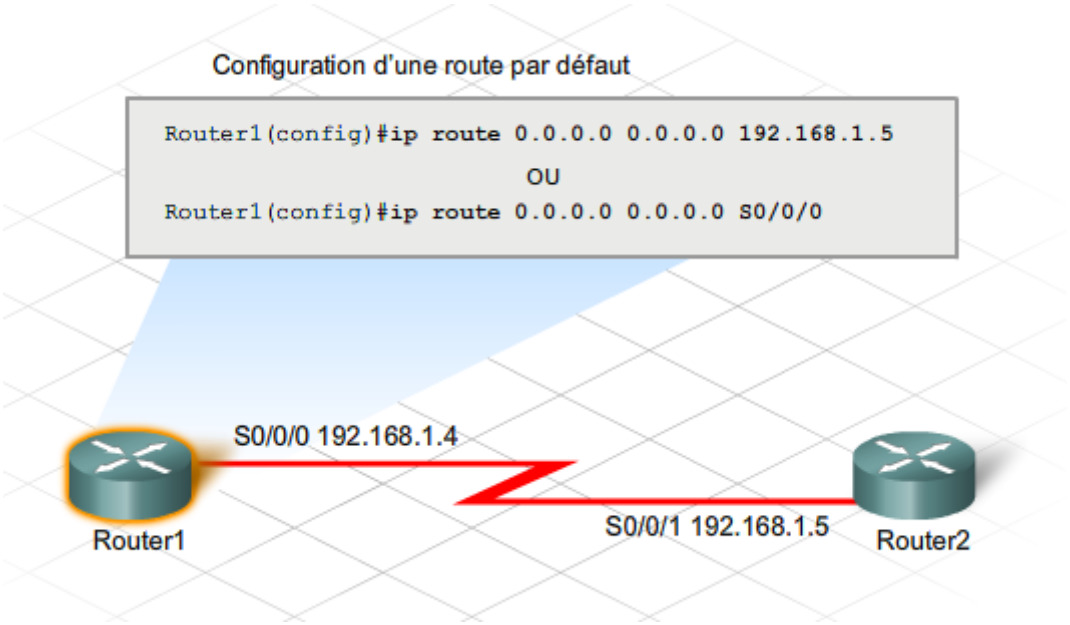
En général, la route par défaut pointe vers le routeur du tronçon suivant sur le chemin de connexion Internet. Les informations nécessaires pour configurer la route par défaut sont l'adresse IP du routeur du tronçon suivant ou l'interface que le routeur doit utiliser pour transférer le trafic dont le réseau de destination est inconnu.

La configuration de la route par défaut sur un routeur à services intégrés Cisco doit être effectuée en mode de configuration globale.

Router(config)# **ip route 0.0.0.0 0.0.0.0** <*adresse-IP-tronçon-suivant*>

ou

Router(config)# **ip route 0.0.0.0 0.0.0.0** <*type-interface*> <*numéro*>




**Exercice Packet Tracer :** Configurez une route par défaut sur des routeurs dans la topologie réseau d'une entreprise de taille moyenne.

### *3.7 Configuration des services DHCP*

L'interface de ligne de commande Cisco IOS peut être utilisée pour configurer un routeur de manière à fonctionner comme serveur DHCP.

L'utilisation d'un routeur configuré avec le protocole DHCP simplifie la gestion des adresses IP sur un réseau. L'administrateur ne doit alors mettre à jour qu'un seul routeur central en cas de modification des paramètres de configuration IP. La configuration du protocole DHCP à l'aide de l'ILC est légèrement plus complexe qu'à l'aide du gestionnaire SDM.

La configuration du protocole DHCP à l'aide de l'ILC s'effectue essentiellement en huit étapes.

**Étape 1.** Création d'un pool d'adresses DHCP

**Étape 2.** Spécification du réseau ou sous-réseau

**Étape 3.** Exclusion d'adresses IP spécifiques

**Étape 4.** Spécification du nom du domaine

**Étape 5.** Spécification de l'adresse IP du serveur DNS

**Étape 6.** Définition de la passerelle par défaut

**Étape 7.** Définition de la durée du bail

**Étape 8.** Vérification de la configuration

**Exercice Packet Tracer** : Configurez un routeur en tant que serveur DHCP pour les clients connectés.

**Travaux pratiques** : Utilisez Cisco SDM et l'interface de ligne de commande Cisco IOS pour configurer un routeur en tant que serveur DHCP.

### *3.8 Configuration de la fonction NAT statique avec Cisco IOS*

La fonctionnalité de traduction d'adresses de réseau (NAT) permet aux hôtes munis d'une adresse privée interne de communiquer sur Internet. Lors de la configuration de la fonction NAT, une interface au moins doit être configurée en tant qu'interface interne. L'interface interne est connectée au réseau privé interne. Une autre interface, généralement l'interface

utilisée pour accéder à Internet, doit être configurée comme interface externe. Lorsque les périphériques du réseau interne communiquent avec l'extérieur via l'interface externe, les adresses sont traduites en une ou plusieurs adresses IP enregistrées

Il peut arriver que le serveur situé sur un réseau interne doive être accessible à partir d'Internet. Pour cela, le serveur doit disposer d'une adresse enregistrée spécifique que les utilisateurs externes peuvent spécifier. La configuration d'une traduction NAT statique est l'une des manières possibles de fournir à un serveur interne une adresse accessible via Internet.

La fonction NAT statique assure que les adresses affectées aux hôtes sur le réseau interne sont toujours traduites en la même adresse IP enregistrée.

La configuration des fonctions NAT et NAT statique à l'aide de l'interface de ligne de commande Cisco IOS s'effectue en plusieurs étapes.

**Étape 1.**Spécification de l'interface interne

**Étape 2.** Définition de l'adresse IP principale de l'interface interne

**Étape 3.** Identification de l'interface interne à l'aide de la commande **ip nat inside**

**Étape 4.**Spécification de l'interface externe

**Étape 5.** Définition de l'adresse IP principale de l'interface externe

**Étape 6.** Identification de l'interface externe à l'aide de la commande **ip nat outside**

**Étape 7.** Définition de la traduction d'adresse statique

**Étape 8.** Vérification de la configuration

L'interface de ligne de commande du routeur offre plusieurs commandes pour afficher les opérations de traduction d'adresses de réseau à des fins d'analyse ou de dépannage.

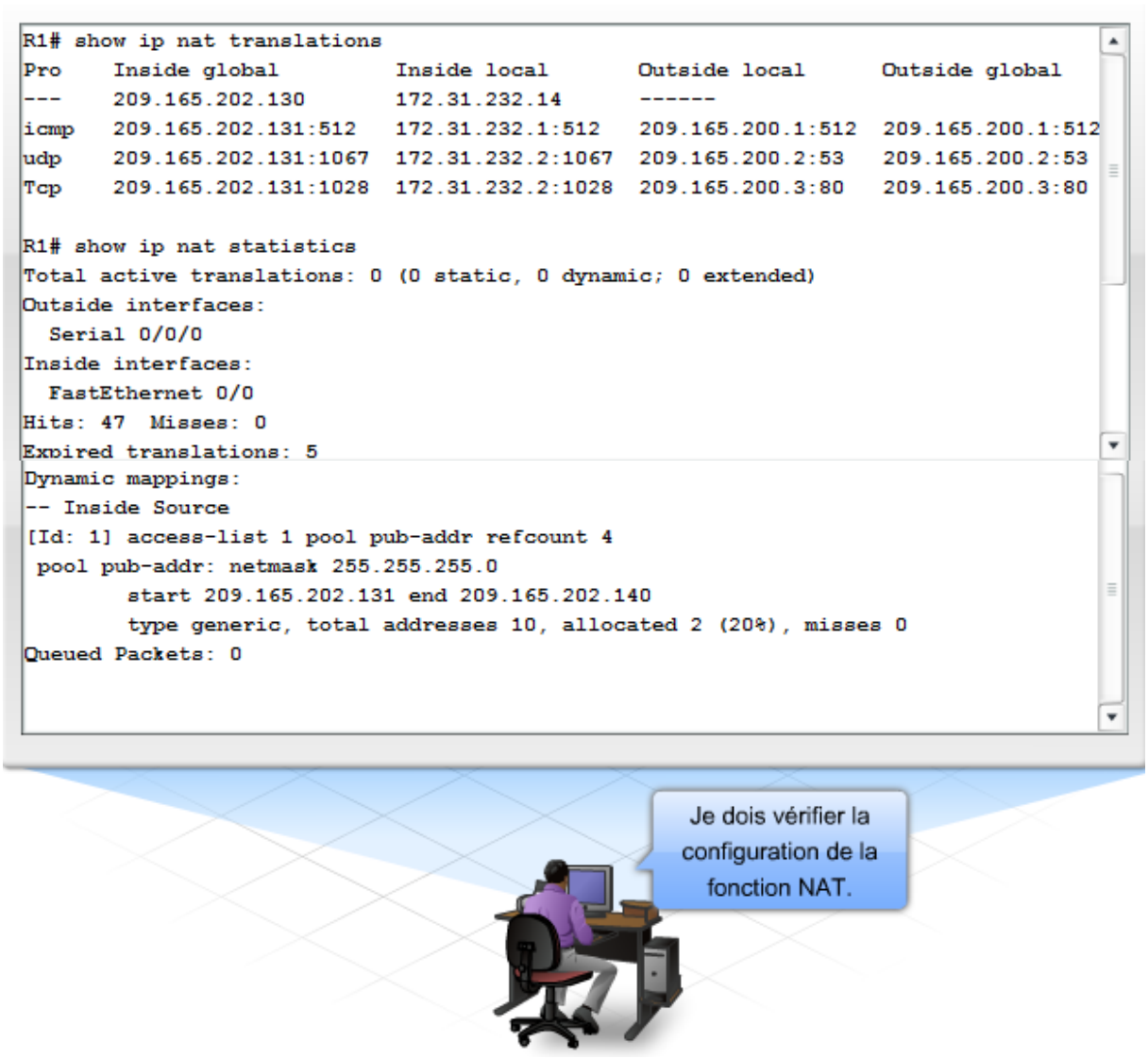
L'une des commandes les plus utiles est **show ip nat translations**. Les résultats affichent les affectations NAT en détail. La commande montre toutes les traductions statiques qui ont été configurées ainsi que les éventuelles traductions dynamiques créées par le trafic. Chaque traduction est identifiée par son protocole ainsi que par ses adresses locales et globales, internes et externes.

La commande **show ip nat statistics** affiche les informations sur le nombre total de traductions actives, les paramètres de configuration NAT, le nombre d'adresses dans le pool et le nombre d'adresses attribuées.

En outre, vous pouvez utiliser la commande **show run** pour afficher les configurations NAT.

Par défaut, si la fonction NAT dynamique est configurée, les entrées de traduction expirent au bout de 24 heures. Il est parfois utile d'effacer les entrées dynamiques avant l'expiration de ce délai par défaut, notamment lorsque vous testez la configuration NAT. Pour effacer des

entrées dynamiques avant expiration du délai d'attente, utilisez la commande globale **clear ip nat translation *** en mode actif. Seules les traductions dynamiques seront effacées de la table. Les traductions statiques ne peuvent pas être effacées de la table de traduction.




**Exercice Packet Tracer** : Configurez la fonction NAT statique sur un routeur.

**Travaux pratiques** : Configurez la fonction PAT à l'aide de Cisco SDM et la fonction NAT statique à l'aide de l'ILC Cisco IOS.

### *3.9 Sauvegarde d'une configuration de routeur Cisco*

Une fois votre routeur configuré, vous devriez enregistrer la configuration en cours dans le fichier de configuration initiale. Il est également recommandé d'enregistrer le fichier de configuration dans un autre emplacement, comme un serveur réseau par exemple. En cas de défaillance ou d'altération de la mémoire vive non volatile et si le routeur est dans l'incapacité de charger le fichier de configuration initiale, une autre copie est alors disponible. Vous disposez de plusieurs options pour enregistrer un fichier de configuration.

L'une des méthodes disponibles est d'enregistrer le fichier sur un serveur réseau à l'aide du protocole TFTP. Le routeur doit pouvoir accéder au serveur TFTP via une connexion réseau.

**Étape 1.** Entrez la commande **copy startup-config tftp**.

**Étape 2.** Entrez l'adresse IP de l'hôte sur lequel le fichier de configuration sera stocké.

**Étape 3.** Entrez le nom du fichier de configuration ou acceptez le nom attribué par défaut.

**Étape 4.** Confirmez chacun de vos choix en cliquant sur Yes (Oui).

La configuration en cours peut également être stockée sur un serveur TFTP à l'aide de la commande **copy running-config tftp**.

Pour restaurer le fichier de configuration de sauvegarde, le routeur doit avoir une interface au moins configurée et être en mesure d'accéder au serveur TFTP via une connexion réseau.

**Étape 1.** Entrez la commande **copy tftp running-config**.

**Étape 2.** Entrez l'adresse IP de l'hôte distant sur lequel est situé le serveur TFTP.

**Étape 3.** Entrez le nom du fichier de configuration ou acceptez le nom attribué par défaut.

**Étape 4.** Confirmez le nom du fichier de configuration et l'adresse du serveur TFTP.

**Étape 5.** À l'aide de la commande **copy run start**, copiez le fichier de configuration en cours dans le fichier de configuration initiale pour assurer que la configuration restaurée est enregistrée.

Lors de la restauration de la configuration, vous pouvez copier le fichier tftp dans le fichier de configuration initiale. Toutefois, ceci nécessite un redémarrage du routeur pour charger le fichier de configuration initiale dans la configuration en cours.

Une autre méthode pour créer une copie de sauvegarde de la configuration consiste à capturer les résultats de la commande **show running-config**. Pour faire cela à partir de la session du terminal, copiez les résultats, collez-les dans un fichier texte, puis enregistrez le fichier texte.

Les étapes suivantes permettent de capturer la configuration à partir d'un écran HyperTerminal.

**Étape 1.** Sélectionnez **Transférer**.

**Étape 2.** Sélectionnez **Capturer le texte.**

**Étape 3.** Spécifiez le nom du fichier texte dans lequel vous allez capturer la configuration.

**Étape 4.** Sélectionnez **Démarrer** pour commencer la capture du texte.

**Étape 5.** Utilisez la commande **show running-config** pour afficher la configuration à l'écran.

**Étape 6.** Appuyez sur Espace à chaque invite « - Plus - ».

Une fois la totalité de la configuration affichée, procédez comme suit pour arrêter la capture :

**Étape 1.**Sélectionnez **Transférer**.

**Étape 2.** Sélectionnez **Capturer le texte.**

**Étape 3.**Sélectionnez **Arrêter**.

Une fois la capture terminée, le fichier de configuration doit être édité pour supprimer les textes superflus, tels que le message « building configuration » de Cisco IOS. Vous devez également ajouter la commande **no shutdown** à la fin de chaque section d'interface. Cliquez sur **Fichier** > **Enregistrer** pour enregistrer la configuration. Le fichier de configuration peut être édité à l'aide d'un éditeur de texte tel que le Bloc-notes.

La configuration de sauvegarde peut être restaurée à partir d'une session HyperTerminal. Avant de restaurer la configuration, assurez-vous de supprimer les autres configurations éventuelles du routeur en exécutant la commande **erase startup-config** en mode d'exécution privilégié. Vous pouvez alors redémarrer le routeur à l'aide de la commande **reload**.

Pour copier la configuration de sauvegarde sur le routeur, procédez comme suit :

**Étape 1.** Passez en mode de configuration globale du routeur.

**Étape 2.** Dans HyperTerminal, sélectionnez **Transférer** > **Envoyer un fichier texte**.

**Étape 3.** Sélectionnez le nom du fichier de la configuration de sauvegarde enregistrée.

**Étape 4.** Restaurez la configuration initiale à l'aide de la commande **copy run start**.


**Exercice Packet Tracer** : Sauvegardez la configuration en cours sur un serveur TFTP.

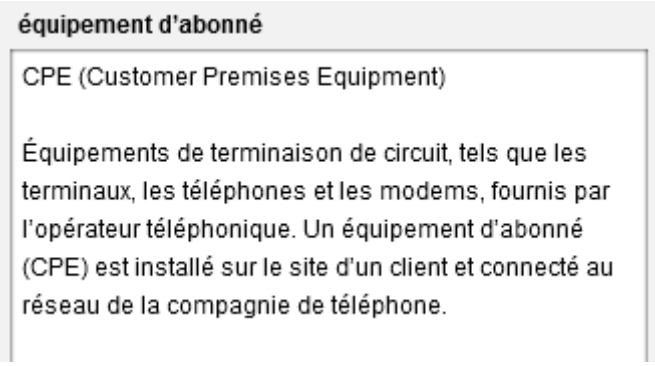
**Travaux pratiques** : Utilisez HyperTerminal pour enregistrer et charger la configuration en cours.

**Travaux pratiques** : Utilisez TFTP pour enregistrer et charger la configuration en cours.

# 4 Connexion de l’équipement d’abonné au FAI

## *4.1 Installation de l’équipement d’abonné*

Une des principales responsabilités du technicien réseau sur site consiste à installer et mettre à niveau l’équipement situé au domicile ou dans les locaux de l’entreprise d’un client. Les périphériques réseau installés dans les locaux du client sont désignés par le terme « équipement d’abonné » (CPE) et peuvent inclure des périphériques tels que des routeurs, des modems et des commutateurs.




L’installation ou la mise à niveau d’un routeur peut constituer une perturbation pour l’entreprise. De nombreuses entreprises dépendent d’Internet pour leur correspondance et fournissent des services de commerce électronique qui doivent demeurer accessibles tout au long de la journée. La planification de l’installation ou de la mise à jour constitue une étape essentielle pour assurer une exécution sans heurts. En outre, la planification permet d’explorer diverses options sur papier, ce qui permet de corriger les erreurs facilement et à moindres frais.

Le personnel technique du FAI rencontre généralement les représentants de l’entreprise cliente pour planifier l’installation ou la mise à niveau du routeur. Au cours des réunions de planification, le technicien détermine la configuration du routeur afin de répondre aux besoins du client et identifie les logiciels réseau pouvant être affectés par l’installation ou la mise à niveau.

Le technicien collabore avec le personnel du service informatique du client pour décider de la configuration du routeur à utiliser et pour développer la procédure de vérification de cette configuration. Il rédige alors une liste de contrôle de configuration à partir de ces informations.

La liste de contrôle de configuration fournit la liste des composants le plus souvent configurés. Elle inclut en général une description de chaque composant et du paramètre de configuration correspondant. La liste est un outil permettant de vérifier que tout est configuré correctement sur les nouvelles installations de routeurs. Elle est également utile pour résoudre les problèmes liés à des routeurs existants.

Les listes de contrôle de configuration peuvent prendre différents formats, dont certains peuvent être assez complexes. Les FAI doivent s'assurer que les techniciens d'assistance disposent de listes de contrôle de configuration des routeurs et les utilisent.

Planifiez l'installation avec le client. Installez le routeur conformément au plan.

Lorsqu'un client nécessite un nouvel équipement, les périphériques sont généralement configurés et testés sur le site du FAI avant d'être installés sur le site du client. Tout élément ne fonctionnant pas comme il se doit est immédiatement remplacé ou réparé. S'il s'agit de l'installation d'un nouveau routeur, le technicien réseau s'assure que le routeur est entièrement configuré et que cette configuration est vérifiée.

Après avoir vérifié la configuration du routeur, il rassemble tous les câbles réseau, les cordons d'alimentation, les câbles console, la documentation du fabricant, le logiciel du fabricant, la documentation de la configuration, ainsi que les outils spéciaux nécessaires à l'installation du routeur. Le technicien réseau utilise une liste de contrôle d'inventaire pour vérifier que tout l'équipement nécessaire à l'installation du routeur est réuni. En général, il signe la liste de contrôle pour indiquer que tout a été vérifié. La liste de contrôle d'inventaire signée et datée est fournie avec le routeur lorsqu'il est conditionné pour être expédié au site du client.

Le routeur est alors prêt à être installé par le technicien sur site. Il est important de convenir d'une heure qui minimise la perturbation des activités du client. Il ne sera peut-être pas possible d'installer ou de mettre à niveau un équipement réseau pendant les heures ouvrées normales. Si l'installation du nouvel équipement nécessite l'interruption du réseau, le technicien réseau, le vendeur FAI et un représentant de l'entreprise collaborent à la préparation d'un plan d'installation du routeur. Ce plan assure au client une perturbation minimale du service lors de l'installation du nouvel équipement. Le plan d'installation du routeur indique en outre le contact du client et les arrangements pour l'accès au site après les heures ouvrées. Dans le cadre du plan d'installation, une liste de contrôle d'installation est créée pour assurer que l'équipement est installé de façon appropriée.

Remplissez la liste de contrôle et passez en revue l'installation avec le représentant du client.

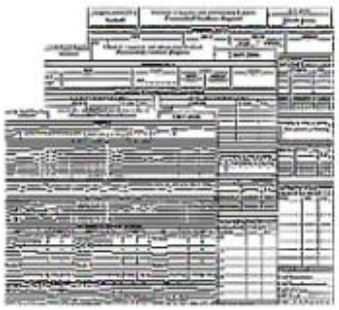
Obtenez du client son acceptation du nouvel équipement et son approbation de l'installation.

Le technicien réseau sur site doit installer le routeur dans les locaux du client à l'aide du plan d'installation et de la liste de contrôle. Lors de l'installation d'un équipement d'abonné, il est important d'effectuer le travail de façon professionnelle. Cela signifie notamment que tous les câbles réseau doivent être correctement étiquetés et attachés ensemble ou organisés à l'aide d'un équipement de gestion du câblage approprié. Les longueurs excessives de câbles doivent être soigneusement enroulées et placées à l'écart.

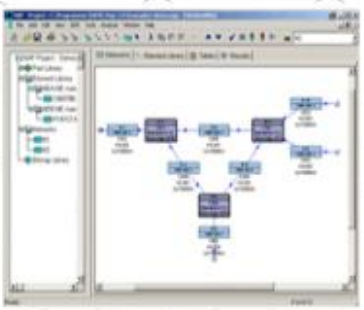
La documentation doit être mise à jour avec la configuration actuelle du routeur et les diagrammes de réseau doivent être modifiés pour indiquer l'emplacement de l'équipement et du câblage installés.

Une fois que le routeur est correctement installé et testé, le technicien réseau complète la liste de contrôle d'installation. La liste de contrôle remplie est alors vérifiée par le représentant du client. La vérification de l'installation du routeur inclut souvent une démonstration du bon fonctionnement du routeur et des services qui en dépendent.

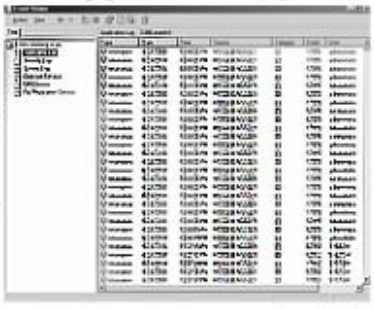
Lorsque le représentant du client s'est assuré que le routeur est correctement installé et opérationnel, il signe et date la liste de contrôle. Parfois, un document supplémentaire d'acceptation vient s'ajouter à la liste de contrôle. Cette procédure est souvent appelée « phase de validation ». Il est essentiel que le représentant du client valide le travail car, sans cette signature, le FAI ne peut pas facturer au client le travail réalisé.



Vérification des listes de contrôle



Actualisation des diagrammes de réseau



Préparation des journaux d'activité

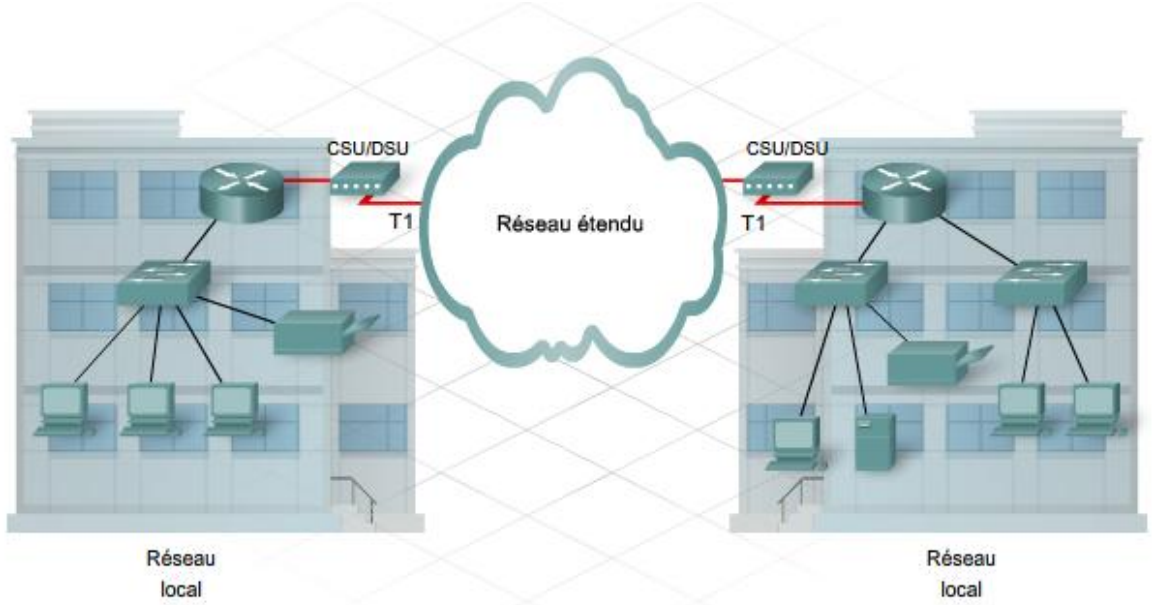
**Documentation de l'installation**

Lorsque l'équipement d'abonné est configuré et installé dans les locaux du client, il est important de documenter l'ensemble du processus. La documentation inclut tous les aspects de la configuration de l'équipement, les diagrammes d'installation et les listes de contrôle indispensables à la validation d'une installation réussie. Si une nouvelle configuration est requise, la documentation est comparée à la configuration précédente du routeur afin de déterminer si et dans quelle mesure la nouvelle configuration a été modifiée. Les journaux d'activité permettent d'effectuer le suivi des modifications et de l'accès aux équipements. Des journaux d'activité bien tenus sont précieux pour la résolution de problèmes.

Le technicien commence à documenter le travail lors de l'installation du routeur. Tous les câbles et tout l'équipement sont correctement étiquetés et indiqués sur un diagramme afin de faciliter leur identification ultérieure.

Le technicien utilise la liste de contrôle d'installation et de vérification lors de l'installation d'un routeur. Cette liste de contrôle répertorie les tâches qui doivent être accomplies dans les locaux du client. La liste de contrôle évite au technicien réseau de commettre des erreurs et lui permet de s'assurer que l'installation est effectuée correctement et efficacement.

Une copie de la documentation finale est remise au client.




## *4.2 Connexions du client sur un réseau WAN*

Le nouvel équipement sur le site du client doit être reconnecté au FAI pour fournir des services Internet. Lorsqu'un équipement d'abonné est mis à niveau, il est parfois nécessaire de mettre également à niveau le type de connectivité fournie par le FAI.

### Réseaux étendus

Lorsqu'une entreprise ou une organisation comprend des sites géographiquement éloignés, elle peut avoir recours à un fournisseur de services de télécommunications (TSP) pour interconnecter les réseaux locaux de ces différents sites. Les réseaux connectant les réseaux

locaux de sites géographiquement éloignés sont connus sous le nom de réseaux étendus (WAN).

Les fournisseurs de services de télécommunications exploitent d'importants réseaux régionaux pouvant s'étendre sur de grandes distances. Auparavant, ils transportaient les communications vocales et les données sur des réseaux distincts. De plus en plus, ces fournisseurs offrent à leurs abonnés des services réseau qui opèrent une convergence voix et données.

Les organisations louent généralement des connexions via le réseau TSP. Bien que l'organisation gère l'ensemble des stratégies et de l'administration des réseaux locaux aux deux extrémités de la connexion, les stratégies au sein du réseau du fournisseur de services de communications sont gérées par le FAI.

Les FAI vendent divers types de connexions WAN à leurs clients. Celles-ci varient en termes de type de connecteur utilisé, de bande passante et de coût. Au fur et à mesure que les petites entreprises se développent, elles ont besoin de la bande passante supplémentaire offerte par certaines connexions WAN plus coûteuses. L'une des tâches à réaliser au sein d'un FAI ou d'une entreprise de taille moyenne consiste à évaluer de quel type de connexion WAN l'organisation a besoin.

Afficher le multimédia visuel

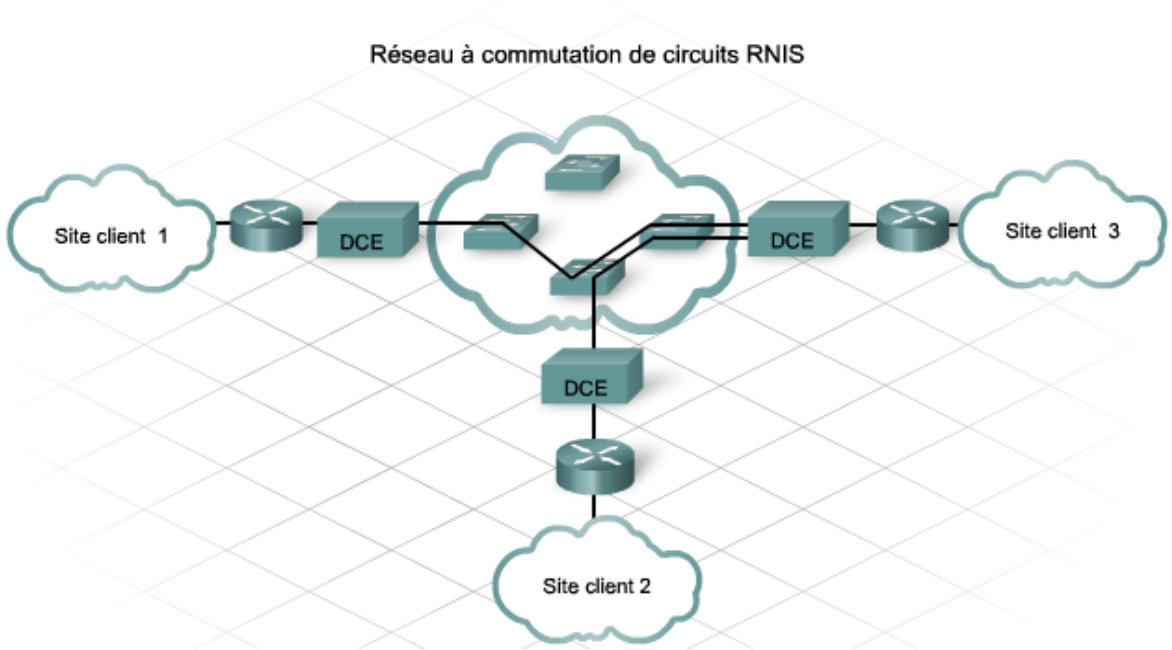
Il existe plusieurs types de connexions WAN série.

**Point à point**

Une connexion point à point est un chemin de communication prédéfini à partir des locaux du client via un réseau TSP. Il s'agit d'un circuit dédié avec une bande passante fixe disponible en permanence. Les lignes point à point sont généralement louées au fournisseur de services de télécommunications et sont connues sous le nom de lignes louées. Les connexions point à point sont généralement les connexions WAN les plus coûteuses et leur coût est fonction de la bande passante requise, ainsi que de la distance qui sépare les deux points connectés. Les liaisons T1 ou E1 sont un exemple de connexion WAN point à point.

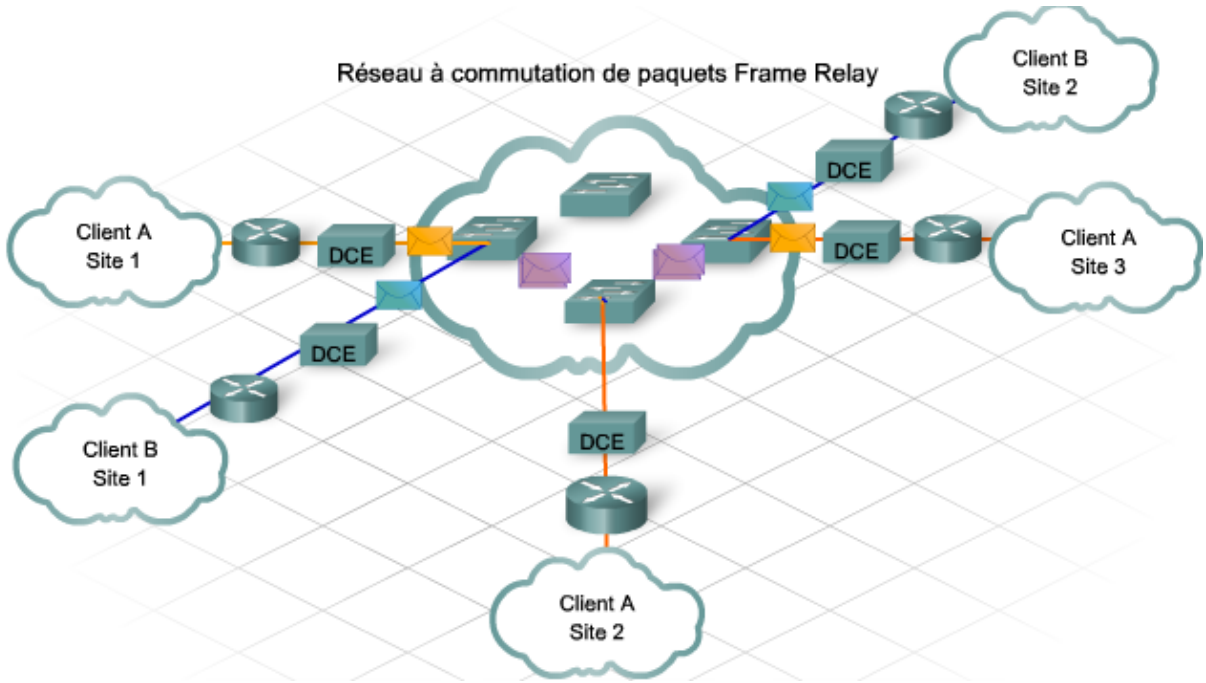

**À commutation de circuits**

Une connexion à commutation de circuits fonctionne de la même manière qu'un appel téléphonique effectué sur un réseau téléphonique. Lorsque vous téléphonez à un ami, vous décrochez le combiné, vous ouvrez le circuit, puis composez le numéro. L'appelant raccroche le téléphone une fois la conversation terminée et ferme ainsi le circuit. Les connexions RNIS ou commutées sont un exemple de connexion WAN à commutation de circuits.




## À commutation de paquets

Dans une connexion à commutation de paquets, les réseaux ont des connexions dans le réseau commuté TSP. De nombreux clients partagent ce réseau TSP. Plutôt que d'avoir un circuit réservé physiquement de la source à la destination, comme dans un réseau à commutation de circuits, les connexions à commutation de paquets offrent à chaque client son propre circuit virtuel. Un circuit virtuel est un chemin logique reliant l'émetteur et le récepteur, et non pas un chemin physique. Un exemple de réseau à commutation de paquets est le protocole Frame Relay.




## *4.3 Choix d'une connexion WAN*

Lors du choix d'une connexion WAN, la décision dépend principalement de la bande passante et du coût de la connexion. Les entreprises plus petites ne peuvent pas se permettre certaines des options de connexions WAN les plus coûteuses, telles que les connexions WAN SONET ou ATM. Elles installent généralement des connexions plus abordables telles que les connexions DSL, câble et T1. En outre, la disponibilité des connexions WAN à bande passante plus large peut être limitée dans les régions géographiquement isolées. Si les bureaux pris en charge sont proches d'un centre urbain, le choix de connexions WAN est plus vaste.

Un autre facteur affectant le choix d'une connexion WAN est la manière dont l'entreprise envisage d'utiliser la connexion. Si l'entreprise fournit des services sur Internet, elle nécessitera peut-être une bande passante ascendante plus large. Par exemple, si une entreprise héberge un serveur Web pour des activités de commerce électronique, elle a besoin d'assez de bande passante ascendante pour accueillir tous les clients externes qui visitent son site. Par contre, si le site de commerce électronique de l'entreprise est géré par un FAI, ses besoins en matière de bande passante ascendante sont réduits.

La possibilité d'obtenir un accord de niveau de service associé à la connexion WAN affecte également la décision de certaines entreprises. Les connexions WAN moins coûteuses, telles que les lignes commutées, DSL et câble, ne sont généralement pas fournies avec un accord de niveau de service, tandis que les connexions plus onéreuses le sont.

| Connexion | Bande passante | Coût |
|---|---|---|
| Liaison commutée | Jusqu'à 56 Kbits/s | Faible |
| Frame Relay | 128 Kbits/s - 512 Kbits/s | Faible - Moyen |
| DSL | 128 Kbits/s - 6+ Mbits/s[1] | Faible |
| Câble | 128 Kbits/s - 10+ Mbits/s[1] | Faible |
| T1 fractionnée | 64 Kbits/s - 1,544 Mbits/s | Faible - Moyen |
| T1/E1 | 1,544/2,048 Mbits/s | Moyen |
| T3 fractionnée | 1,544 Mbits/s - 44,736 Mbits/s | Moyen - Élevé |
| T3/E3 | 44,736/34,368 Mbits/s | Élevé |
| SONET | 51,840 Mbits/s - 9 953,280 Mbits/s | Élevé - Très élevé |
| ATM | 622 Mbits/s | Très élevé |

*Cette liste est un échantillon des options disponibles auprès d'un fournisseur de services Internet ou Telco.
La disponibilité varie selon le fournisseur et le lieu.

[1]La bande passante ascendante est généralement plus faible que la bande passante descendante annoncée.

De nombreux facteurs sont à prendre en compte lors de la planification d'une mise à niveau de réseau étendu. Le FAI initie le processus en analysant les besoins du client et en révisant les options disponibles. Une proposition est ensuite générée pour le client. La proposition décrit l'infrastructure existante, les besoins du client et les options WAN possibles.

**Infrastructure existante**

Il s'agit d'une description de l'infrastructure actuelle utilisée par l'entreprise. Elle permet au client de comprendre comment la connexion WAN existante fournit des services à son domicile ou son entreprise.

**Besoins du client**

Cette section de la proposition décrit pourquoi une mise à niveau de réseau étendu est nécessaire pour le client. Elle souligne les points où la connexion WAN courante ne satisfait pas les besoins du client. Elle inclut également une liste des besoins actuels et futurs du client que la nouvelle connexion WAN doit satisfaire.

**Options WAN**

Une liste de toutes les options WAN disponibles avec la bande passante et le coût correspondants, ainsi que d'autres fonctionnalités applicables à l'entreprise, est également incluse dans la proposition. La solution recommandée est indiquée, y compris d'autres options possibles.

La proposition de mise à niveau de réseau étendu est présentée aux décideurs de l'entreprise, qui revoient le document et considèrent les options. Une fois qu'ils ont pris leur décision, le FAI collabore avec le client pour développer un plan et coordonner le processus de la mise à niveau de réseau étendu.

**Travaux pratiques** : Complétez un plan de mise à niveau de réseau étendu en fonction du scénario d'entreprise présenté.

### *4.4 Configuration de connexions WAN*

Le mode de configuration d'un réseau étendu dépend du type de connexion WAN requise. Certaines connexions WAN prennent en charge les interfaces Ethernet. D'autres prennent en charge les interfaces série.

Les connexions WAN à ligne louée utilisent généralement une connexion série et nécessitent un dispositif de service d'accès aux canaux (CSU)/dispositif de service d'accès aux données (DSU) pour la connexion au réseau du FAI. L'équipement du FAI doit être configuré pour pouvoir communiquer avec les locaux du client via l'unité CSU/DSU.

Dans le cas d'une connexion série, il est important que la fréquence d'horloge préconfigurée soit la même aux deux extrémités de la connexion. La fréquence d'horloge est définie par le périphérique DCE, qui est généralement l'unité CSU/DSU. Le périphérique d'équipement terminal de traitement de données (ETTD), en général le routeur, accepte la fréquence d'horloge définie par le périphérique DCE.

L'encapsulation série par défaut de Cisco est le protocole HDLC. Il peut être remplacé par le protocole PPP, qui fournit une encapsulation plus souple et qui prend en charge l'authentification par le périphérique distant.

**Exercice Packet Tracer** : Configurez une connexion WAN série d'un routeur ISR Cisco vers une unité CSU/DSU d'un FAI.

# 5 Configuration initiale du commutateur Cisco 2960

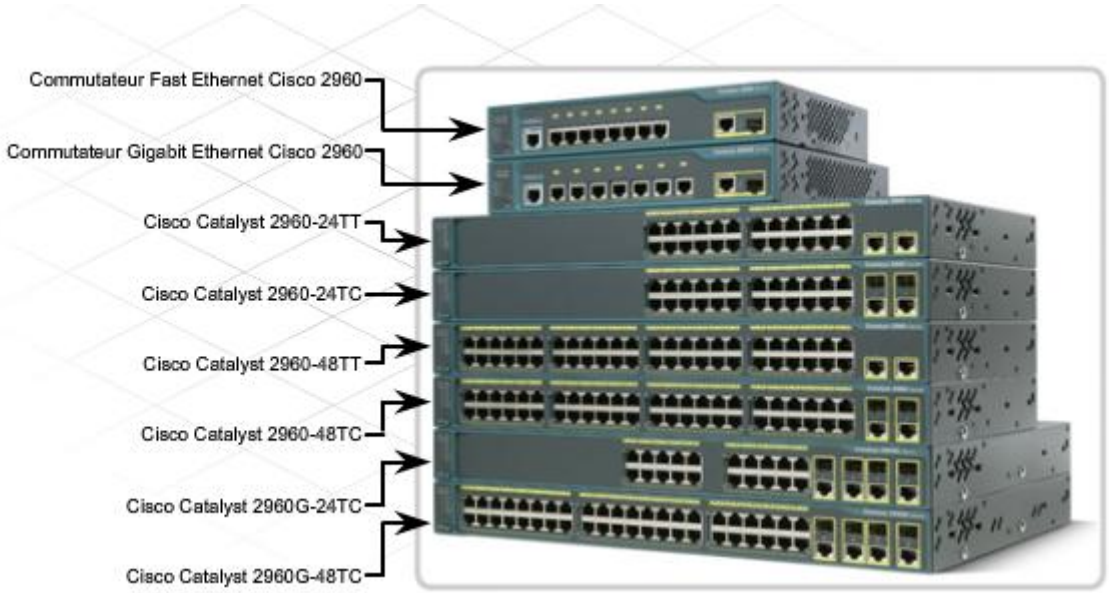
## *5.1 Commutateurs autonomes*

Bien que le module de commutation intégré du routeur ISR 1841 soit capable de connecter un nombre réduit d'hôtes au réseau local, il sera peut-être nécessaire d'ajouter des commutateurs plus grands et d'une capacité supérieure pour prendre en charge les utilisateurs supplémentaires au fur et à mesure que le réseau se développe.

Un commutateur est un périphérique qui dirige un flux de messages d'un port à un autre en fonction de l'adresse MAC de destination dans la trame. Un commutateur ne peut pas diriger le trafic entre deux réseaux locaux distincts. Dans le contexte du modèle OSI, un commutateur exécute les fonctions de couche 2, connue sous le nom de couche liaison de données.

Plusieurs modèles de commutateurs Ethernet sont disponibles sur le marché pour répondre aux différents besoins des utilisateurs. Le commutateur Ethernet de la gamme Catalyst 2960 de Cisco est conçu pour les réseaux d'entreprises de taille moyenne et de filiales d'entreprise.

Les commutateurs de la gamme Catalyst 2960 sont des périphériques autonomes à configuration fixe qui ne prennent pas en charge les modules ni les logements de cartes Flash. Étant donné que leur configuration physique ne peut pas être modifiée, le choix d'un commutateur à configuration fixe doit être basé sur le nombre et le type de ports requis. Les commutateurs de la gamme 2960 offrent une connectivité Fast Ethernet 10/100 et Gigabit Ethernet 10/100/1000. Ces commutateurs utilisent la plateforme logicielle Cisco IOS et peuvent être configurés à laide de l'interface graphique utilisateur de Cisco Network Assistant ou de l'interface de ligne de commande.


Commutateur Fast Ethernet Cisco 2960
Commutateur Gigabit Ethernet Cisco 2960
Cisco Catalyst 2960-24TT
Cisco Catalyst 2960-24TC
Cisco Catalyst 2960-48TT
Cisco Catalyst 2960-48TC
Cisco Catalyst 2960G-24TC
Cisco Catalyst 2960G-48TC


Commutateur de la gamme 2960
Vues
1:1
Avant
Arrière
Ports 10/100 et 10/100/1000 :
Les ports Ethernet 10/100 peuvent être configurés pour des vitesses de 10 ou 100 Mbits/s.
Les ports 10/100/1000 fonctionnent à 10, 100 ou 1000 Mbits/s.
Catalyst 2960 Series


Commutateur de la gamme 2960
Vues
1:1
Avant
Arrière
Ports SFP :
Un port SFP Ethernet compatible gigabit peut être utilisé pour prendre en charge des modules émetteurs-récepteurs fibre et cuivre. Les émetteurs-récepteurs fibre acceptent les câbles en fibre optique. Les émetteurs-récepteurs cuivre acceptent les câbles de catégorie 5 avec connecteurs RJ-45.
La possibilité de les brancher sur les ports SFP Gigabit Ethernet rend les émetteurs-récepteurs cuivre et fibre facilement remplaçables sur site en cas de défaillance d'une connexion.
Catalyst 2960 Series

Tous les commutateurs prennent en charge les modes bidirectionnels non simultané et simultané.

Un port en mode bidirectionnel non simultané peut, à tout moment, soit envoyer, soit recevoir des données mais pas les deux à la fois. Un port en mode bidirectionnel simultané peut envoyer et recevoir simultanément des données, ce qui permet de doubler le débit.

Le port et le périphérique connecté doivent tous les deux être définis sur le même mode bidirectionnel. Si ce n'est pas le cas, un décalage se crée dans le mode bidirectionnel, ce qui peut provoquer un nombre excessif de collisions et une dégradation des communications.

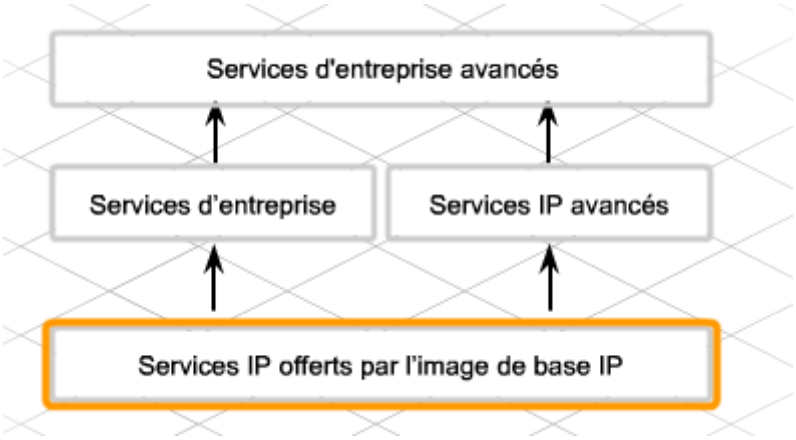
Vous pouvez définir manuellement le débit et le mode bidirectionnel des ports de commutateur ou utiliser la fonction d'autonégociation L'autonégociation permet au commutateur de détecter automatiquement le débit et le mode bidirectionnel du périphérique connecté au port. La fonction d'autonégociation est activée par défaut sur de nombreux commutateurs Cisco.

Pour que la fonction d'autonégociation s'exécute correctement, les deux périphériques connectés doivent la prendre en charge. Si le commutateur est en mode d'autonégociation et que le périphérique connecté ne prend pas en charge cette fonction, le commutateur utilise le débit de l'autre périphérique (10, 100 ou 1000) et est défini en mode bidirectionnel non simultané. Ce paramétrage par défaut en mode bidirectionnel non simultané peut provoquer des problèmes si le périphérique qui n'est pas en mode d'autonégociation est défini sur le mode bidirectionnel simultané.

Si le périphérique connecté ne prend pas en charge la fonction d'autonégociation, configurez manuellement les paramètres de mode bidirectionnel du commutateur pour les faire correspondre à ceux du périphérique connecté. Le paramètre de débit peut s'ajuster automatiquement, même lorsque le port connecté ne prend pas en charge la fonction d'autonégociation.

Les paramètres des commutateurs, notamment les paramètres de débit et de mode directionnel des ports, peuvent être configurés à l'aide de l'interface de ligne de commande (ILC) Cisco IOS. Lors de la configuration d'un commutateur à l'aide de l'ILC Cisco IOS, la structure d'interface et de commande est très similaire à celle des routeurs Cisco.

Comme pour les routeurs Cisco, vous disposez de plusieurs options d'images Cisco IOS pour les commutateurs. L'image logicielle de base IP est fournie avec le commutateur Catalyst 2960 de Cisco. Cette image fournit au commutateur les capacités de commutation et les services IP de base. D'autres images logicielles Cisco IOS ajoutent des services supplémentaires à l'image de base IP.




## *5.2 Mise sous tension du commutateur Cisco 2960*

La mise sous tension d'un commutateur Cisco 2960 est semblable à celle d'un ISR Cisco 1841.

Les trois principales étapes de la mise sous tension d'un commutateur sont les suivantes :

**Étape 1.** Vérification des composants

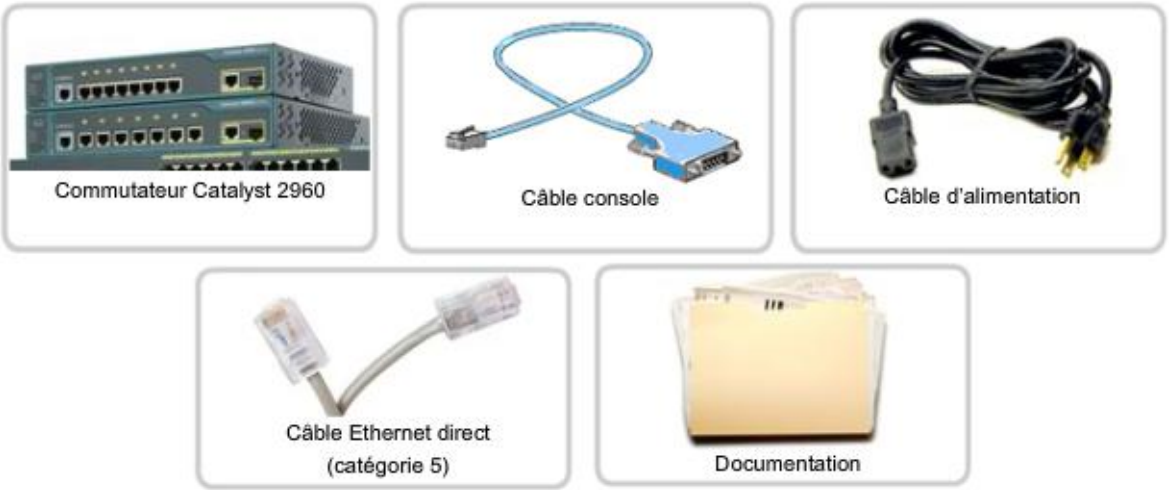
**Étape 2.** Branchement des câbles au commutateur

**Étape 3.** Mise sous tension du commutateur

Dès que le commutateur est sous tension, le test de démarrage POST (Power-On Self-Test) commence. Durant le test POST, les diodes électroluminescentes (LED) clignotent pendant qu'une série de tests détermine si le commutateur fonctionne correctement.

Le test POST est terminé lorsque la LED système SYST est verte et clignote rapidement. Si le commutateur échoue au test POST, la LED système vire à l'orange. Si un commutateur échoue à un test POST, il doit être renvoyé en réparation.

À la fin des procédures de démarrage, le commutateur Cisco 2960 est prêt à être configuré.



### Étape 1 - Vérification des composants

Vérifiez que vous disposez de tous les composants livrés avec le commutateur Cisco 2960 : le câble console, le cordon d'alimentation, le câble Ethernet et la documentation du commutateur.

### Étape 2 - Branchement des câbles au commutateur

Connectez l'ordinateur au commutateur à l'aide d'un câble console, puis démarrez une session d'émulation de terminal. Connectez le cordon d'alimentation au commutateur et à une prise de courant alternatif avec mise à la terre.

### Étape 3 - Activation du commutateur

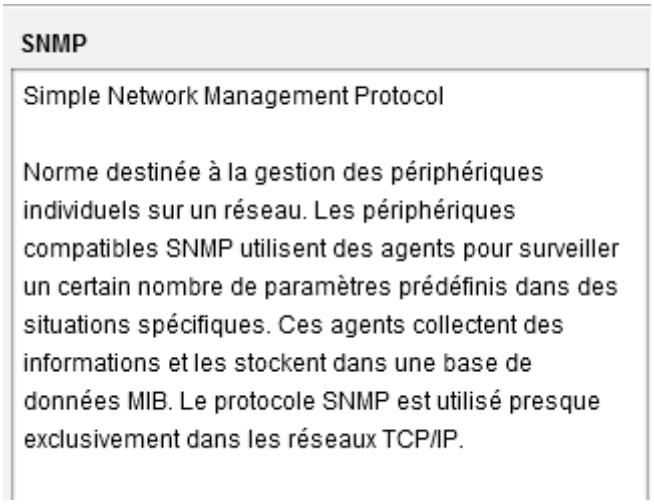
Certains modèles de commutateurs Cisco n'ont pas d'interrupteur marche/arrêt. Le commutateur 2960 se met en marche dès que le câble d'alimentation est branché au secteur.

**Travaux pratiques** : Mettez sous tension un commutateur Cisco 2960.

## *5.3 Configuration initiale d'un commutateur*

Vous disposez de plusieurs options pour configurer et gérer un commutateur LAN Cisco.

- Cisco Network Assistant
- Cisco Device Manager
- ICL Cisco IOS
- Logiciel de gestion CiscoView
- Produits de gestion de réseau SNMP




Certaines de ces méthodes utilisent la connectivité IP ou un navigateur Web pour la connexion au commutateur, ce qui nécessite une adresse IP. Contrairement à une interface de routeur, aucune adresse IP n'est attribuée à un port de commutateur. Pour utiliser un produit de gestion basé sur IP ou une session Telnet pour gérer un commutateur Cisco, une adresse IP de gestion doit être configurée sur le commutateur.

Si le commutateur n'a pas d'adresse IP, il est nécessaire de se connecter directement au port de console et d'utiliser un programme d'émulation de terminal pour réaliser les tâches de configuration.

```
Switch>enable
Switch#configure terminal
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.2 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#ip default-gateway 192.168.1.1
Switch(config)#end
Switch#copy running-config startup-config
```

Le commutateur Cisco Catalyst 2960 est livré préconfiguré et nécessite uniquement l'attribution d'informations de sécurité de base avant d'être connecté au réseau.

Les commandes utilisées pour configurer le nom d'hôte et les mots de passe du commutateur sont identiques à celles utilisées pour configurer le routeur à services intégrés (ISR). Pour utiliser un produit de gestion basé sur IP ou Telnet avec un commutateur Cisco, vous devez configurer une adresse IP de gestion.

Pour affecter une adresse à un commutateur, l'adresse doit être affectée à une interface VLAN de réseau local virtuel. Un réseau VLAN permet de regrouper logiquement plusieurs ports physiques. Par défaut, il existe un réseau VLAN préconfiguré dans le commutateur (VLAN 1) pour fournir l'accès aux fonctions de gestion.

**réseau local virtuel**

VLAN

Dans un réseau, groupe logique de périphériques qui sont situés ou non sur le même emplacement.

Pour configurer l'adresse IP affectée à l'interface de gestion sur VLAN 1, passez en mode de configuration globale.

Switch>**enable**

Switch#**configure terminal**

Ensuite, passez en mode de configuration d'interface pour le réseau local virtuel VLAN 1.

Switch(config)#**interface vlan 1**

Configurez l'adresse IP, le masque de sous-réseau et la passerelle par défaut pour l'interface de gestion. L'adresse IP doit être valide pour le réseau local sur lequel est installé le commutateur.

Switch(config-if)#**ip address 192.168.1.2 255.255.255.0**

Switch(config-if)#**exit**

Switch(config)#**ip default-gateway 192.168.1.1**

Switch(config)#**end**

Enregistrez la configuration à l'aide de la commande **copy running-configuration startup-configuration**.

**Travaux pratiques en ligne** : Configurez les paramètres de base sur un commutateur Cisco Catalyst.

**Exercice Packet Tracer** : Effectuez une configuration de base d'un commutateur.

### *5.4 Connexion du commutateur LAN au routeur*

**Connexion du commutateur au réseau**

Pour connecter le commutateur à un routeur, utilisez un câble direct. Les LED du commutateur et du routeur indiquent que la connexion est établie correctement.

Une fois le commutateur et le routeur connectés, déterminez si ces deux périphériques sont capables d'échanger des messages.

Vérifiez tout d'abord la configuration de l'adresse IP. Utilisez la commande **show running-configuration** pour vérifier que l'adresse IP de l'interface de gestion sur le commutateur VLAN 1 et l'adresse IP de l'interface du routeur directement connecté sont sur le même réseau local.

Ensuite, testez la connexion à l'aide de la commande **ping**. À partir du commutateur, envoyez une requête ping à l'adresse IP de l'interface du routeur directement connecté. Répétez ce processus à partir du routeur en envoyant une requête ping à l'adresse IP de l'interface de gestion affectée au commutateur VLAN 1.

Si la requête ping échoue, vérifiez à nouveau les connexions et les configurations. Vérifiez que les câbles ne sont pas défectueux et que les connexions sont stables.

Une fois que la communication entre le commutateur et le routeur est correctement établie, les différents ordinateurs peuvent être connectés au commutateur à l'aide de câbles directs. Ces câbles peuvent être connectés directement aux ordinateurs ou faire partie du câblage structuré branché aux prises murales.

Les ports des commutateurs constituent un point d'accès potentiel au réseau pour les utilisateurs non autorisés. Pour éviter ce risque de sécurité, les commutateurs comprennent une fonction appelée « sécurité des ports ». La sécurité des ports restreint le nombre d'adresses MAC valides autorisées sur un port. Le port ne transmet aucun paquet provenant d'adresses MAC sources en dehors du groupe des adresses définies.

Il existe trois façons de configurer la sécurité des ports.

**Statique**

Les adresses MAC sont affectées manuellement à l'aide de la commande de configuration d'interface **switchport port-security mac-address <*adresse-mac*>**. Les adresses MAC statiques sont stockées dans la table d'adresses et ajoutées à la configuration en cours.

Configuration de la sécurité statique des ports

| Syntaxe de commande de l'interface de ligne de commande Cisco IOS | |
|---|---|
| Passez en mode de configuration globale. | S1#**configure terminal** |
| Précisez le type et le numéro de l'interface physique à configurer (par exemple, fastEthernet Fa0/18) et passez en mode de configuration d'interface. | S1(config)#**interface fastEthernet 0/18** |
| Définissez le mode d'interface sur : access. Vous ne pouvez pas configurer une interface en tant que port sécurisé selon le mode dynamique par défaut approprié. | S1(config-if)#**switchport mode access** |
| Activez la sécurité des ports sur l'interface. | S1(config-if)#**switchport port-security** mac-address *[adresse-mac]* |
| Repassez en mode d'exécution privilégié. | S1(config-if)#**end** |

**Dynamique**

Les adresses MAC sont acquises de manière dynamique et stockées dans la table d'adresses. Le nombre d'adresses acquises peut être contrôlé. Par défaut, le nombre maximal d'adresses MAC acquises sur un port est de un. Les adresses acquises sont effacées de la table si le port est désactivé ou si le commutateur est redémarré.

Configuration de la sécurité des ports sur un commutateur Cisco Catalyst

| Syntaxe de commande de l'interface de ligne de commande Cisco IOS | |
|---|---|
| Passez en mode de configuration globale. | S1#**configure terminal** |
| Précisez le type et le numéro de l'interface physique à configurer (par exemple, fastEthernet Fa0/18) et passez en mode de configuration d'interface. | S1(config)#**interface fastEthernet 0/18** |
| Définissez le mode d'interface sur : access. Vous ne pouvez pas configurer une interface en tant que port sécurisé selon le mode dynamique par défaut approprié. | S1(config-if)#**switchport mode access** |
| Activez la sécurité des ports sur l'interface. | S1(config-if)#**switchport port-security** |
| Repassez en mode d'exécution privilégié. | S1(config-if)#**end** |

**Rémanente**

Semblable à l'adresse dynamique, sauf que les adresses sont également enregistrées dans la configuration en cours.

La sécurité des ports est désactivée par défaut. Si la sécurité des ports est activée, toute violation entraîne la désactivation du port. Par exemple, si la sécurité des ports dynamique est activée et que le nombre maximal d'adresses MAC par port est de un, la première adresse acquise devient l'adresse sécurisée. Si une autre station de travail tente d'accéder au port avec une adresse MAC différente, une violation de sécurité se produit.

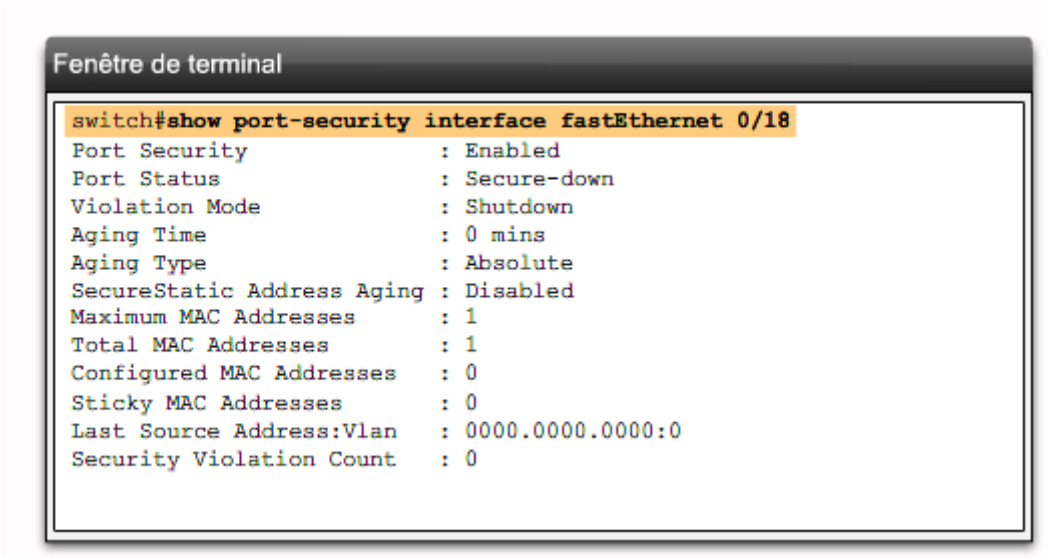
Script de configuration de la sécurité des ports

| Syntaxe de commande de l'interface de ligne de commande Cisco IOS | |
|---|---|
| Passez en mode de configuration globale. | S1#**configure terminal** |
| Précisez le type et le numéro de l'interface physique à configurer. | S1(config)#**interface fastEthernet 0/18** |
| Définissez le mode d'interface sur : access. | S1(config-if)#**switchport mode access** |
| Activez la sécurité des ports sur l'interface. | S1(config-if)#**switchport port-security** |
| Définir le nombre maximal d'adresses sécurisées sur 50 | S1(config-if)#**switchport port-security maximum 50** |
| Activer l'acquisition rémanente d'adresses MAC | S1(config-if)#**switchport port-security mac-address sticky** |
| Repassez en mode d'exécution privilégié. | S1(config-if)#**end** |

Il y a violation de la sécurité lorsque l'une des situations suivantes se présente :

- Le nombre maximal d'adresses MAC sécurisées a été ajouté dans la table d'adresses et un périphérique dont l'adresse MAC ne figure pas dans cette table tente d'accéder à l'interface.
- Une adresse acquise ou configurée dans une interface sécurisée est visible sur une autre interface sécurisée dans le même réseau local virtuel.

Pour activer la sécurité des ports, vous devez tout d'abord définir le port en mode d'accès à l'aide de la commande **switchport mode access**.




Pour vérifier les paramètres de sécurité des ports du commutateur ou de l'interface spécifiée, utilisez la commande **show port-security interface *id-interface***. Les résultats affichent les éléments suivants :

- le nombre maximal autorisé d'adresses MAC sécurisées pour chaque interface ;
- le nombre d'adresses MAC sécurisées dans l'interface ;
- le nombre de violations de sécurité ;
- le mode de violation.

En outre, la commande show port-security address affiche les adresses MAC sécurisées pour tous les ports et la commande show port-security affiche les paramètres de sécurité des ports du commutateur.

Si vous avez activé la sécurité des ports statique ou rémanente, vous pouvez utilisez la commande show running-config pour afficher l'adresse MAC associée à un port spécifique. Vous disposez de plusieurs options pour effacer une adresse MAC acquise enregistrée dans la configuration en cours :

- Utilisez la commande **clear port-security sticky interface <*port#*> access** pour effacer toutes les adresses acquises. Ensuite, désactivez le port à l'aide de la commande **shutdown**. Enfin, réactivez le port à l'aide de la commande **no shutdown**.
- Désactivez la sécurité des ports à l'aide de la commande d'interface **no switchport port-security**. Une fois désactivée, réactivez-la.
- Redémarrez le commutateur.

Le redémarrage du commutateur ne produira l'effet voulu que si la configuration en cours n'est pas enregistrée dans le fichier de configuration initiale. Si la configuration en cours est enregistrée dans le fichier de configuration initiale, il ne sera pas nécessaire pour le commutateur d'assimiler à nouveau les adresses lors du redémarrage du système. Toutefois,

l'adresse MAC acquise sera toujours associée à un port spécifique, à moins que le port soit effacé à l'aide de la commande **clear port-security** ou en désactivant la sécurité des ports. Si c'est le cas, veillez à réenregistrer la configuration en cours dans le fichier de configuration initiale pour empêcher le commutateur de rétablir l'adresse MAC associée à l'origine lors du redémarrage.

S'il existe des ports inutilisés sur un commutateur, il est recommandé de les désactiver. La désactivation de ports sur un commutateur est un jeu d'enfant. Accédez à chaque port inutilisé et exécutez la commande **shutdown**. Si vous devez activer un port, entrez manuellement la commande **no shutdown** dans cette interface.

Outre l'activation de la sécurité des ports et la désactivation des ports inutilisés, d'autres configurations de sécurité possibles sur un commutateur sont notamment la définition de mots de passe sur les ports vty, l'activation de bannières d'ouverture de session et le chiffrement des mots de passe à l'aide de la commande **service password-encryption**. Vous utiliserez pour ces configurations les mêmes commandes d'interface de ligne de commande Cisco IOS que pour configurer un routeur.

Fenêtre de terminal

```
switch#show port-security address
        Secure Mac Address Table
------------------------------------------------------------------------
Vlan   Mac Address       Type                Ports     Remaining Age (mins)
99     0050.BAA6.06CE    SecureConfigured    Fa0/18    -
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8320
```

**Exercice Packet Tracer** : Configurez et connectez le commutateur au réseau local à l'aide d'une liste de contrôle de configuration.

**Travaux pratiques** : Configurez et connectez le commutateur Cisco 2960.

### *5.5 Cisco Discovery Protocol*

Le protocole CDP (Cisco Discovery Protocol) est un outil de collecte des informations utilisé sur un commutateur, un routeur à services intégrés (ISR) ou un routeur pour partager les informations avec les autres périphériques Cisco directement connectés. Par défaut, l'exécution du protocole CDP commence dès le démarrage du périphérique. Il envoie ensuite des messages périodiques, appelés « annonces CDP », sur ses réseaux directement connectés.

Le protocole CDP fonctionne uniquement au niveau de la couche 2 et peut être utilisé sur de nombreux types de réseaux locaux, notamment les réseaux Ethernet et série. En tant que protocole de couche 2, il peut servir à déterminer l'état d'un lien connecté directement si aucune adresse IP n'a été configurée ou si l'adresse IP est incorrecte.

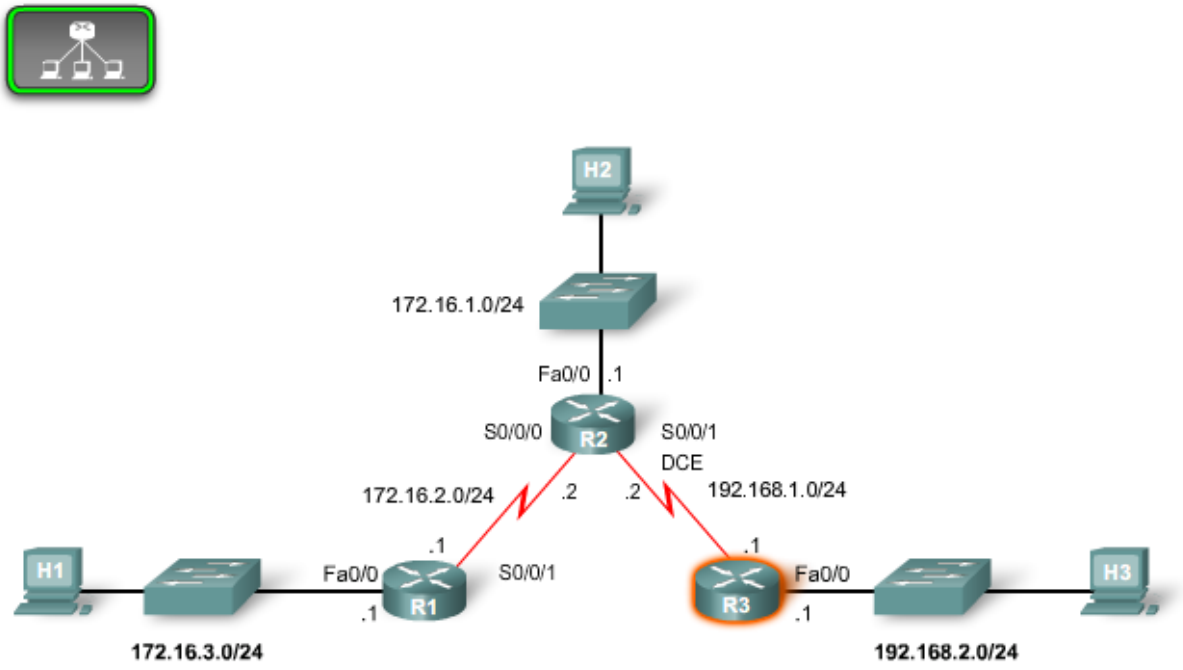
Lorsque deux périphériques Cisco sont connectés directement sur un même réseau local, ils sont dits « voisins ». Il est important de comprendre le concept de périphériques voisins pour interpréter le résultat des commandes CDP.

Les informations collectées par le protocole CDP incluent notamment :

- Identificateurs de périphérique : nom d'hôte configuré
- Liste d'adresses : adresse de couche 3, si configurée
- Identificateur de port : port connecté directement, par exemple Serial 0/0/0
- Liste de capacités : la ou les fonctions fournies par le périphérique
- Plateforme : plateforme matérielle du périphérique, par exemple Cisco 1841

Les résultats des commandes **show cdp neighbors** et **show cdp neighbors detail** affichent les informations que le périphérique Cisco collecte auprès de ses voisins directement connectés.

Pour afficher les informations CDP, l'utilisateur n'a pas besoin d'ouvrir de session sur les périphériques distants. Dans la mesure où le protocole CDP permet de collecter et d'afficher de nombreuses informations sur les voisins directement connectés sans devoir ouvrir une session sur ceux-ci, il est généralement désactivé sur les réseaux de production pour des raisons de sécurité. En outre, ce protocole consomme de la bande passante et peut avoir un impact sur les performances réseau.



## Voisins CDP

```
R3#show cdp neighbors
Capability Codes: R - Router, T- Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Hose, I - IGMP, r - Repeater, P - Phone

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Switch           Fas 0/0            133         S I       WS-C2950-2Fas 0/11
R2               Ser 0/0/           149        R S I      Cisco 1841Ser 0/0/1
```

## Détails des voisins CDP

```
R3#show cdp neighbors detail
-------------------------
Device ID: R2
Entry address(es):
  IP address: 192.168.1.2
Platform: Cisco 1841,  Capabilities: Router Switch IGMP
Interface: Serial0/0/1,  Port ID (outgoing port): Serial0/0/1
Holdtime : 161 sec

Version :
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(10b),
RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Fri 19-Jan-07 15:15 by prod_rel_team

advertisement version: 2
```

## Désactivation/Activation de CDP

```
!Pour désactiver l'utilisation globale de CDP...
R3(config)# no cdp run
!
!ou, pour désactiver CDP sur une interface uniquement...
R3(config-if)# no cdp enable
!Si CDP est désactivé globalement, il doit être activé globalement et par interface à l'aide des deux commandes suivantes :
Router(config)# cdp run
Router(config-if)# cdp enable
```

**Exercice Packet Tracer** : Utilisez les commandes show CDP pour découvrir des informations sur des périphériques du réseau.

# 6 Résumé du chapitre

- Les principaux composants d'un routeur à services intégrés Cisco 1841 sont :
  - Les logements HWIC
  - Le module Compact Flash
  - Le port USB
  - Les ports 10/100 Fast Ethernet à double fonction
  - Les ports de console et auxiliaires
  - Les voyants d'alimentation système
  - L'image logicielle Cisco IOS

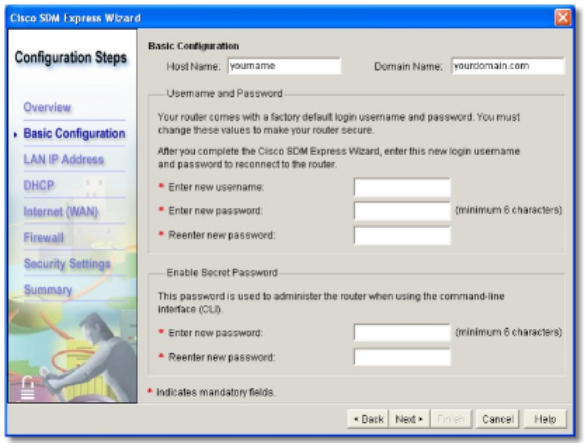
- Le processus d'amorçage du routeur comprend trois étapes:
  1. Exécution de la routine POST
  2. Localisation et chargement du logiciel Cisco IOS
  3. Localisation et exécution du fichier de configuration du démarrage

- Il existe deux méthodes pour connecter un ordinateur à un périphérique réseau pour des tâches de configuration et de surveillance, à savoir la gestion intrabande et la gestion hors bande.

- Cisco Router and Security Device Manager (SDM) est un outil à interface utilisateur graphique qui permet de configurer, de surveiller et d'assurer la maintenance des périphériques Cisco. Cisco SDM est le meilleur moyen de configurer un nouveau routeur à services intégrés Cisco.

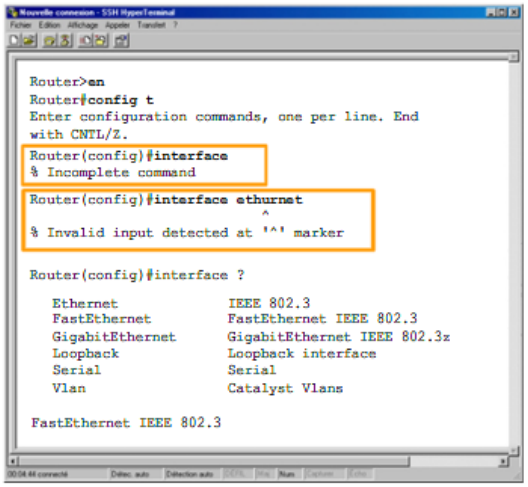
- L'interface de ligne de commande (ILC) Cisco IOS est un programme de type texte qui permet d'entrer et d'exécuter des commandes Cisco IOS pour configurer, surveiller et maintenir les périphériques Cisco. L'ILC Cisco IOS est utilisée pour la configuration avancée des périphériques Cisco et pour la configuration de périphériques plus anciens qui ne prennent pas en charge SDM.

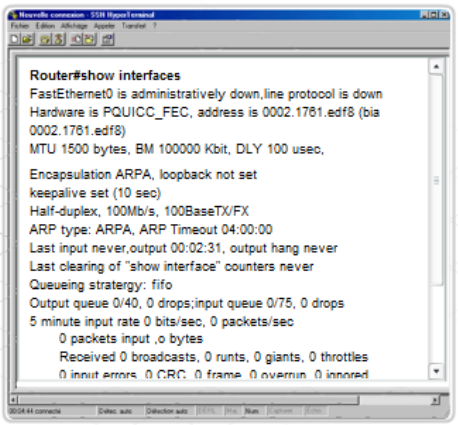
- L'aide aux tâches de la liste de contrôle de configuration est un outil important qui permet de s'assurer que le client reçoit bien la configuration qu'il a demandée.




- SDM Express est un outil intégré dans Cisco Router and Security Device Manager qui facilite la création d'une configuration de routeur de base.
- SDM est une interface graphique utilisateur plus évoluée qui propose davantage d'options de configuration.
- SDM et SDM Express comprennent tous deux des assistants de configuration à interface graphique qui simplifient la tâche de configuration des périphériques Cisco.
- Les fonctionnalités configurables peuvent être notamment: la configuration de base, les configurations IP de réseau local, le protocole DHCP, les configurations IP de réseau étendu et la traduction d'adresses de réseau (NAT).

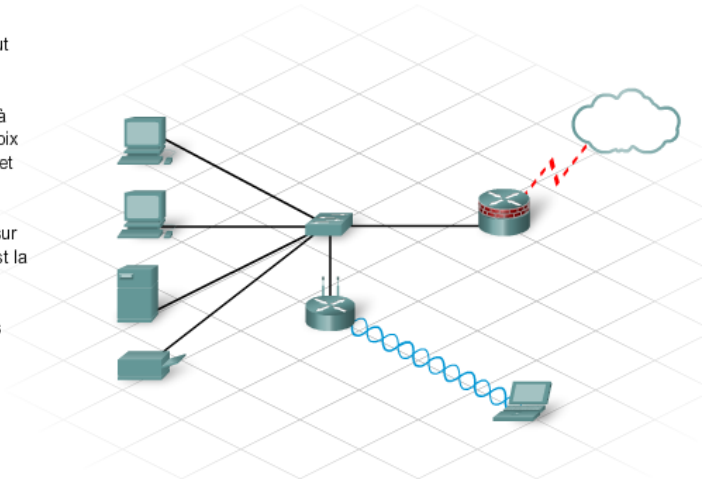
- L'interface de ligne de commande n'offre pas d'assistance étape par étape pour la configuration, c'est pourquoi sa mise en œuvre requiert plus de planification et d'expertise.
- Les modes d'exécution privilégié, de configuration globale et d'interface sont tous utilisés lors de la configuration d'un routeur à l'aide de l'interface de ligne de commande Cisco IOS.
- L'aide contextuelle propose des suggestions pour l'entrée des commandes et le choix de paramètres de commande supplémentaires.




- Les commandes IOS **show** sont un outil essentiel pour la vérification et le dépannage des configurations des routeurs.
- Le fichier de configuration initiale est stocké sur le périphérique dans la mémoire vive non volatile (NVRAM) ; il est chargé dans la mémoire de travail et initie la mise en route du périphérique.
- La configuration en cours est le jeu de commandes actuellement activé dans la mémoire RAM du périphérique.
- L'interface de ligne de commande IOS permet de configurer des paramètres de base du routeur, notamment le nom du routeur, les mots de passe et les bannières. Elle peut également être utilisée pour configurer les interfaces série et Ethernet, ainsi que les fonctions DHCP et NAT.

- Une connexion WAN est un type de connexion réseau qui peut envoyer un signal réseau sur de longues distances.
- Il existe trois types de connexions WAN série : point à point, à commutation de circuits et à commutation de paquets. Le choix de la connexion WAN appropriée nécessite une planification et une réflexion.
- Les périphériques Cisco peuvent être configurés à distance sur une connexion WAN au moyen de Telnet ou de SSH. SSH est la meilleure méthode.
- Certaines connexions WAN prennent en charge les interfaces Ethernet. D'autres prennent en charge les interfaces série.



- Les principaux composants d'un commutateur de la gamme Cisco Catalyst 2960 sont :
  - 24 ports Ethernet 10/100
  - Les voyants d'état des ports
  - Le bouton Mode
  - Le port de console
  - Un port 10/100/1000 ou SFP à double fonction
  - L'image logicielle sur le réseau local de Cisco IOS
- Le commutateur 2960 prend en charge l'autonégociation par le port du mode bidirectionnel simultané et de la vitesse de communication.

```
Switch>enable
Switch#configure terminal
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.2 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config-if)#ip default-gateway 192.168.1.1
Switch(config-if)#end
Switch#copy running-config startup-config
```

- En configurant le VLAN1 avec une adresse IP, vous pouvez gérer à distance le commutateur au moyen de SSH ou d'autres applications TCP/IP telles qu'un logiciel de gestion de réseau.
- La configuration de base d'un commutateur inclut le nom du commutateur et des mots de passe chiffrés utilisés pour accéder au commutateur et aux commandes de configuration de l'interface de ligne de commande Cisco.
- La sécurité des ports restreint le nombre d'adresses MAC autorisées sur un port et elle peut être configurée statiquement, dynamiquement ou à l'aide d'adresses MAC sticky dynamiques.

# 7 Questionnaire du chapitre

Question 1

Lors de la configuration d'un périphérique ISR à l'aide de l'Assistant Express Cisco SDM, quel est le rôle du paramètre Crypter les mots de passe ?

- S'assurer que l'autorisation est accordée avant d'accéder à Internet
- Empêcher les utilisateurs non autorisés d'accéder au réseau local
- Contrôler l'accès au mode utilisateur
- Contrôler l'accès au mode privilégié

Question 2

Lors de l'utilisation de l'interface SDM de Cisco, quel type d'encapsulation de réseau local étendu peut être configuré afin de requérir un nom d'utilisateur et un mot de passe pour qu'une connexion puisse être accordée ?

- HDLC (High-level Data Link Control)
- Frame Relay
- PPP (protocole point à point)
- Circuit virtuel permanent ATM

Question 3

Quel paramètre de vitesse et de mode duplex obtiendrez-vous sur un commutateur Catalyst défini sur l'autonégociation et connecté à un port 100 Mbits/s d'un périphérique qui ne prend pas en charge l'autonégociation ?

- 10 bidirectionnel
- 10 bidirectionnel simultané
- 100 bidirectionnel
- 100 bidirectionnel simultané

Question 4

Quelle méthode peut être utilisée pour configurer un commutateur Cisco Catalyst avant qu'une adresse IP ne soit appliquée à l'interface de gestion ?

- Interface de ligne de commande Cisco IOS utilisant Vlan 1
- Interface de ligne de commande Cisco IOS utilisant un port de console
- Gestionnaire de périphériques Cisco utilisant un port de console
- Logiciel CiscoView utilisant Vlan 1

## Question 5

Quelle méthode sécurisée permet à un client de se connecter à un périphérique in band à des fins de contrôle et d'administration à distance ?

- Telnet
- HTTP
- SSH
- Port console

## Question 6

Quel type de connexion de réseau étendu utilise des réseaux « à commutation de paquets » ?

- RNIS
- Commutée
- Frame Relay
- Point-à-point

## Question 7

Une petite entreprise disposant de deux bureaux situés dans un même bâtiment souhaite être informée sur les connexions de réseau étendu. Quelles questions pourront servir de base à un technicien pour effectuer une recommandation ? (Choisissez deux réponses.)

- [ ] Quel système d'exploitation est utilisé dans votre société ?
- [ ] Quel budget a été affecté pour la connexion de réseau étendu ?
- [ ] Quel type de logiciel de messagerie les employés utilisent-ils ?
- [ ] Utilisez-vous des ordinateurs portables ou de bureau ?
- [ ] Les serveurs Web de la société se trouvent-ils sur votre site ou chez le FAI ?

## Question 8

Quel principe fondamental différencie l'interface de ligne de commande Cisco de l'interface SDM ?

- L'interface SDM peut être utilisée avec une administration in band et une administration hors bande.
- L'interface de ligne de commande peut être utilisée avec une administration in band et une administration hors bande.
- L'interface SDM requiert un programme d'émulation de terminal sur le PC.
- L'interface de ligne de commande ne peut pas être utilisée sur une connexion Telnet.

## Question 9

Parmi les énoncés suivants, lesquels décrivent la fonction d'historique des commandes? (Choisissez deux réponses.)

- Elle requiert la configuration d'un tampon d'historique pour pouvoir être utilisée.
- Elle affiche les commandes récemment entrées dans le mode actuel.
- Elle enregistre la sortie des commandes **show** les plus récentes.
- Elle affiche les cinq dernières commandes entrées dans le mode de configuration globale.
- Elle est accessible grâce aux touches fléchées haut et bas.

## Question 10

Quel mode de routeur affiche une invite **Router#** ?

- Mode de configuration globale
- Mode privilégié
- Mode setup
- Mode utilisateur

## Corrigé

Reponse 1: 4

Reponse 2:  3

Reponse 3 : 3

Reponse 4 : 2

Reponse 5 : 3

Reponse 6 : 3

Reponse 7 : 2 et 5

Reponse 8 : 2

Reponse 9 : 2 et 5

Reponse 10 : 2