

Configuration de routeur de base à l'aide de SDM

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Conventions](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configuration de l'interface](#)

[Configuration NAT](#)

[Configuration du routage](#)

[Configuration - Divers](#)

[Configuration CLI](#)

[Vérifier](#)

[Dépannage](#)

[Compatibilité de SDM avec un système d'exploitation 64 bits](#)

[Impossible de lancer le SDM à travers le navigateur Web](#)

[Erreur : dépassement de pile java.bling](#)

[Informations connexes](#)

Introduction

Ce document décrit comment utiliser [Cisco Security Device Manager \(SDM\) pour définir la configuration de base du routeur](#). Cela inclut la configuration de l'adresse IP, du routage par défaut, du routage statique et dynamique, de la fonction NAT statique et dynamique, du nom d'hôte, de la bannière, du mot de passe secret, des comptes utilisateur, drapeau, mot de passe secret, des comptes d'utilisateur, et ainsi de suite. Cisco SDM vous permet de configurer votre routeur dans toutes sortes d'environnements de réseau, notamment de type succursale/bureau à distance (SOHO), succursale (BO), bureau régional et site central/sièges sociaux d'entreprise, à l'aide d'une interface de gestion conviviale basée sur le Web.

Conditions préalables

Exigences

Ce document suppose que le routeur Cisco est complètement opérationnel et configuré pour permettre au Cisco SDM d'apporter des modifications de configuration.

Remarque : référez-vous à [Autoriser l'accès HTTPS pour SDM](#) afin de permettre au routeur d'être configuré par le SDM.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Routeur Cisco 3640 avec Cisco IOS ? Version du logiciel 12.4(8)
- Cisco Security Device Manager (SDM) version 2.3.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Remarque : si vous utilisez un routeur à services intégrés Cisco (ISR), reportez-vous à [Configuration de routeur de base à l'aide de Cisco Configuration Professional](#) pour obtenir des détails de configuration similaires avec des fonctionnalités plus puissantes. Pour plus d'informations sur les routeurs qui sont pris en charge par Cisco CP, référez-vous à la section [Routeurs pris en charge](#) des Notes de version pour Cisco Configuration Professional 2.5.

Conventions

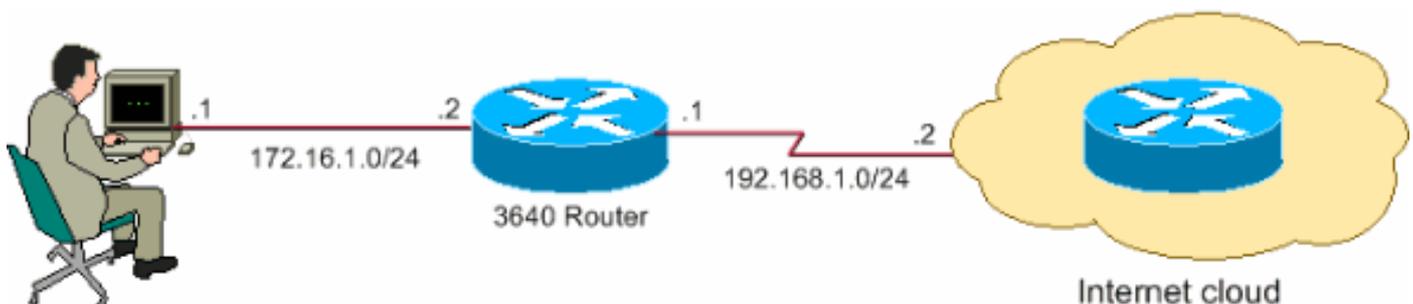
Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux [Conventions relatives aux conseils techniques Cisco](#).

Configurer

Cette section vous présente les informations pour configurer les paramètres de base pour un routeur dans un réseau.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



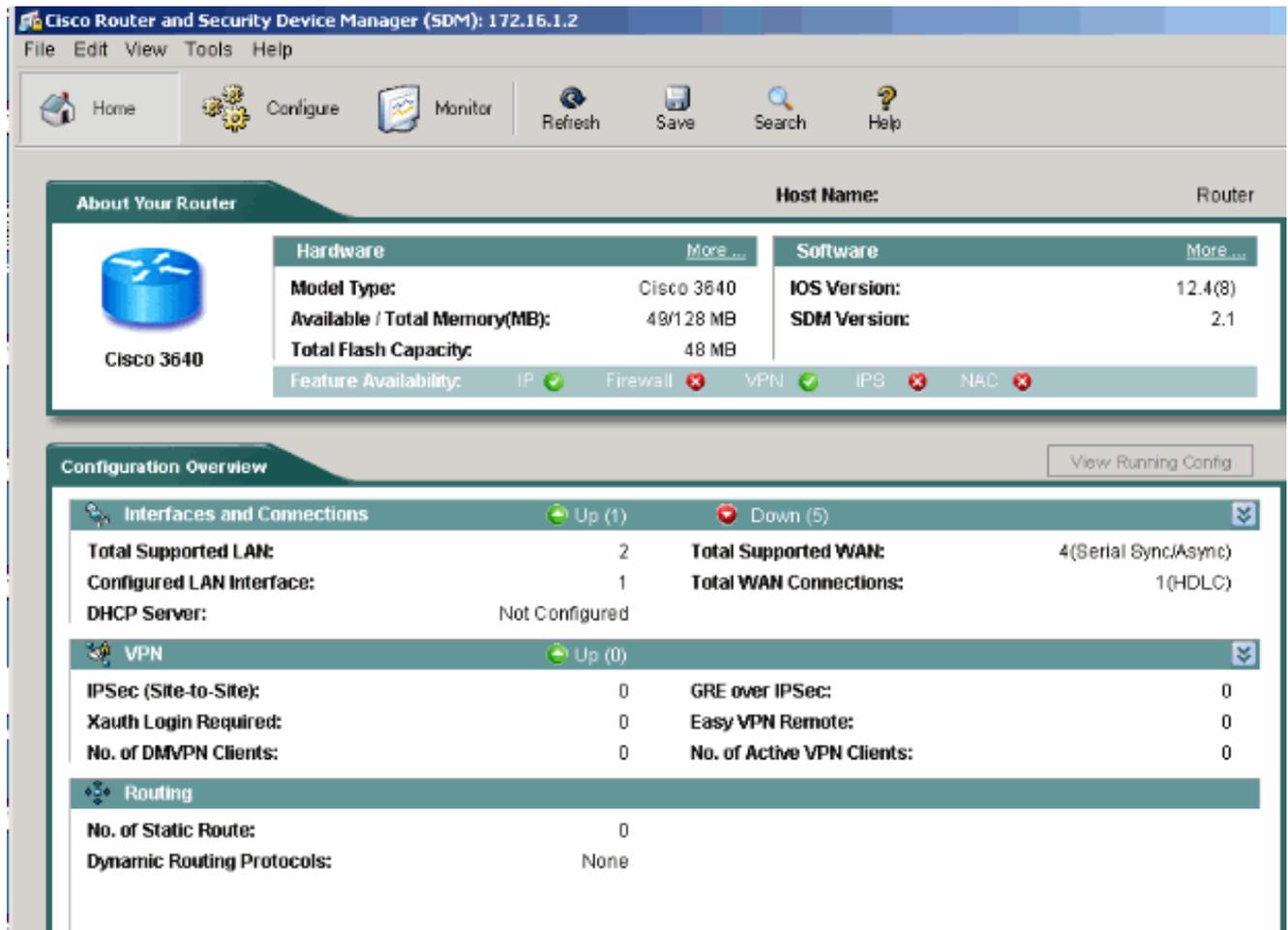
Remarque : les schémas d'adressage IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses [RFC 1918 qui ont été utilisés dans un environnement de laboratoire](#).

Configuration de l'interface

Complétez ces étapes afin de configurer les interfaces d'un routeur Cisco.

1. Cliquez sur Home afin d'aller à la page d'accueil SDM.

La page d'accueil SDM fournit des informations telles que le matériel et le logiciel du routeur, la disponibilité des fonctionnalités et un récapitulatif de la configuration. Les cercles verts montrent les fonctionnalités prises en charge dans ce routeur et les cercles rouges montrent les fonctionnalités non prises en charge.



The screenshot displays the Cisco Router and Security Device Manager (SDM) interface. The title bar indicates the device is a Cisco 3640 router with IP 172.16.1.2. The main content area is divided into two sections: 'About Your Router' and 'Configuration Overview'.

About Your Router: This section provides details about the router's hardware and software. The hardware information includes the model type (Cisco 3640), available and total memory (48/128 MB), and total flash capacity (48 MB). The software information includes the IOS version (12.4(8)) and the SDM version (2.1). A feature availability bar at the bottom shows the status of various features: IP (green), Firewall (red), VPN (green), IPS (red), and NAC (red).

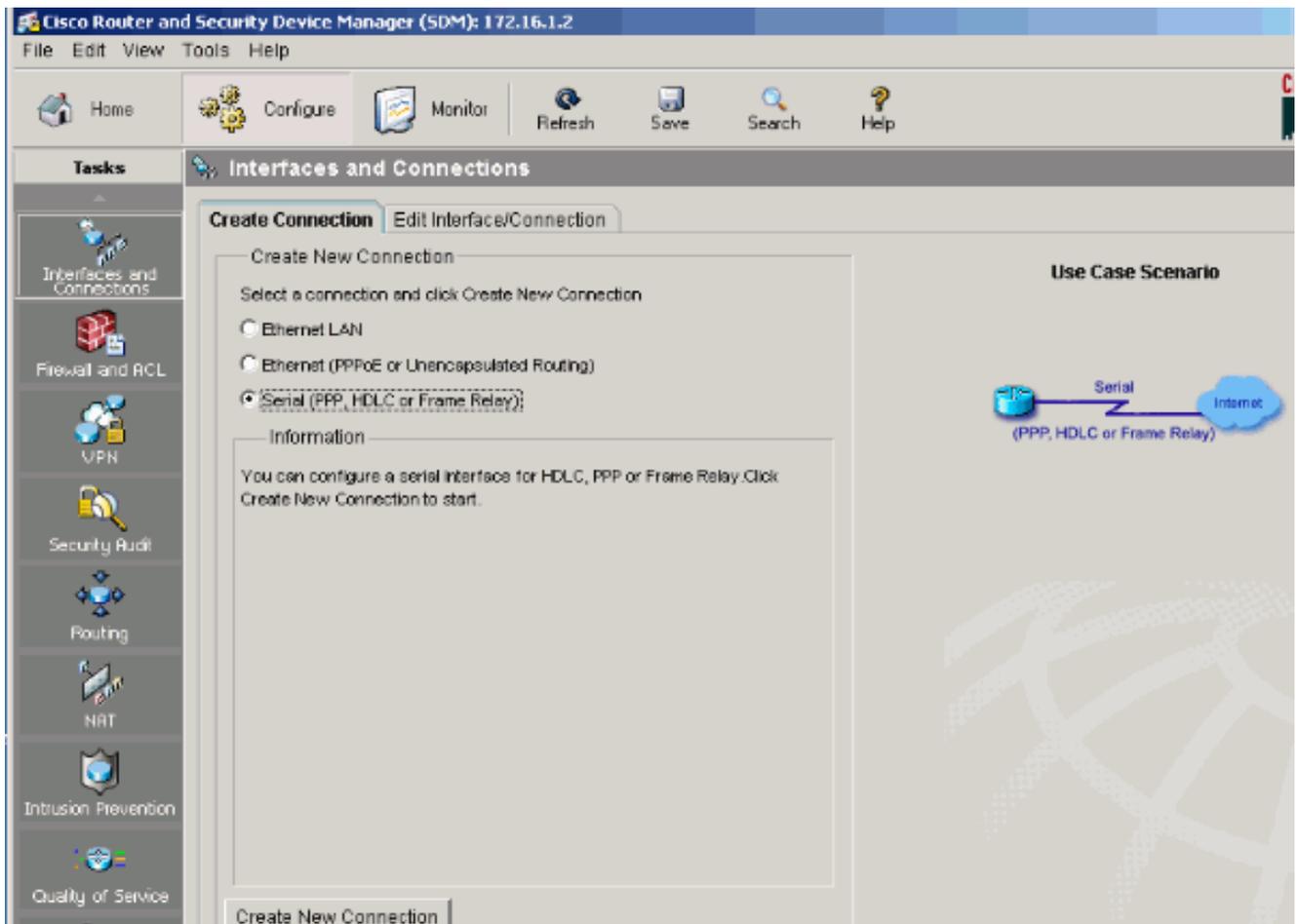
Configuration Overview: This section provides a summary of the router's configuration. It includes a 'View Running Config' button and a table of configuration details.

Interfaces and Connections		VPN		Routing	
Total Supported LAN:	2	Total Supported WAN:	4(Serial Sync/Async)	No. of Static Route:	0
Configured LAN Interface:	1	Total WAN Connections:	1(HDLC)	Dynamic Routing Protocols:	None
DHCP Server:	Not Configured	IPSec (Site-to-Site):	0		
		Xauth Login Required:	0		
		No. of DMVPN Clients:	0		
		GRE over IPSec:	0		
		Easy VPN Remote:	0		
		No. of Active VPN Clients:	0		

2. Choisissez Configure > Interfaces and Connections > Create Connection afin de configurer la connexion WAN pour l'interface.

Comme exemple, pour l'interface série 2/0, choisissez l'option Serial et cliquez Create New Connection.

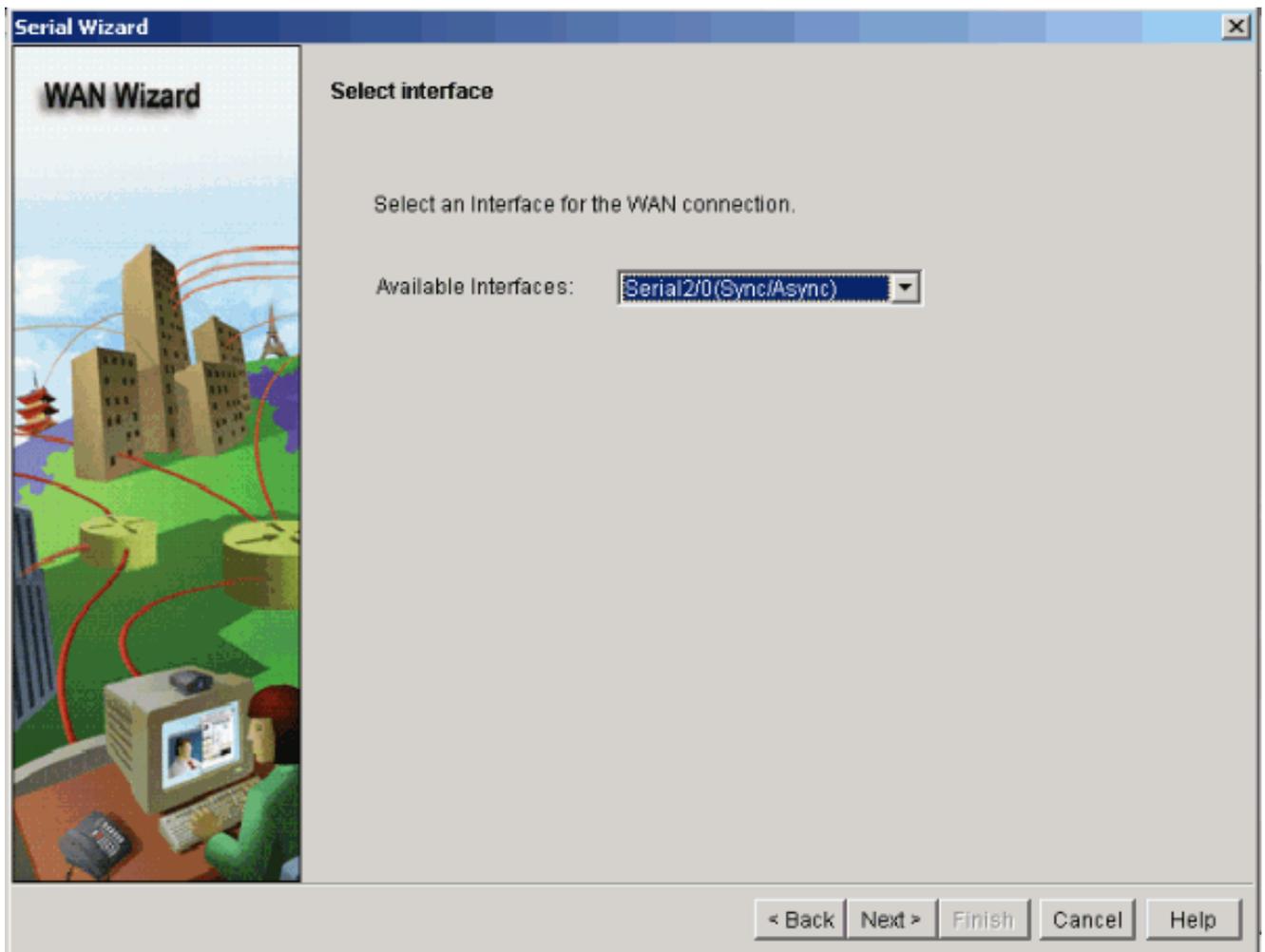
Remarque : pour d'autres types d'interfaces comme Ethernet, choisissez le type d'interface correspondant et continuez en cliquant sur le bouton Create New Connection.



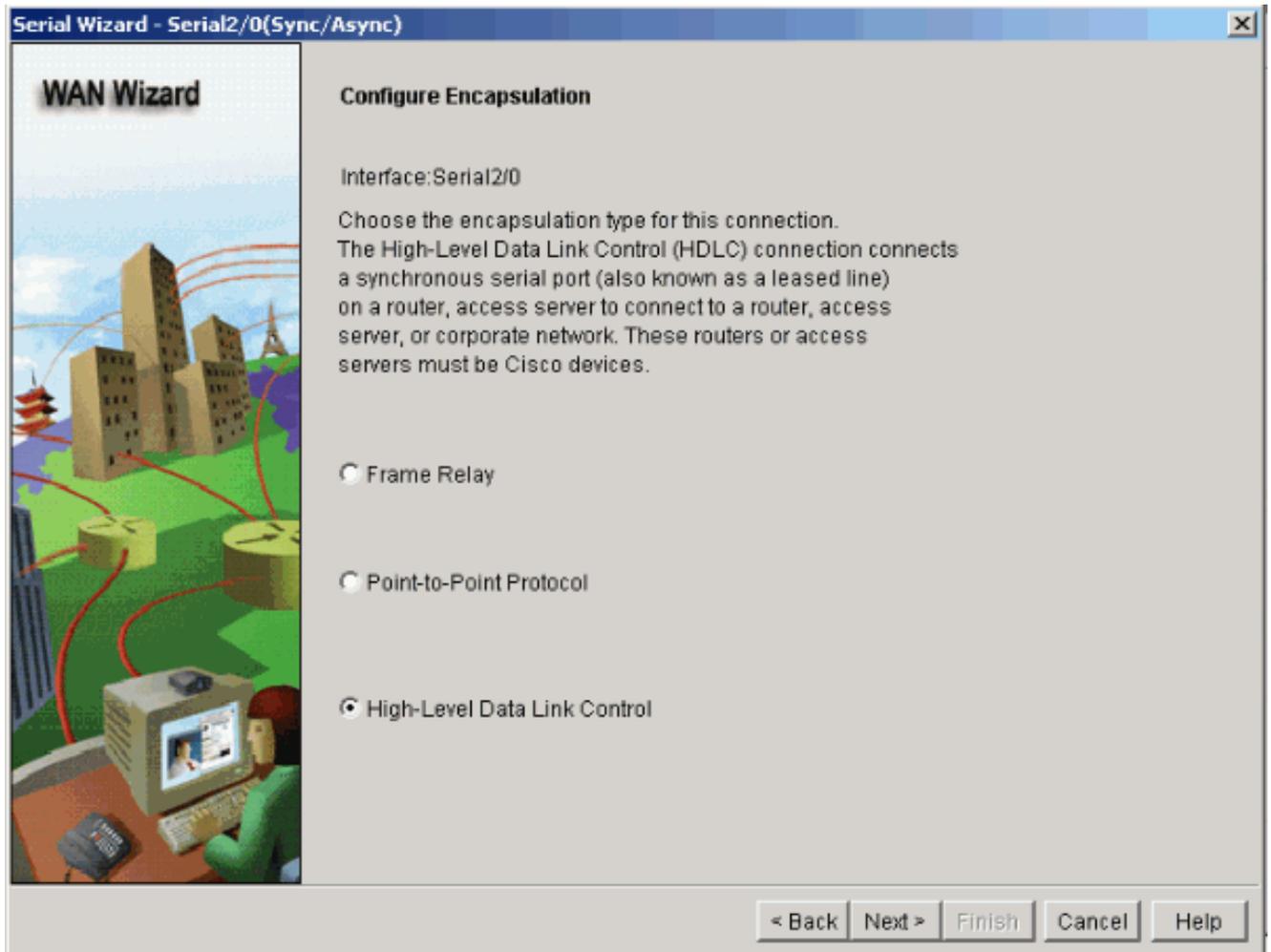
3. Cliquez sur Next afin de poursuivre une fois que cette interface apparaît.



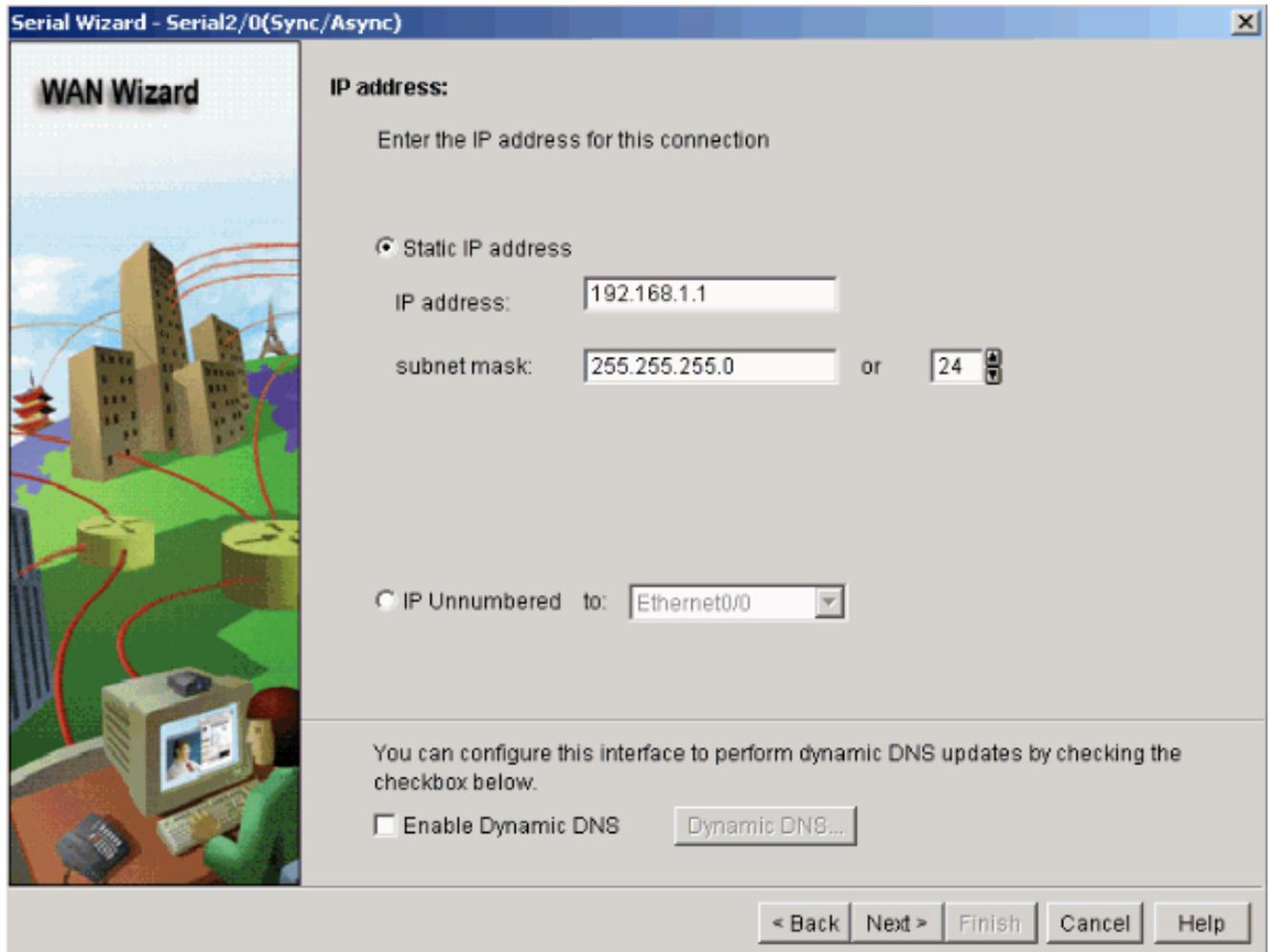
4. Sélectionnez Serial interface 2/0 (souhaitée) à partir de l'option Available Interfaces et cliquez sur Next.



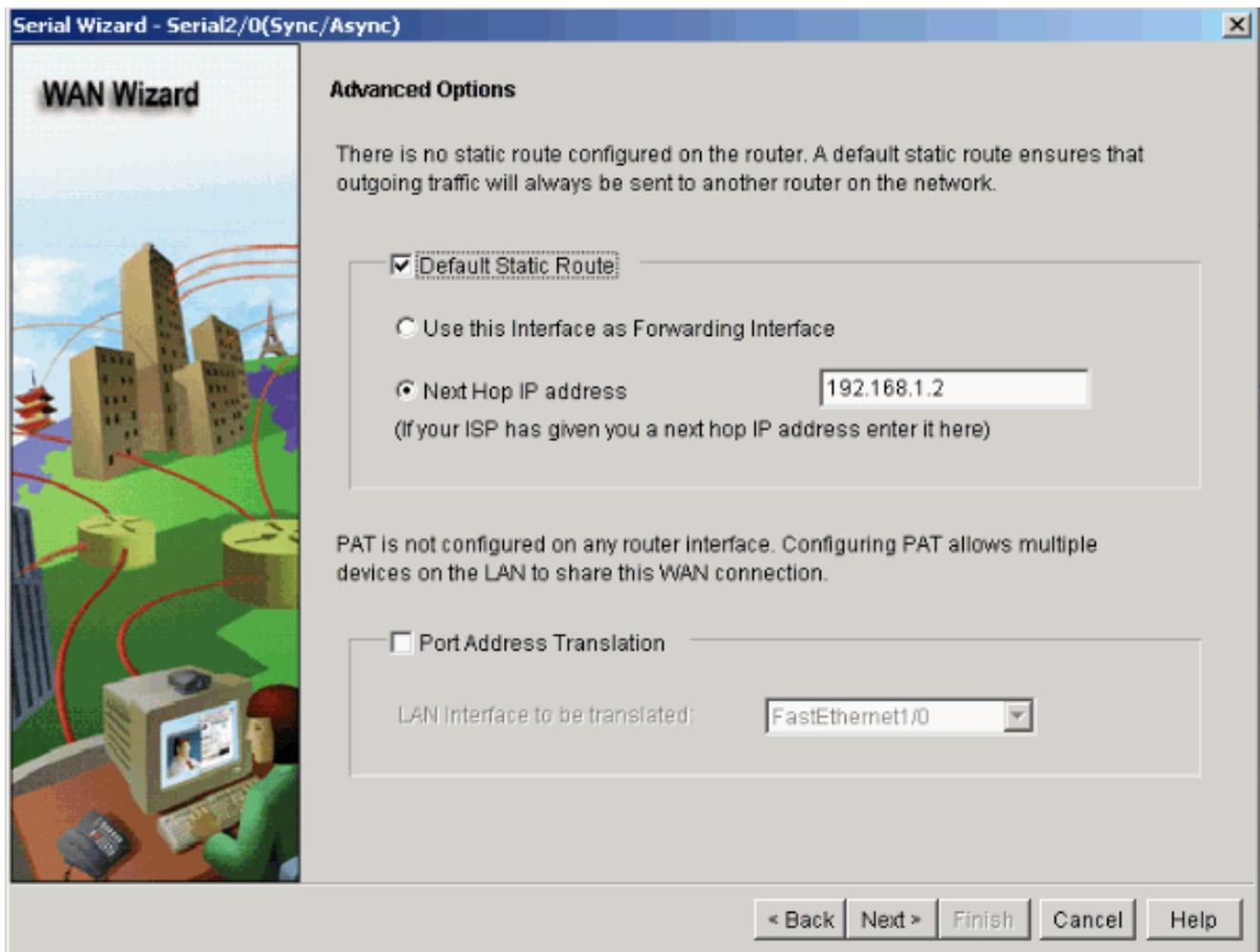
5. Choisissez le type d'encapsulation pour l'interface série et cliquez sur Next.



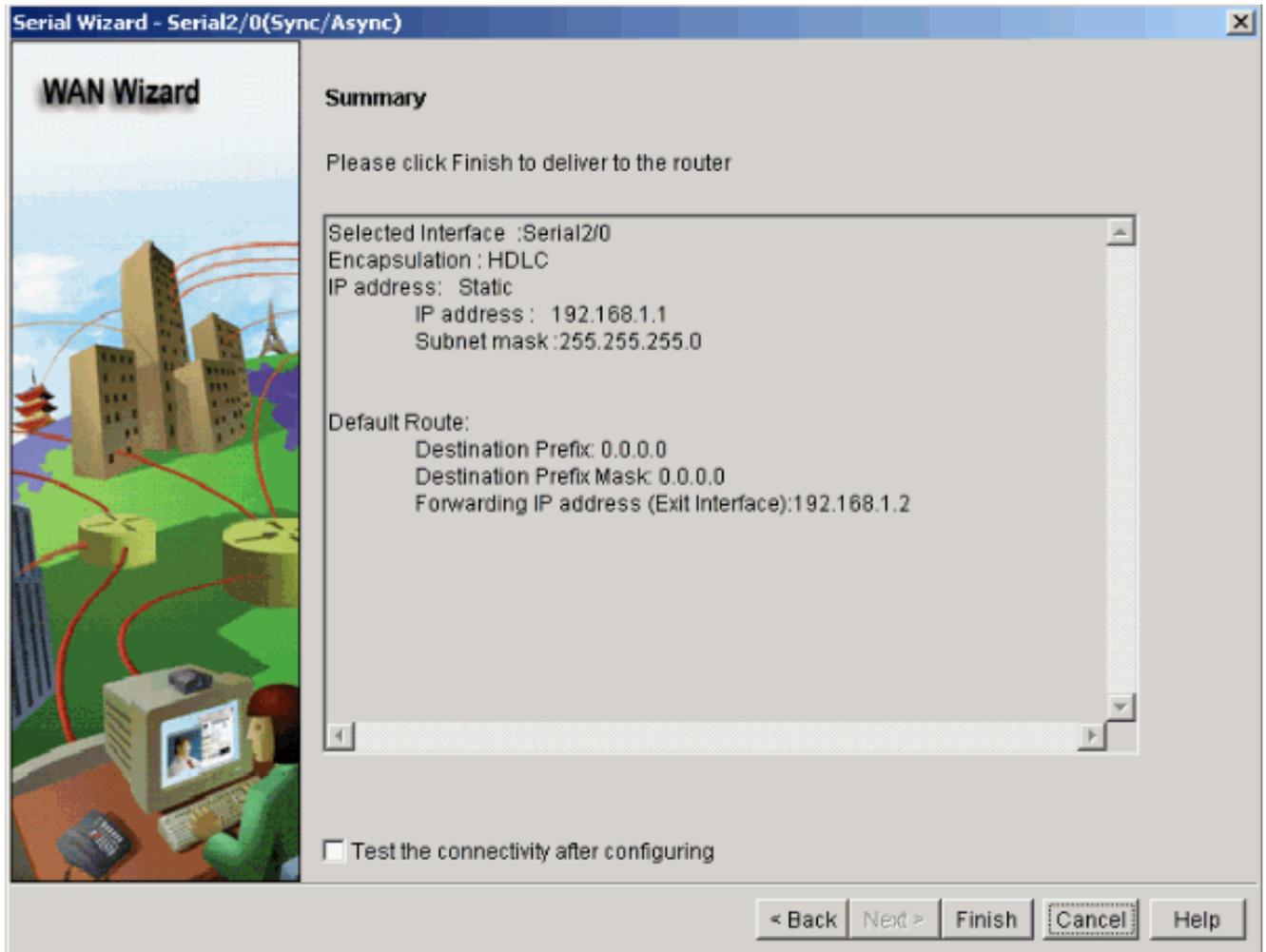
6. Spécifiez l'adresse IP statique avec le masque de sous-réseau correspondant pour l'interface et cliquez sur Next.



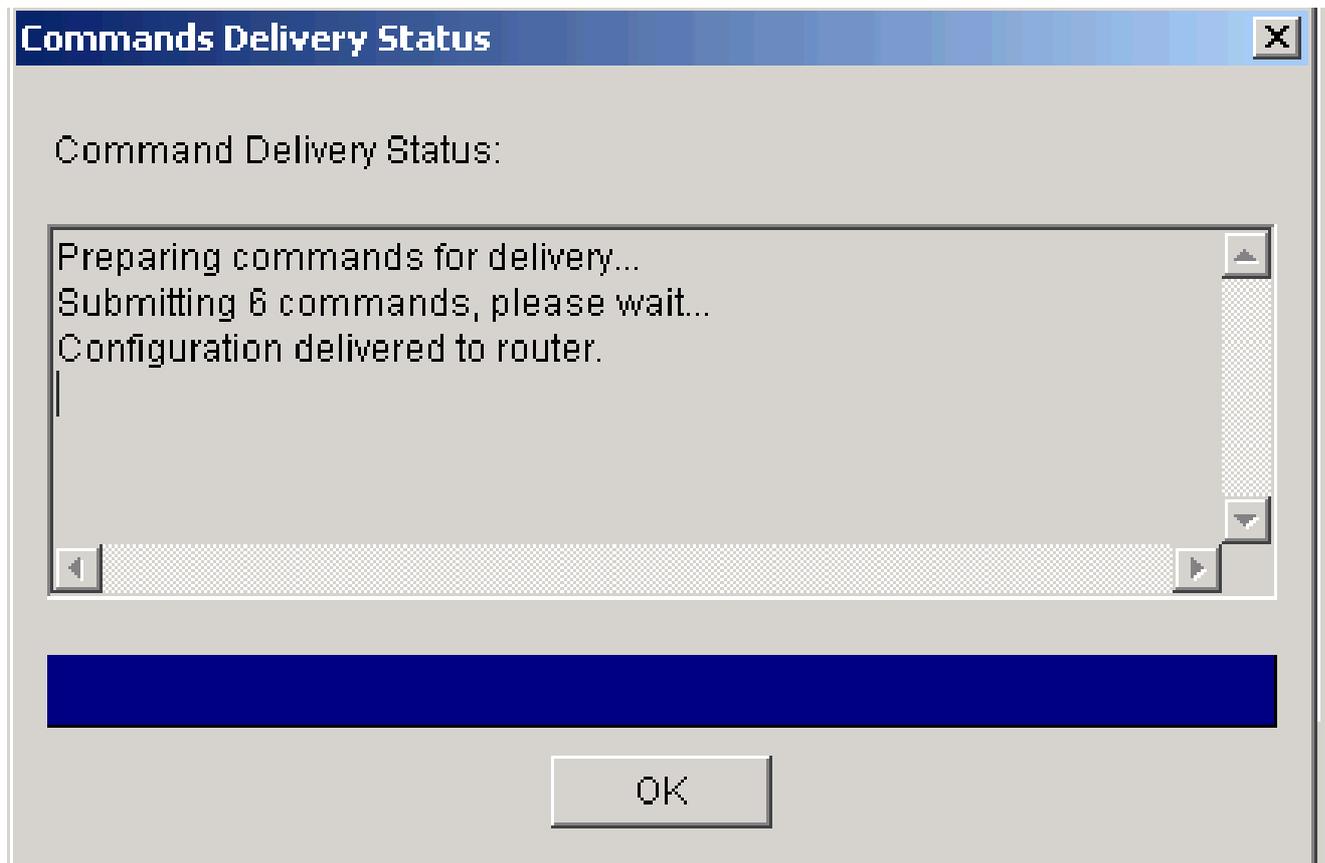
7. Configurez le routage par défaut avec des paramètres facultatifs tels que l'adresse IP du prochain saut (192.168.1.2 selon le diagramme de réseau) fournie par l'ISP et cliquez sur Next.



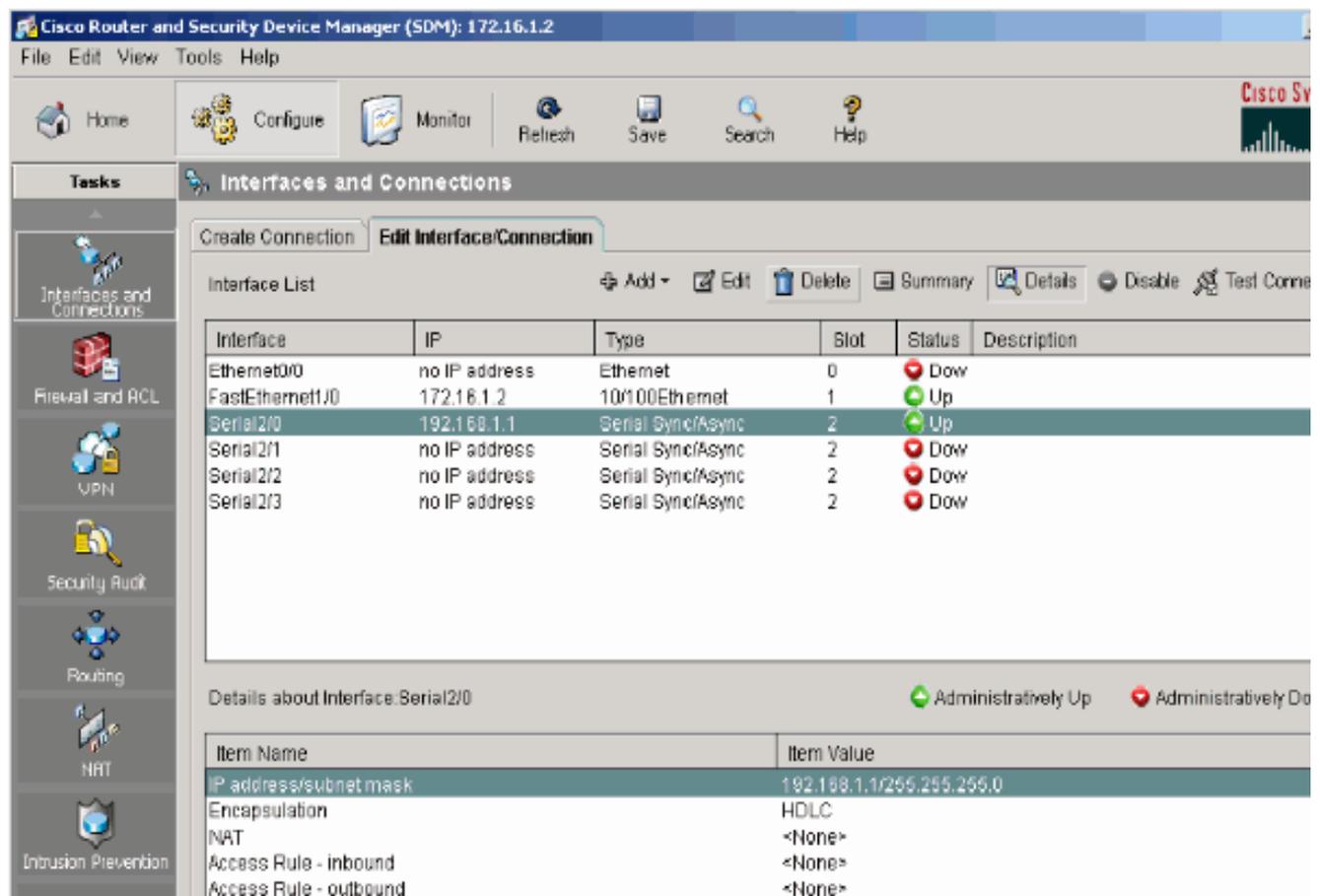
Cette fenêtre apparaît et montre le récapitulatif de configuration configuré par l'utilisateur. Cliquez sur Finish (Terminer).



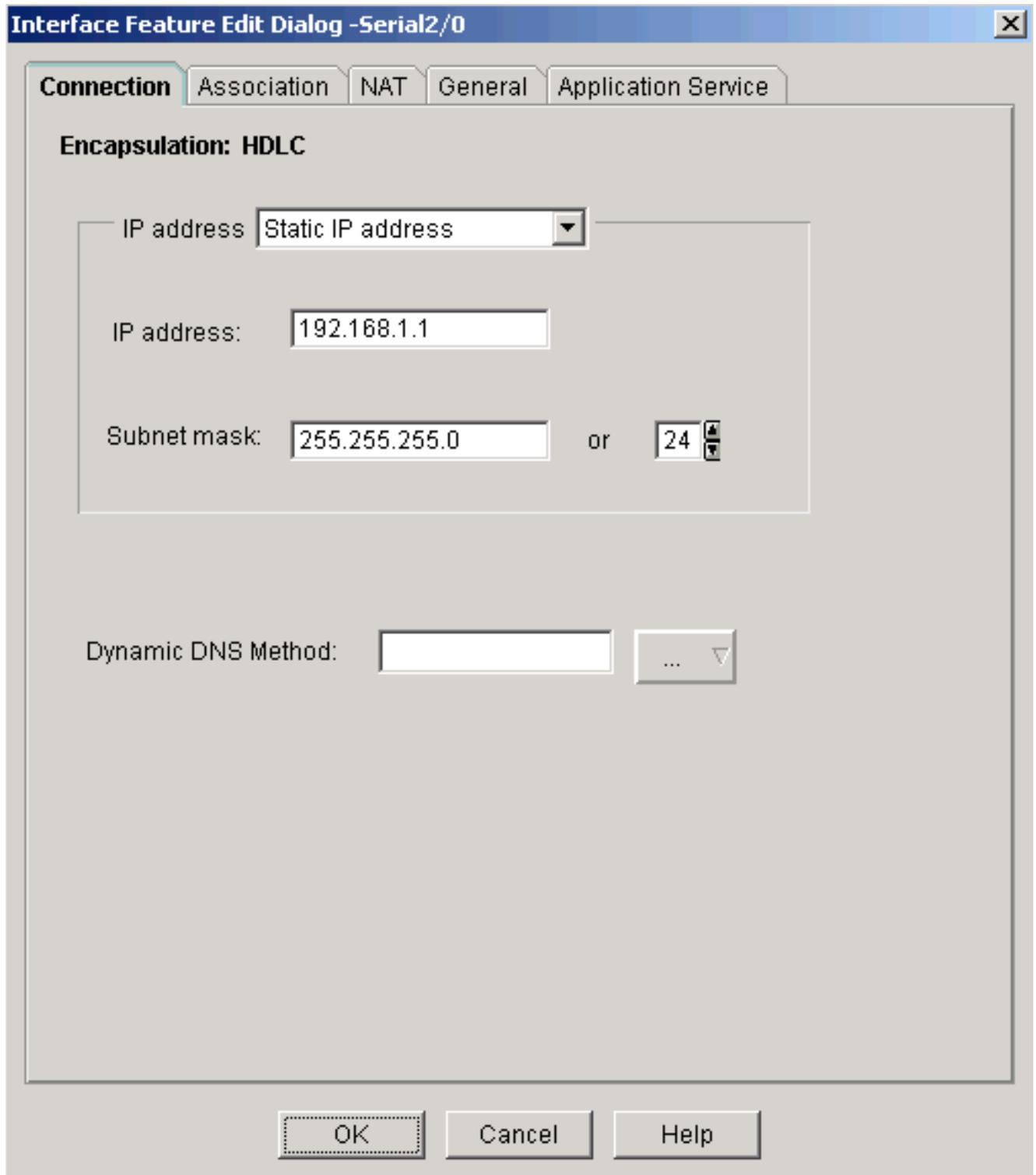
Cette fenêtre apparaît et montre l'état de livraison de la commande au routeur. Sinon, elle affiche des erreurs si la livraison de la commande échoue en raison de commandes incompatibles ou des fonctions non prises en charge.



8. Choisissez Configure > Interfaces and Connections > Edit Interfaces/Connections afin d'ajouter/modifier/supprimer les différentes interfaces.



Sélectionnez l'interface avec laquelle vous souhaitez faire des modifications et cliquez sur Edit si vous voulez modifier la configuration de l'interface. Là vous pouvez modifier l'adresse IP statique existante.

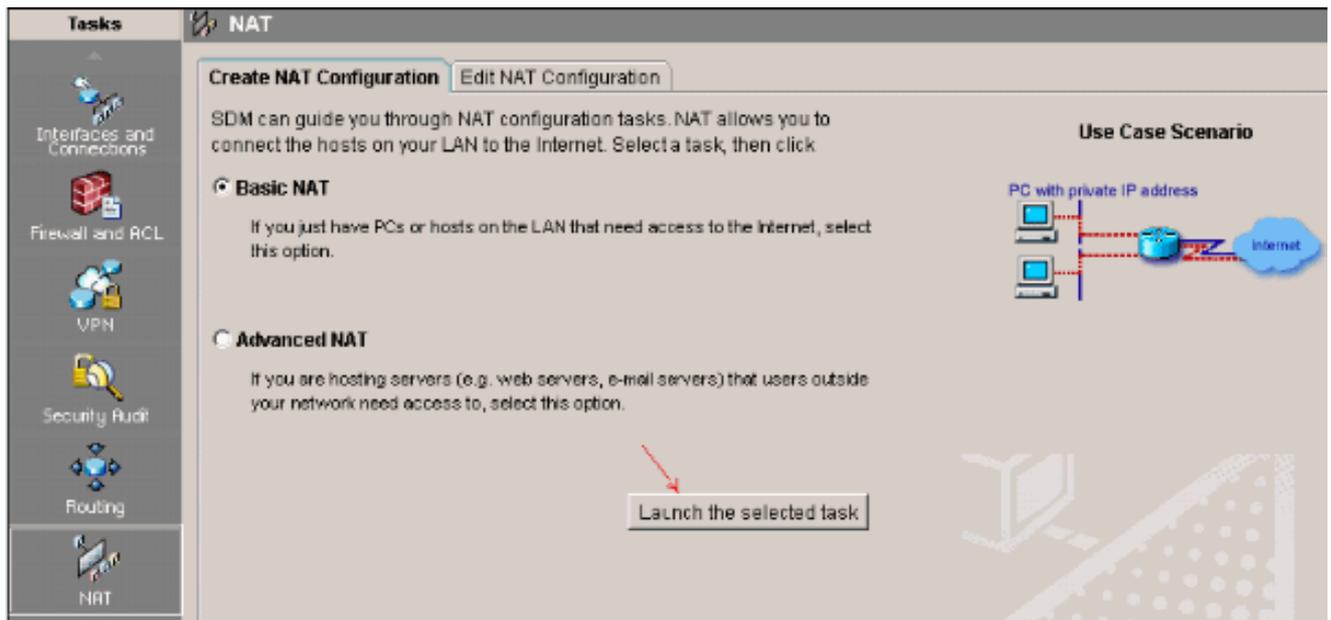


Configuration NAT

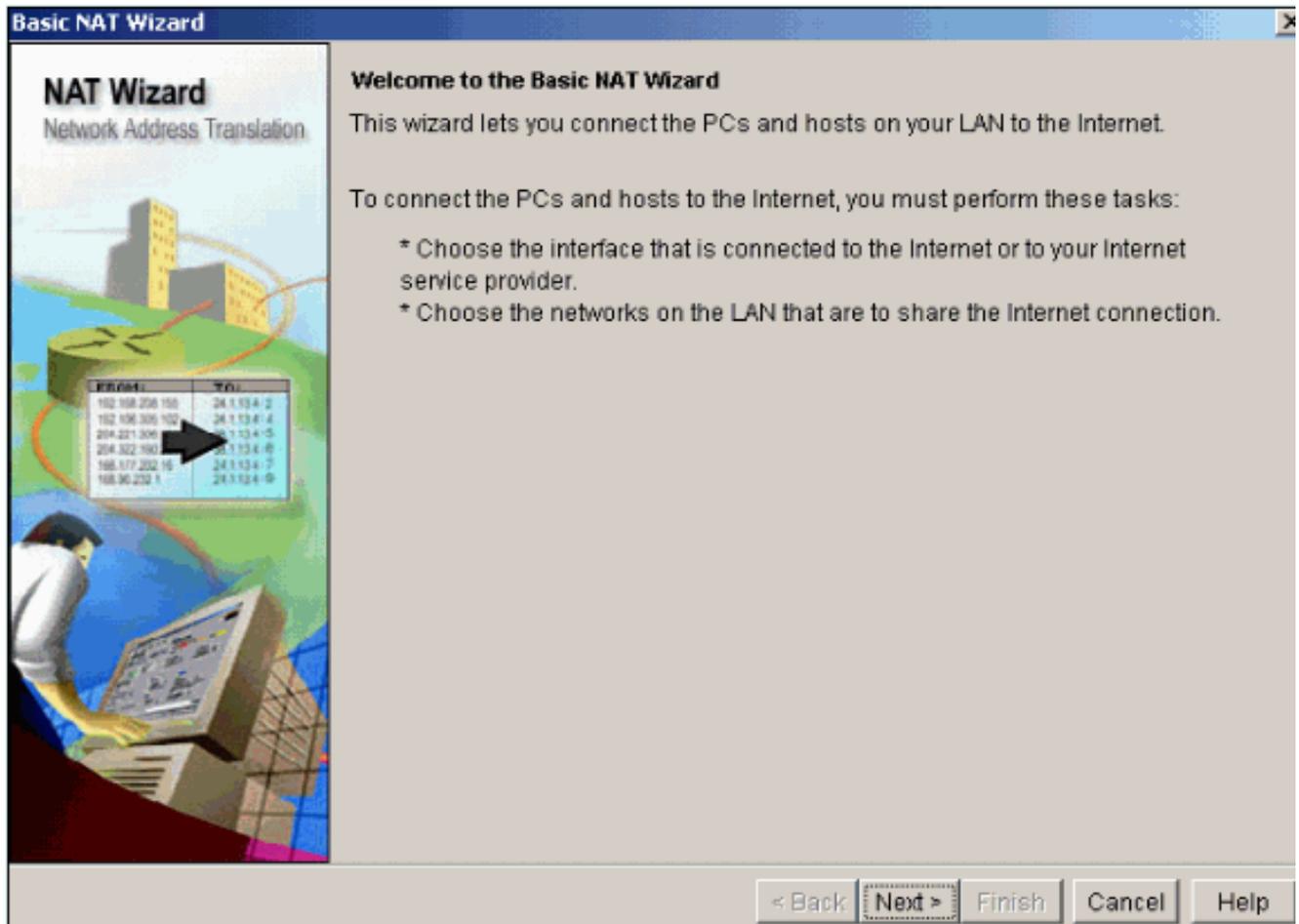
Configuration NAT dynamique

Complétez ces étapes afin de configurer la fonction NAT dynamique dans un routeur Cisco.

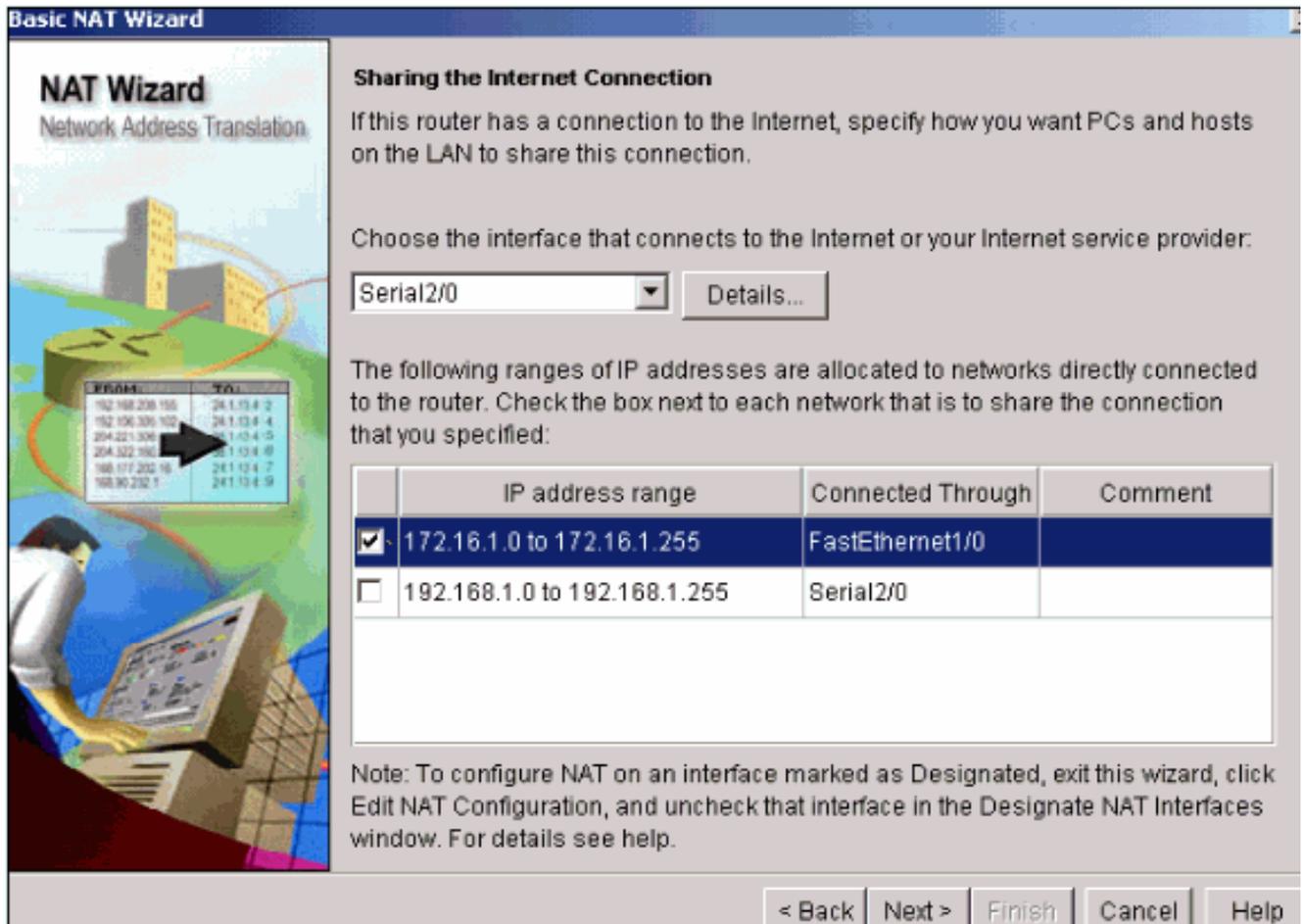
1. Choisissez Configure > NAT > Basic NAT et cliquez sur Launch the selected task afin de configurer la fonction NAT de base.



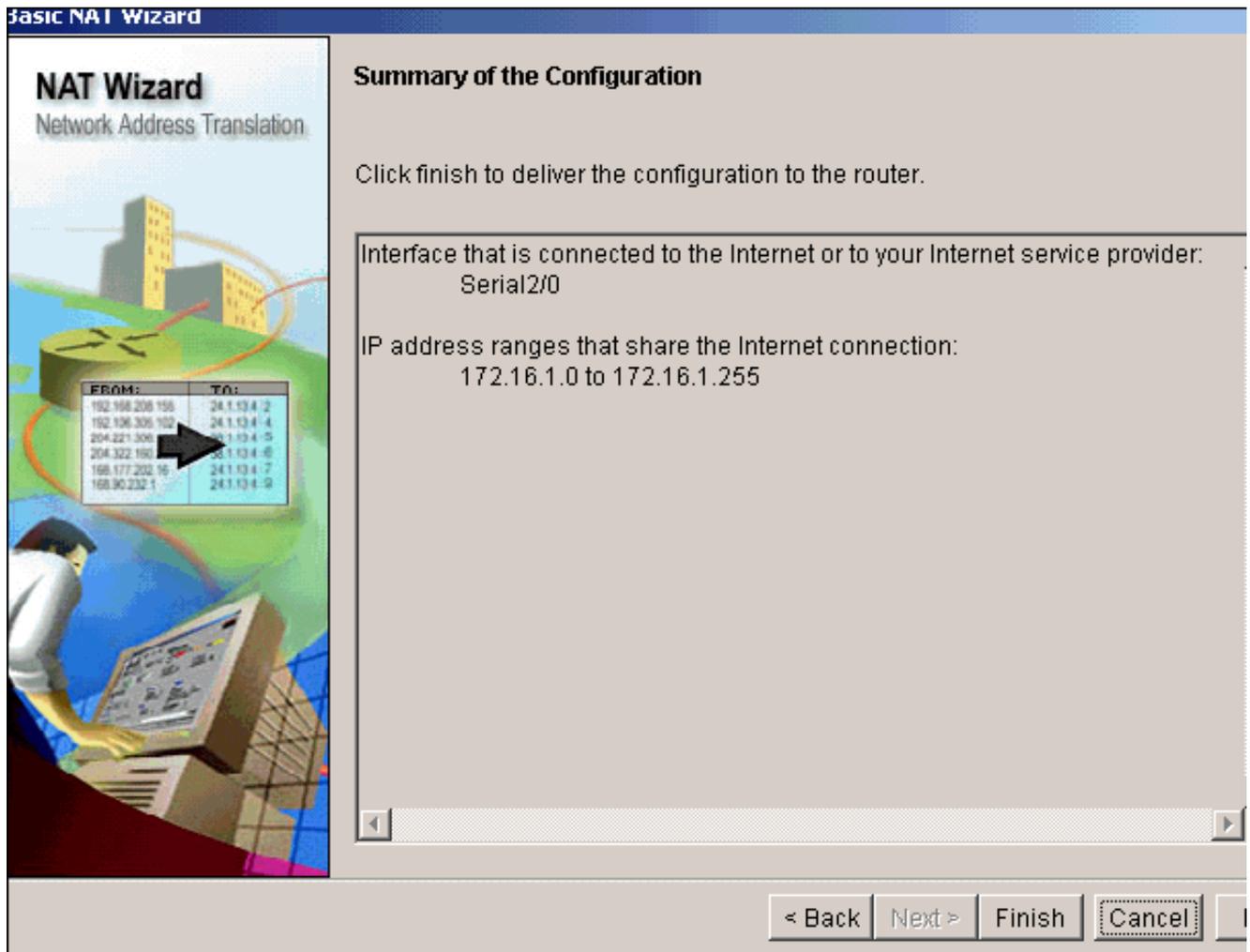
2. Cliquez sur Next (Suivant).



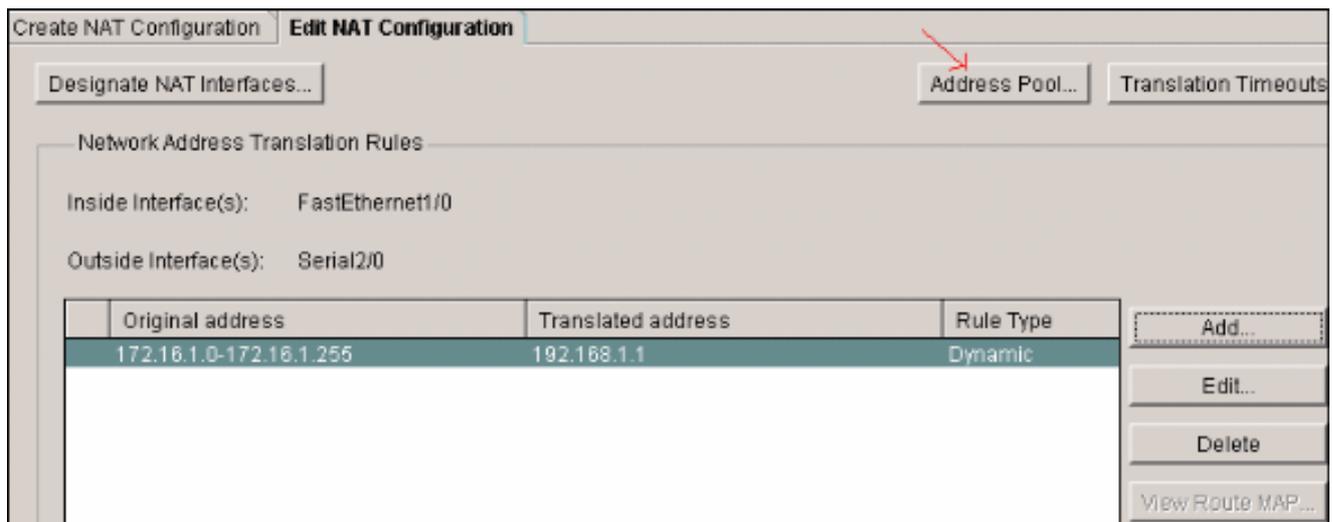
3. Choisissez l'interface qui se connecte à l'Internet ou à votre ISP et choisissez la plage d'adresses IP avec laquelle l'accès Internet doit être partagé.



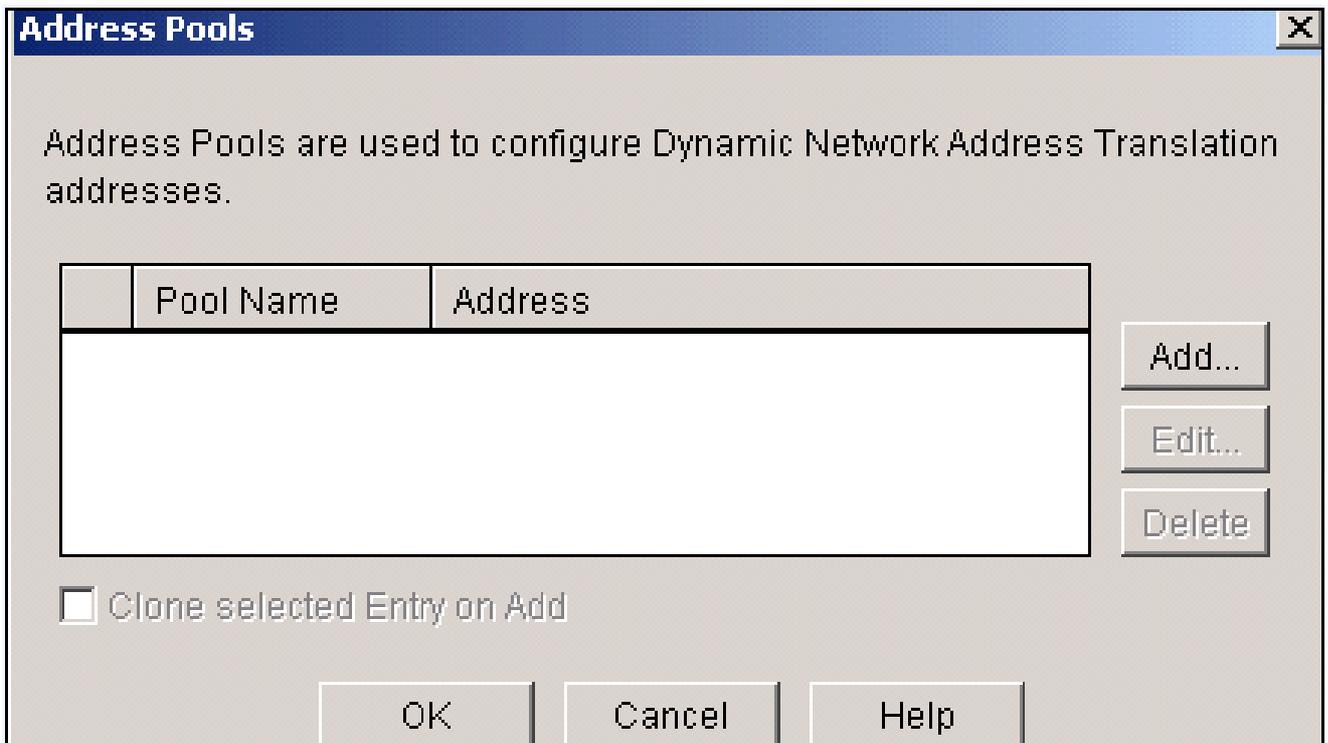
4. Cette fenêtre apparaît et montre le récapitulatif de configuration configuré par l'utilisateur. Cliquez sur Finish (Terminer).



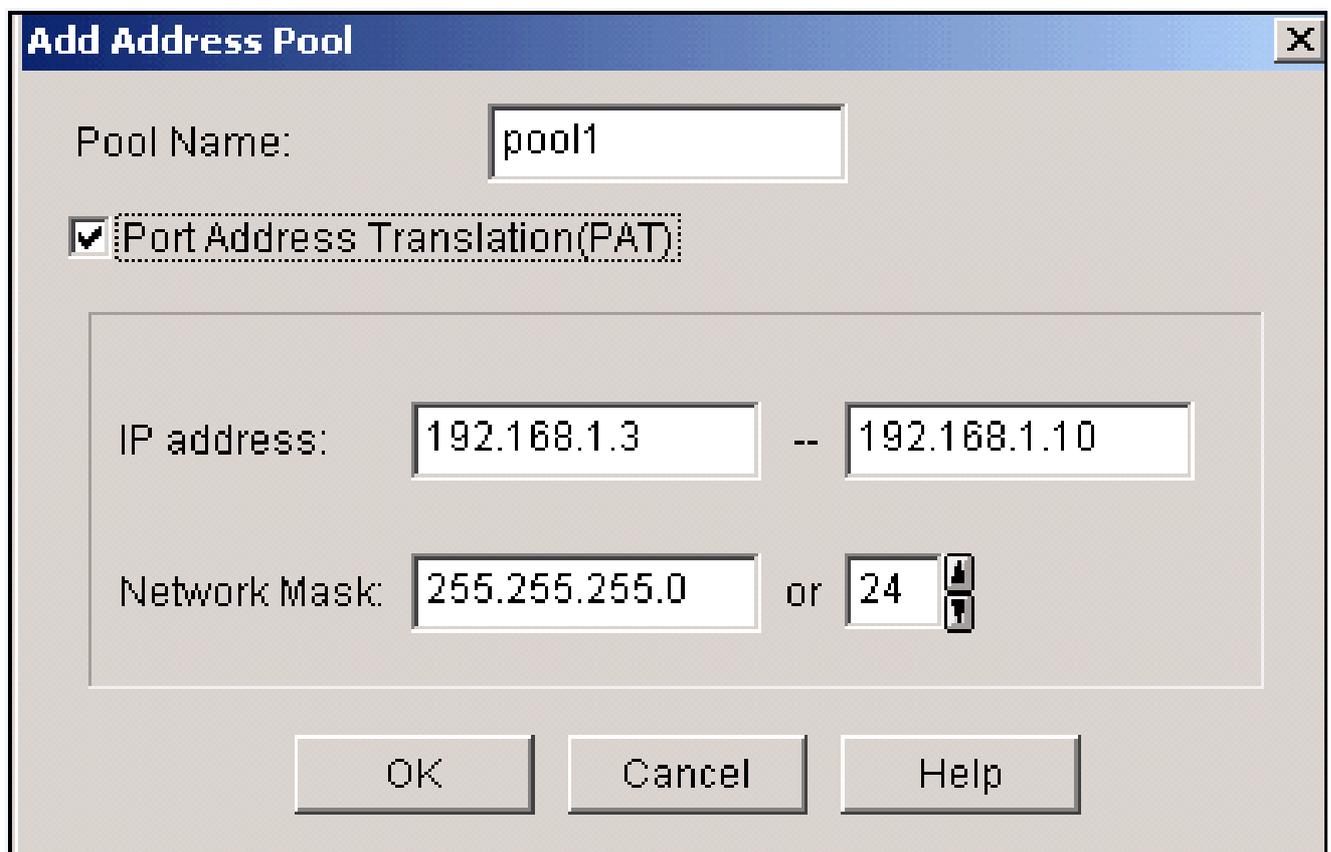
5. La fenêtre Edit NAT Configuration montre la configuration NAT dynamique avec l'adresse IP traduite surchargée (fonction PAT). Si vous voulez configurer le NAT dynamique avec un pool d'adresse, cliquez sur Address Pool.



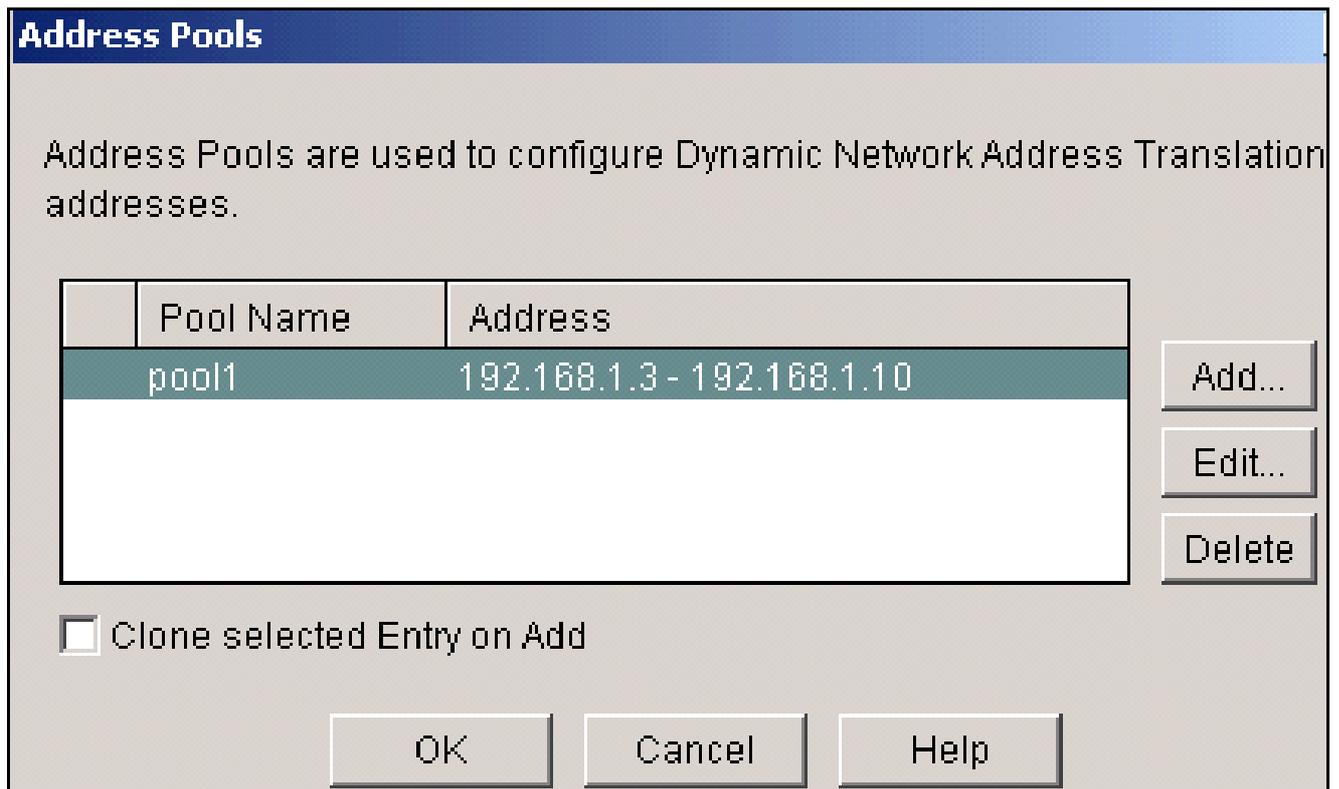
6. Cliquez sur Add.



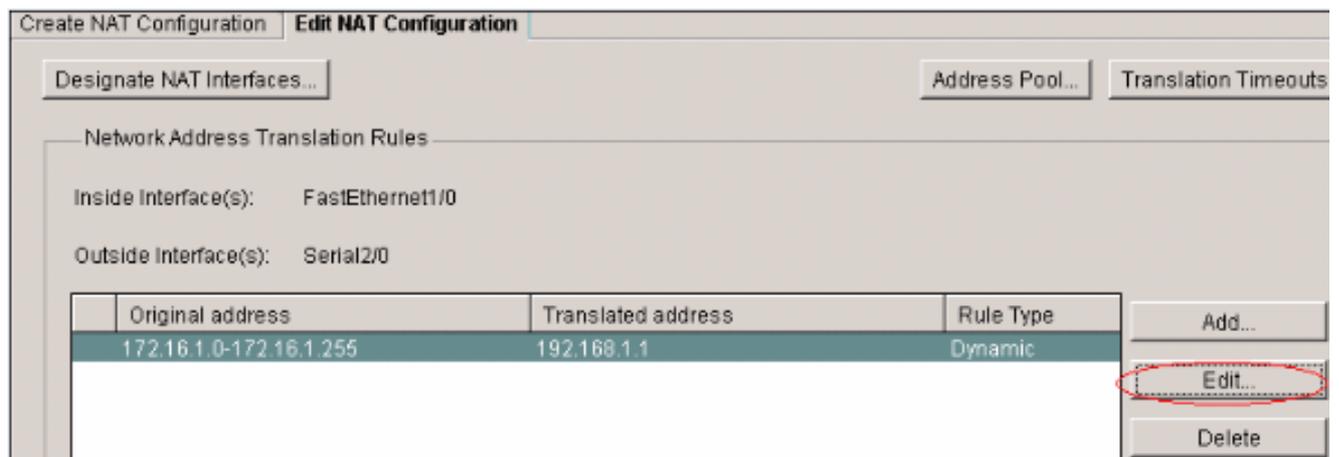
Ici sont fournies des informations telles que le nom du pool et la plage d'adresses IP avec un masque de réseau. Il peut y avoir des périodes où la majeure partie des adresses du pool ont été affectées et où le pool d'adresses IP est presque épuisé. Quand cela se produit, la fonction PAT peut être utilisée avec une adresse IP unique afin de satisfaire les demandes supplémentaires d'adresses IP. Activez la case Port Address Translation (PAT) si vous voulez que le routeur utilise la fonction PAT lorsque le pool d'adresses est presque épuisé.



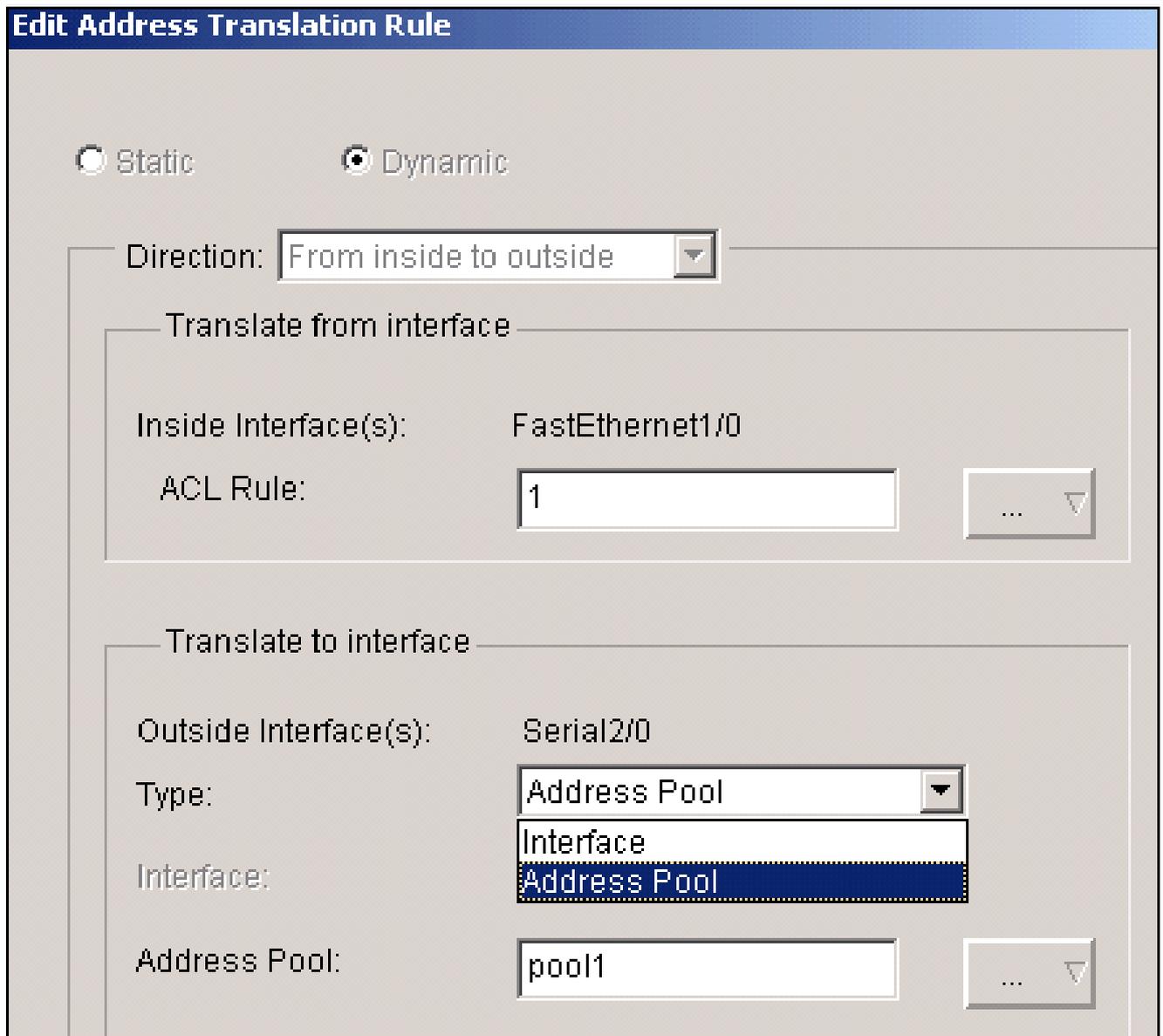
7. Cliquez sur Add.



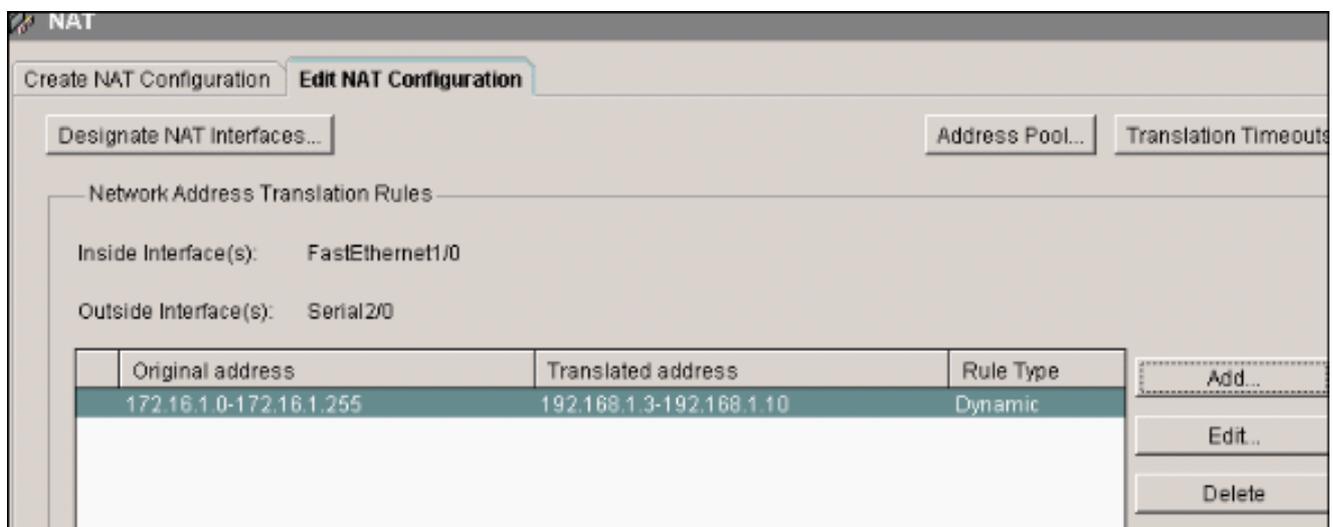
8. Cliquez sur Edit.



9. Choisissez Address Pool dans la zone Type, donnez le nom du pool d'adresses, pool1 , et cliquez sur OK.



10. Cette fenêtre montre la configuration de la fonction NAT dynamique avec le pool d'adresses. Cliquez sur Designate NAT Interfaces.



Utilisez cette fenêtre afin de désigner les interfaces internes et externes que vous voulez

utiliser dans les traductions NAT. La fonction NAT utilise les désignations d'intérieur et d'extérieur quand elle interprète des règles de traduction parce que les traductions sont effectuées de l'intérieur vers l'extérieur, ou de l'extérieur vers l'intérieur.

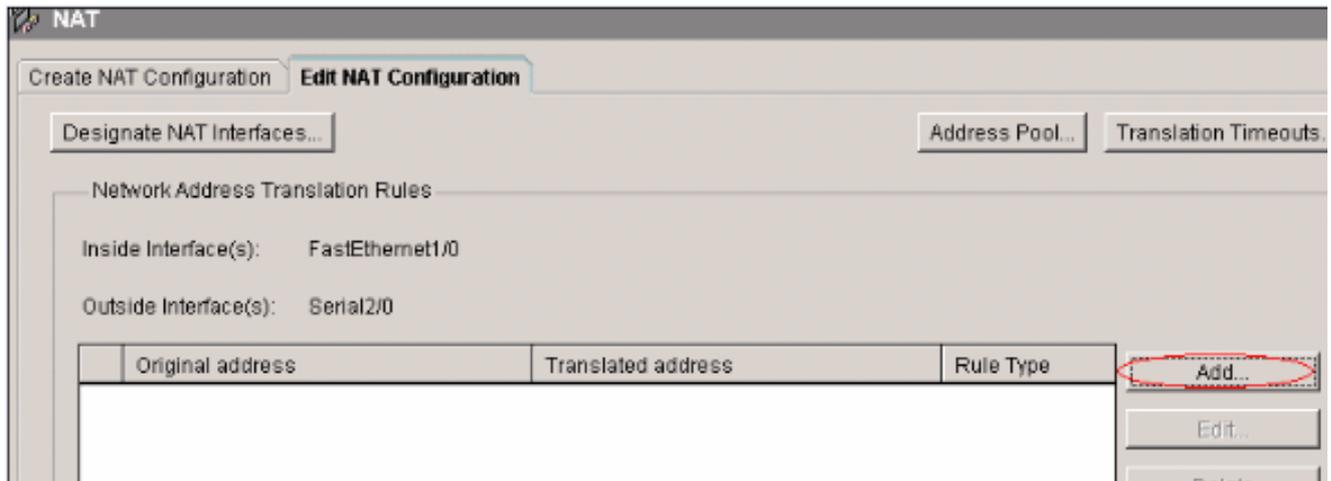
Une fois désignées, ces interfaces sont utilisées dans toutes les règles de traduction NAT. Les interfaces désignées apparaissent au-dessus de la liste de règles de traduction (Translation Rules) dans la fenêtre NAT principale.

interface	inside(trusted)	outside(untruste)
FastEthernet1/0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Serial2/0	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Configuration NAT statique

Complétez ces étapes afin de configurer la fonction NAT statique dans un routeur Cisco.

1. Choisissez Configure > NAT > Edit NAT Configuration et cliquez sur Add afin de configurer la fonction NAT statique.



2. Choisissez la Direction , soit de l'intérieur vers l'extérieur, soit de l'extérieur vers l'intérieur, spécifiez l'adresse IP intérieure à traduire en dessous de Translate from Interface. Pour la zone Translate to Interface , sélectionnez le Type.

- Choisissez IP Address si vous voulez que l'adresse Translate from Address soit traduite en une adresse IP définie dans la zone IP Address.
- Choisissez Interface si vous voulez que l'option Translate from Address utilise l'adresse d'une interface sur le routeur. L'adresse Translate from Address est traduite dans l'adresse IP affectée à l'interface que vous spécifiez dans la zone Interface.

Activez la case à cocher Redirect Port si vous voulez inclure les informations sur le port pour le périphérique interne dans la traduction. Cela vous permet d'utiliser la même adresse IP publique pour plusieurs périphériques, à condition qu'un port différent soit spécifié pour chaque périphérique. Vous devez créer une entrée pour chaque mappage de ports pour cette adresse traduite (Translated to). Cliquez sur TCP s'il s'agit d'un numéro de port TCP et cliquez sur UDP s'il s'agit d'un numéro de port UDP. Dans la zone Original Port, entrez le numéro du port sur le périphérique interne. Dans la zone Translated Port, entrez le numéro du port que le routeur doit utiliser pour cette traduction. Reportez-vous à la section [Autoriser Internet à accéder aux périphériques internes](#) de [Configuration de la traduction d'adresses réseau : Mise en route](#).

Add Address Translation Rule [X]

Static Dynamic

Direction:

Translate from interface

Inside Interface(s):

IP address:

Network Mask(optional): or

Translate to interface

Outside Interface(s):

Type:

Interface:

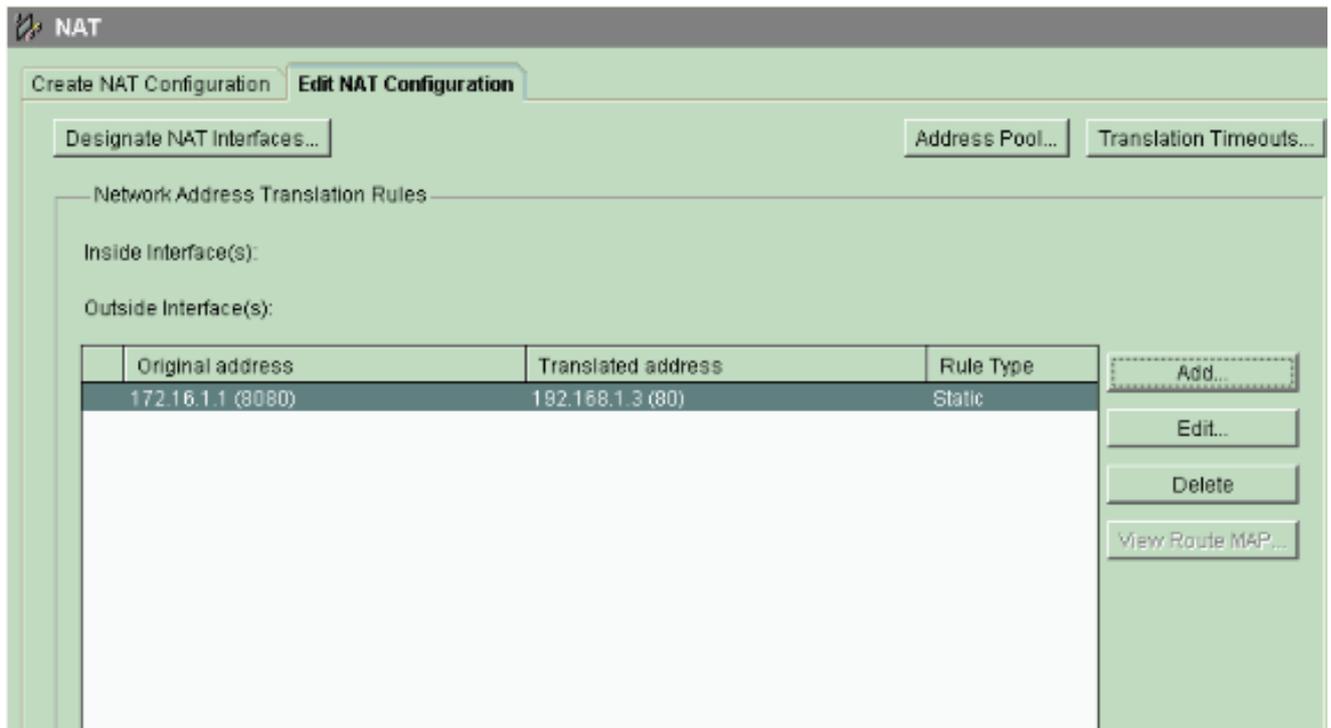
IP address:

Redirect Port

TCP UDP

Original Port: Translated Port:

Cette fenêtre montre la configuration de la fonction NAT statique avec la redirection de port activée.

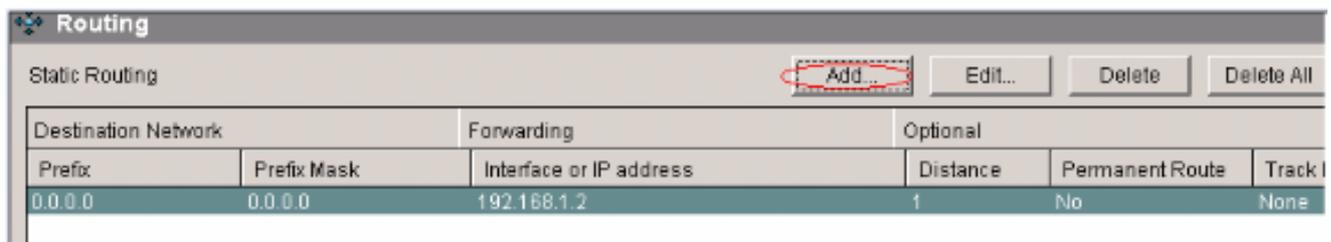


Configuration du routage

Configuration du routage statique

Complétez ces étapes afin de configurer le routage statique dans un routeur Cisco.

1. Choisissez Configure > Routing > Static Routing et cliquez sur Add afin de configurer le routage statique.



2. Entrez l'adresse du réseau de destination (Destination Network) avec le masque et sélectionnez soit l'interface sortante, soit l'adresse IP du prochain saut.

Add IP Static Route

Destination Network

Prefix:

Prefix Mask:

Make this as the default route

Forwarding(Next Hop)

Interface:

IP Address:

Optional

Distance metric for this route:

Permanent route

OK

Cancel

Help

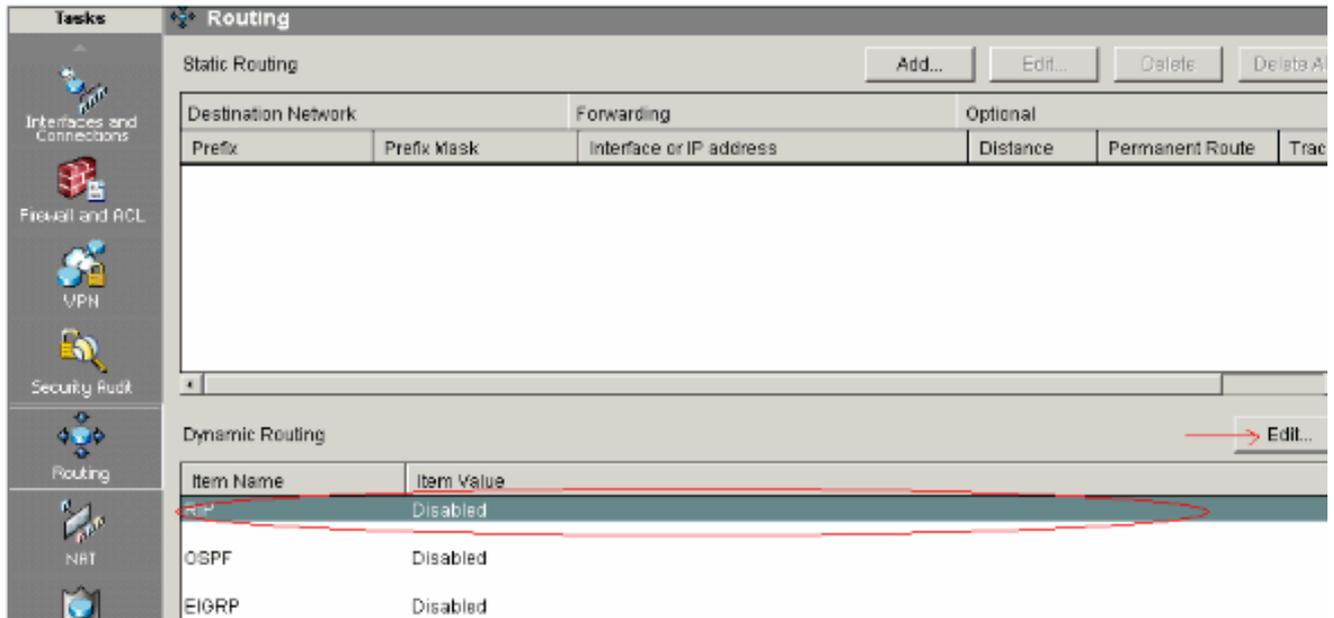
Cette fenêtre montre la route statique configurée pour le réseau 10.1.1.0 avec 192.168.1.2 comme adresse IP du prochain saut.

Routing						
Static Routing						
Destination Network		Forwarding		Optional		
Prefix	Prefix Mask	Interface or IP address		Distance	Permanent Route	Track
10.1.1.0	255.255.255.0	192.168.1.2		1	No	None

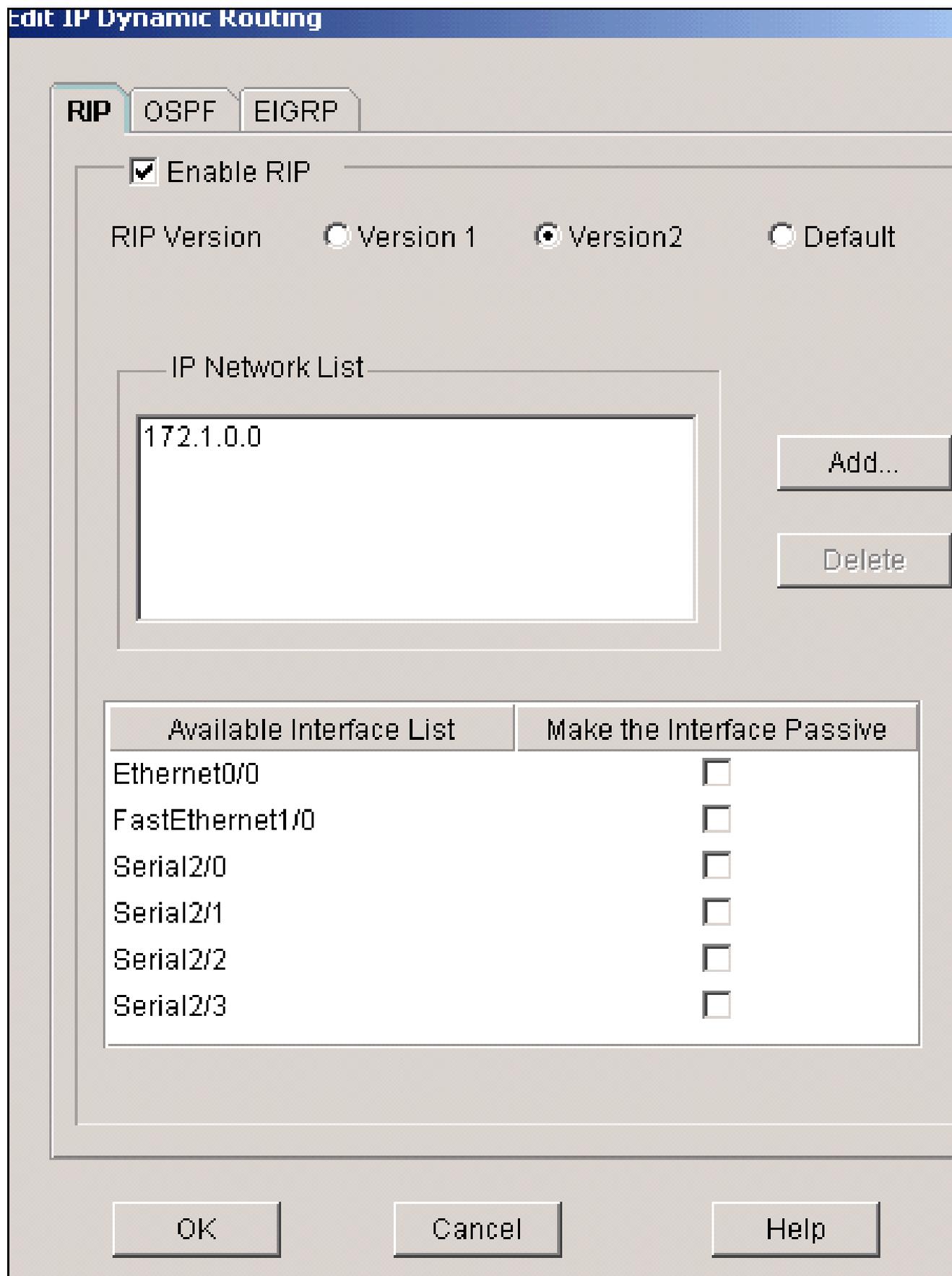
Configuration du routage dynamique

Complétez ces étapes afin de configurer le routage dynamique dans un routeur Cisco.

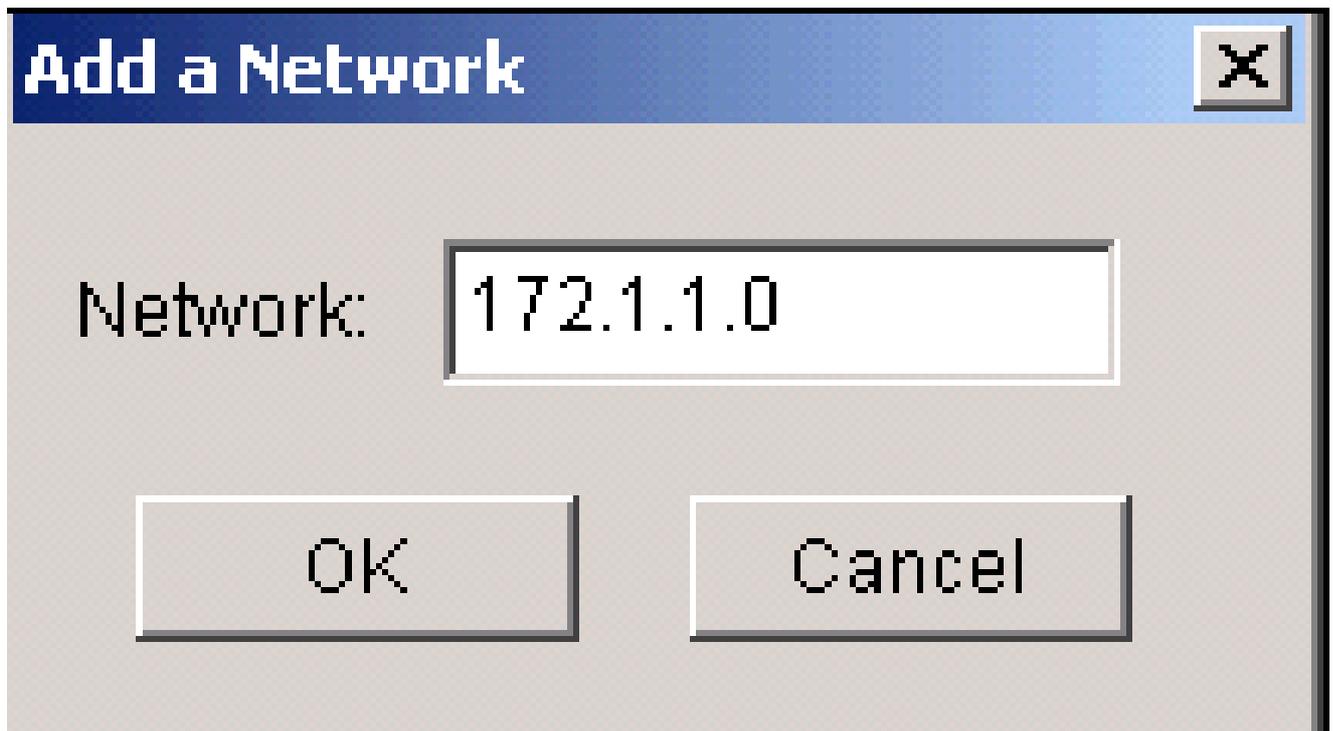
1. Choisissez Configure > Routing > Dynamic Routing.
2. Sélectionnez RIP et cliquez sur Edit.



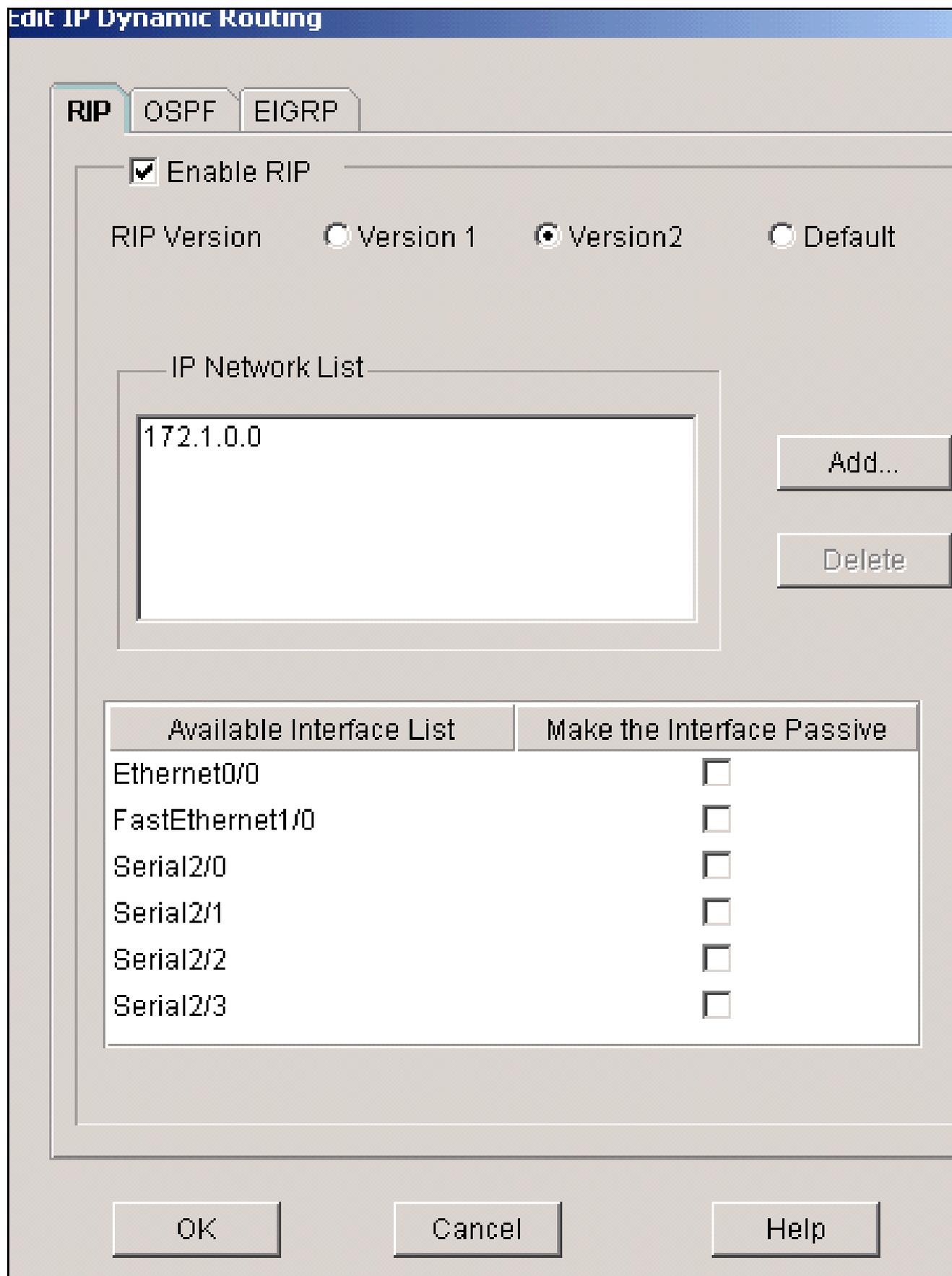
3. Activez la case à cocher Enable RIP, sélectionnez la version RIP, et cliquez sur Add.



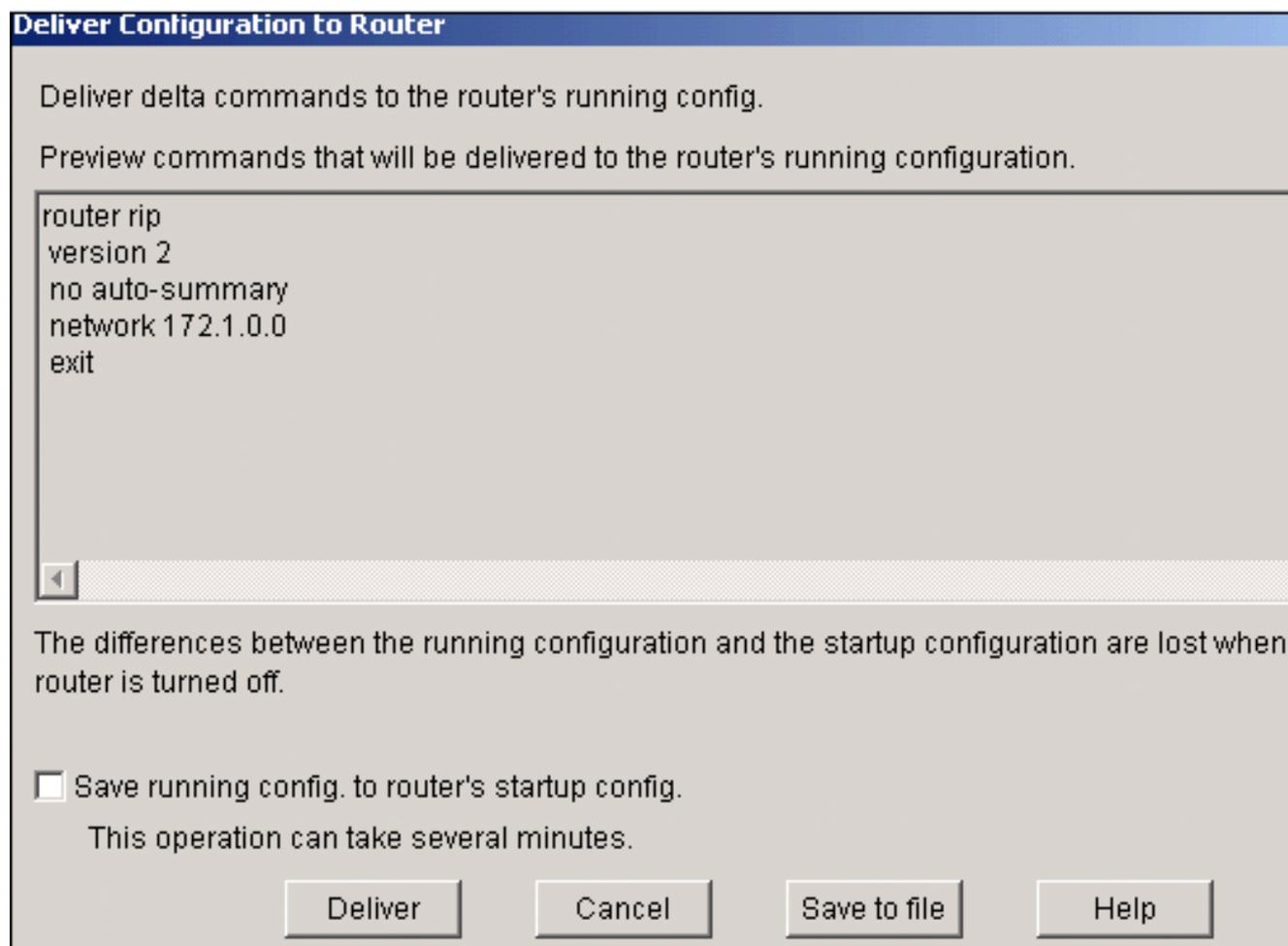
4. Spécifiez l'adresse réseau à annoncer.



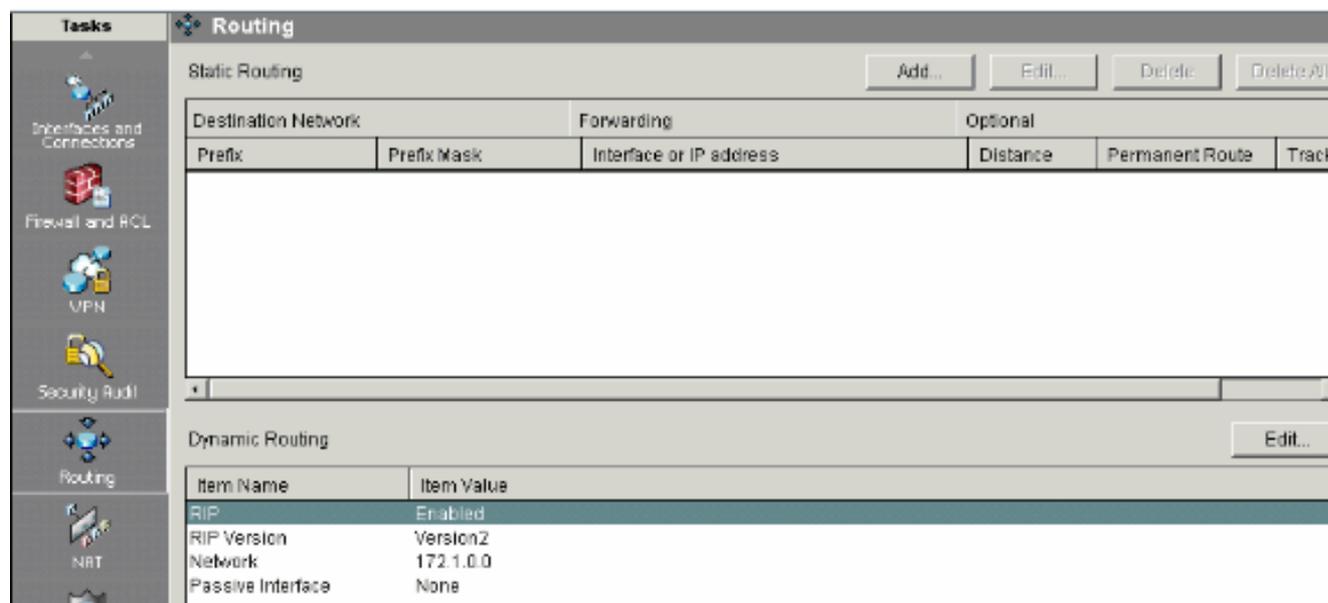
5. Click OK.



6. Cliquez sur Deliver pour transférer les commandes au routeur.



Cette fenêtre montre la configuration du routage RIP dynamique.

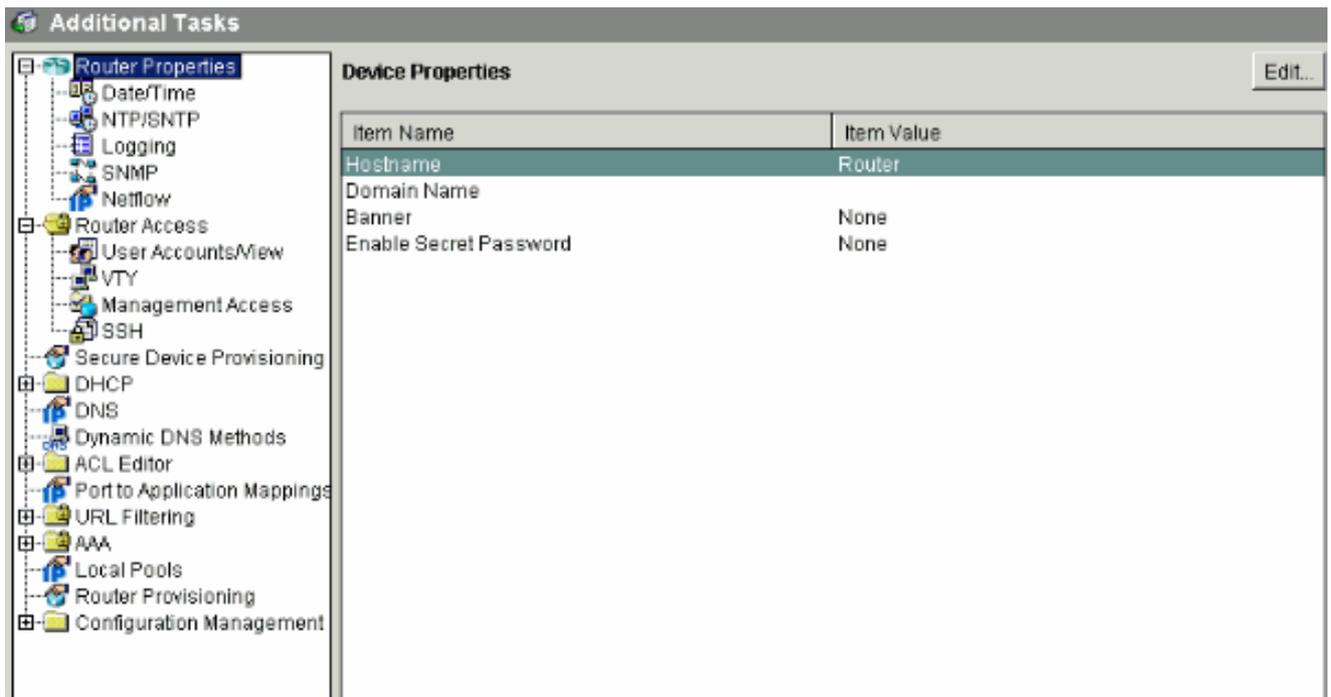


Configuration - Divers

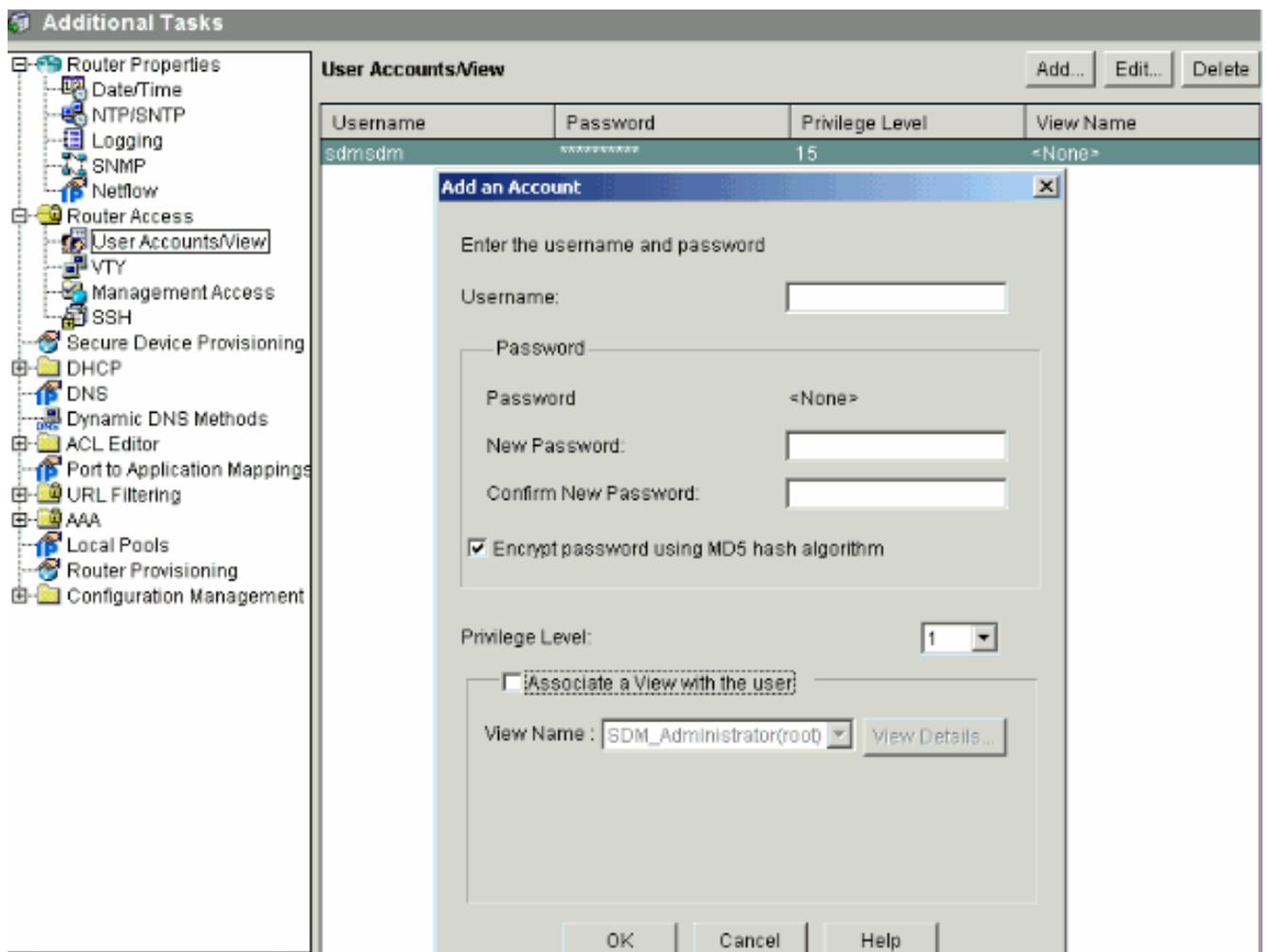
Complétez ces étapes afin de configurer les autres paramètres de base dans un routeur Cisco.

1. Choisissez Configure > Additional Tasks > Router Properties et cliquez sur Edit si vous

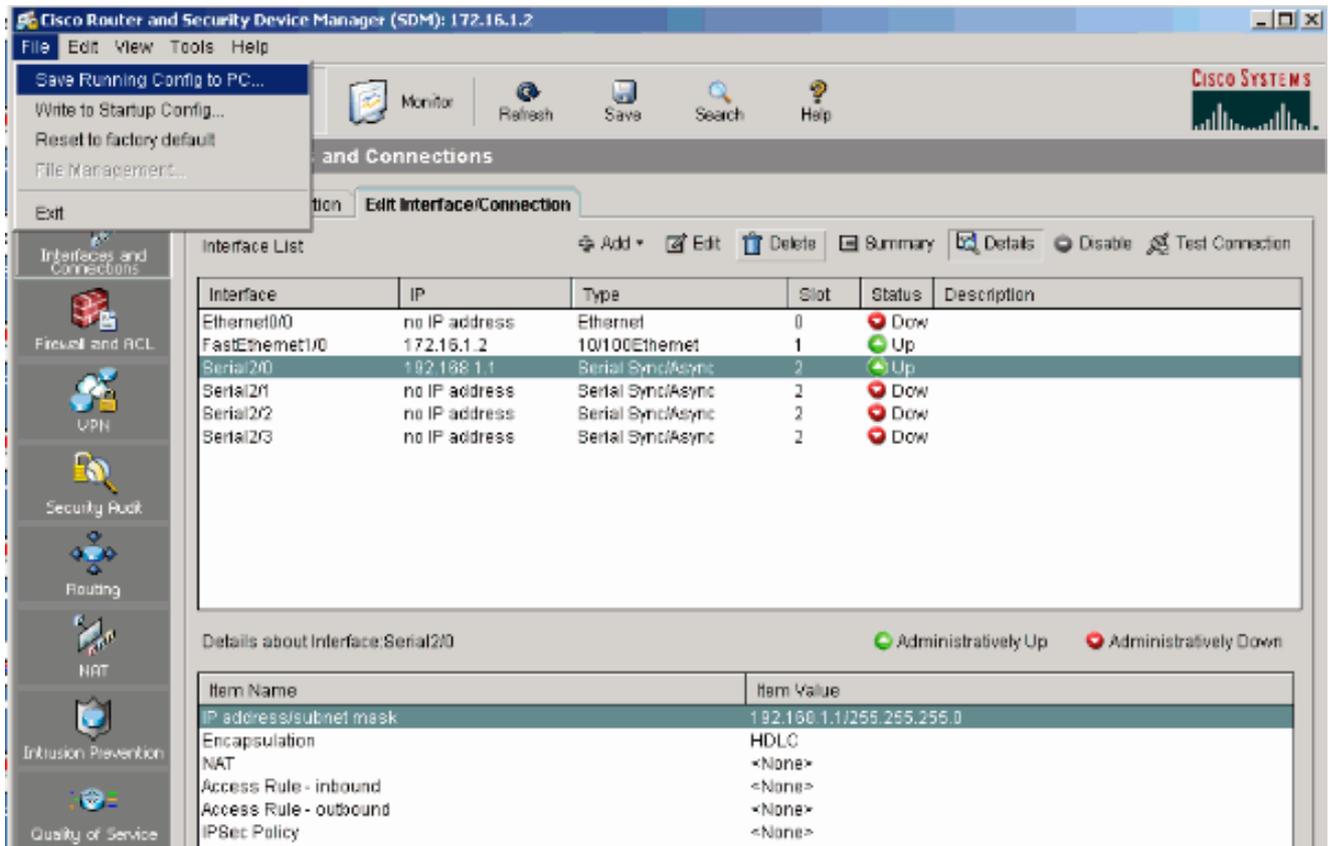
voulez changer les propriétés Hostname, Domain Name, Banner et Enable Secret Password pour un routeur.



2. Choisissez Configure > Additional Tasks > Router Access > User Accounts/View afin d'ajouter/modifier/supprimer les comptes utilisateur pour le routeur.

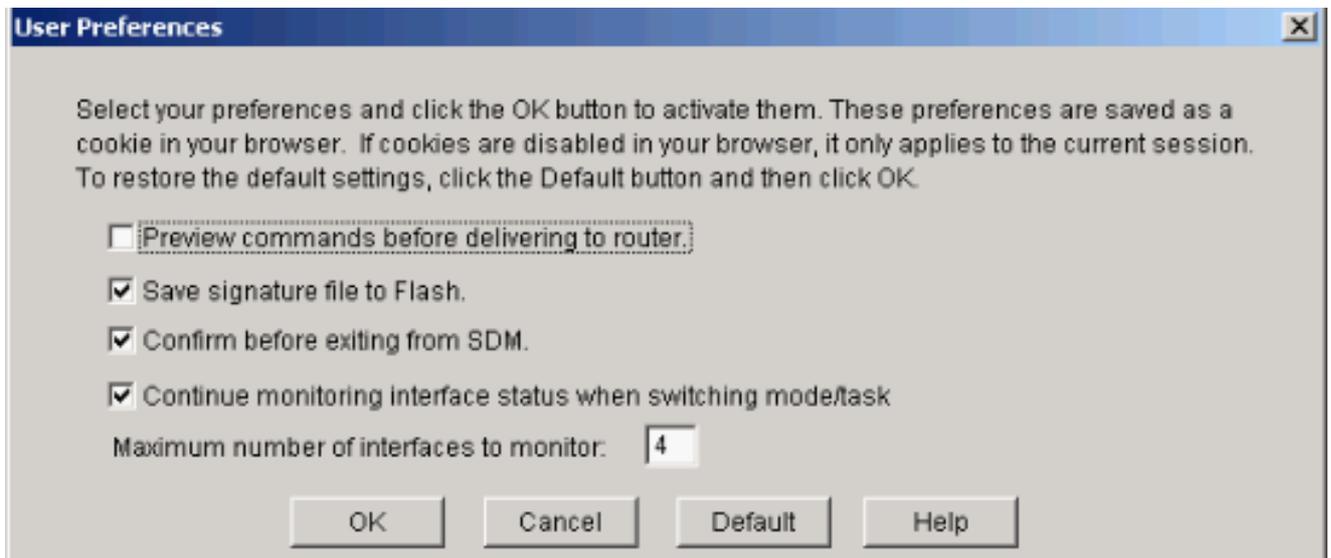


3. Choisissez File > Save Running Config to PC... afin d'enregistrer la configuration dans la mémoire vive non volatile du routeur ainsi que sur le PC et de réinitialiser la configuration actuelle aux paramètres par défaut (usine).



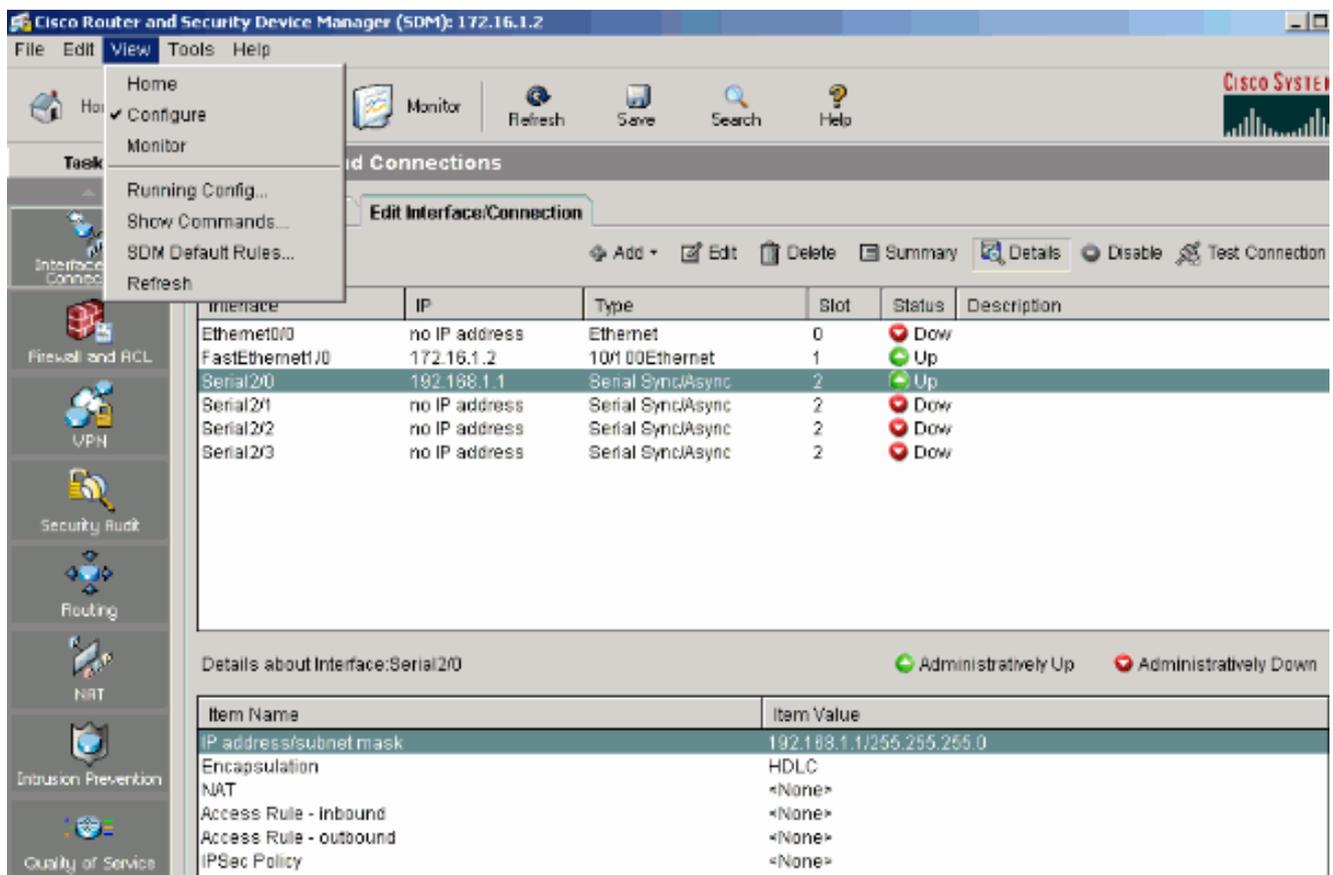
4. Accédez à la barre des tâches et choisissez Edit > Preferences afin d'activer ces options de préférences de l'utilisateur :

- Prévisualisez les commandes avant de les transmettre au routeur.
- Sauvegardez le fichier de signature dans Flash.
- Confirmez avant de quitter le SDM.
- Continuez la surveillance de l'état de l'interface lors du changement de mode/tâche.



5. Choisissez View dans la barre des tâches si vous voulez :

- visualiser les pages Home, Configure ou Monitor ;
- afficher la configuration en cours du routeur ;
- afficher les différentes commandes show ;
- afficher les règles par défaut du SDM.
- Choisissez Refresh pour synchroniser la configuration des routeurs si certains sont configurés par CLI avec le SDM.



Configuration CLI

Configuration du routeur

```
<#root>
Router#
show run
Building configuration...

Current configuration : 2525 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
no logging buffered
enable password cisco
!
no aaa new-model
!
resource policy
!
!
!
ip cef
!
!
!
!--- RSA certificate generated after you enable the !---

ip http secure-server

  command.

crypto pki trustpoint TP-self-signed-392370502
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-392370502
  revocation-check none
  rsakeypair TP-self-signed-392370502
!
!
crypto pki certificate chain TP-self-signed-392370502
  certificate self-signed 01
    3082023C 308201A5 A0030201 02020101 300D0609 2A864886 F70D0101 04050
    30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657
    69666963 6174652D 33393233 37303530 32301E17 0D303530 39323330 34333
    375A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403 13254
    532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3339 32333
    35303230 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818
    C86C0F42 84656325 70922027 EF314C2F 17C8BBE1 B478AFA3 FE2BC2F2 3C272
```

```
A3B5E13A 1392A158 73D8FE0D 20BFD952 6B22890C 38776830 241BE259 EE2AA
CF4124EA 37E41B46 A2076586 2F0F9A74 FDB72B3B 6159EEF7 0DEC7D44 BE489
9E351BF7 F5C808D9 2706C8B7 F5CE4B73 39ED8A61 508F455A 68245A6B D072F
02030100 01A36630 64300F06 03551D13 0101FF04 05300301 01FF3011 06035
11040A30 08820652 6F757465 72301F06 03551D23 04183016 80148943 F2369
ACD8CCA6 CA04EC47 C68B8179 E205301D 0603551D 0E041604 148943F2 36910
D8CCA6CA 04EC47C6 8B8179E2 05300D06 092A8648 86F70D01 01040500 03818
3B93B9DC 7DA78DF5 6D1D0D68 6CE075F3 FFDAD0FB 9C58E269 FE360329 2CEE3
D8661EB4 041DEFEF E14AA79D F33661FC 2E667519 E185D586 13FBD678 F52E1
E3C92ACD 52741FA4 4429D0B7 EB3DF979 0EB9D563 51C950E0 11504B41 4AE79
ODD0BE16 856B688C B727B3DB 30A9A91E 10236FA7 63BAEACB 5F7E8602 0C33D
quit
```

```
!
!
!
!
!
!
!
!
!
!
```

!--- Create a user account named

```
sdmsdm
```

```
with all privileges.
```

```
username sdmsdm privilege 15 password 0 sdmsdm
```

```
!
!
!
!
!
!
```

```
interface Ethernet0/0
```

```
no ip address
```

```
shutdown
```

```
half-duplex
```

```
!
```

!--- The LAN interface configured with a private IP address.

```
interface FastEthernet1/0
```

```
ip address 172.16.1.2 255.255.255.0
```

!--- Designate that traffic that originates from behind !--- the interface is subject to Network Address

```
ip nat inside
```

```
ip virtual-reassembly
```

```
duplex auto
```

```
speed auto
```

```
!
```

!--- This is the WAN interface configured with a routable (public) IP address.

```
interface Serial2/0
```

```
ip address 192.168.1.1 255.255.255.0
```

!--- Designate that this interface is the !--- destination for traffic that has undergone NAT.

```
ip nat outside
  ip virtual-reassembly
  !
interface Serial2/1
  no ip address
  shutdown
  !
interface Serial2/2
  no ip address
  shutdown
  !
interface Serial2/3
  no ip address
  shutdown
  !

!--- RIP version 2 routing is enabled.

router rip
  version 2
  network 172.1.0.0
  no auto-summary

!--- This is where the commands to enable HTTP and HTTPS are configured.

ip http server
ip http secure-server
!

!--- This configuration is for dynamic NAT.

!

!--- Define a pool of outside IP addresses for NAT.

ip nat pool pool1 192.168.1.3 192.168.1.10 netmask 255.255.255.0

!--- In order to enable NAT of the inside source address, !--- specify that traffic from hosts that ma

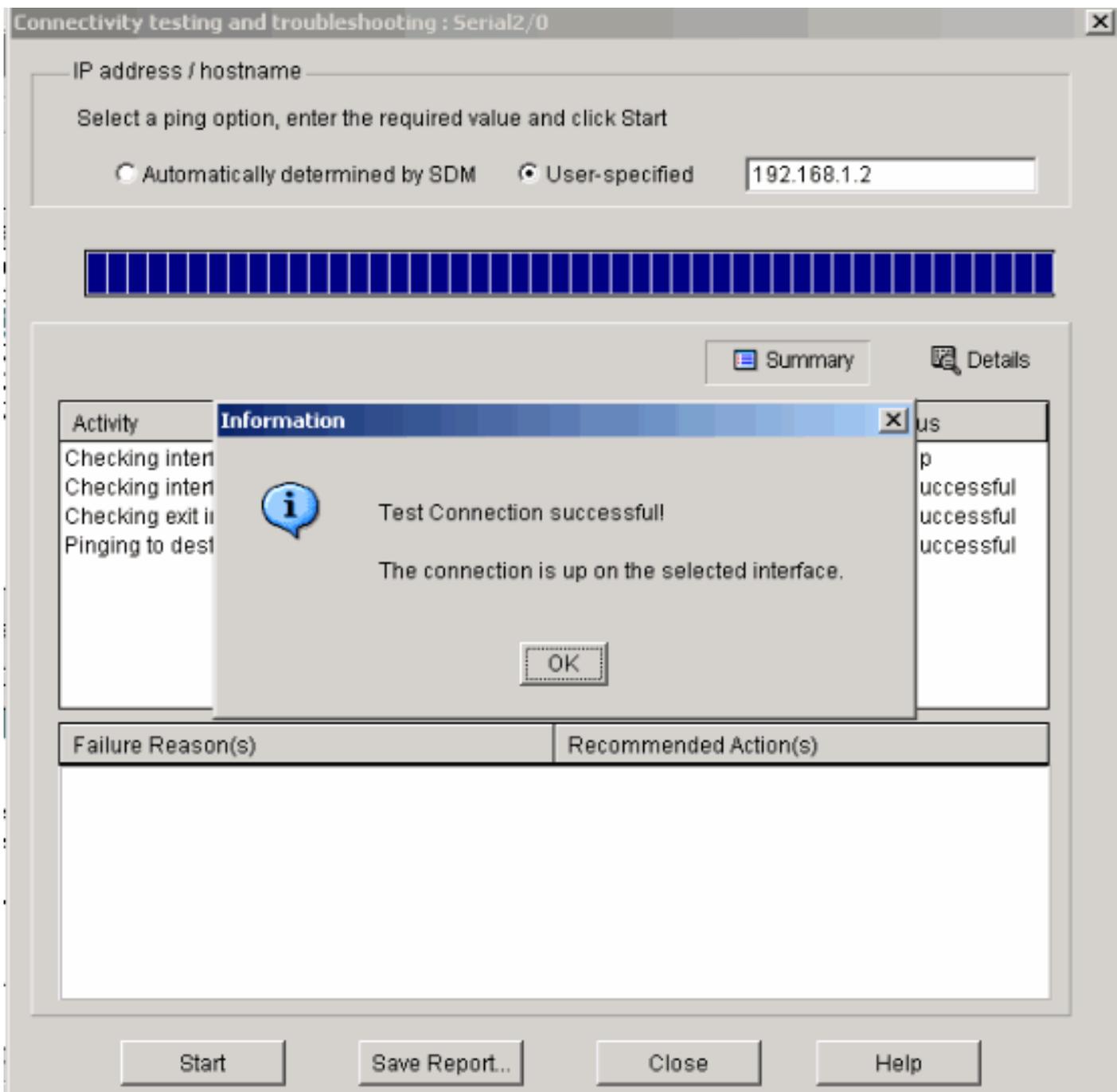
ip nat inside source list 1 pool pool1
!

!--- Access list 1 permits only 172.16.1.0 network to be NATed.

access-list 1 remark SDM_ACL Category=2
access-list 1 permit 172.16.1.0 0.0.0.255
!

!--- This configuration is for static NAT

!--- In order to translate the packets between the real IP address 172.16.1.1 with TCP !--- port 80 and
```

Dépannage

L'[Outil Interpréteur de sortie \(clients enregistrés uniquement\) \(OIT\)](#) prend en charge certaines [commandes show](#). Utilisez l'OIT pour afficher une analyse de la sortie de la commande show .

Remarque : Consultez les renseignements importants sur les commandes de débogage avant d'entrer des commandes de débogage.

Vous pouvez utiliser ces options afin de dépanner :

- Choisissez Tools > Update SDM dans la barre des tâches afin d'envoyer une commande ping, Telnet, et de mettre à niveau le SDM vers la version la plus récente. Vous pouvez faire cela à partir de Cisco.com, du PC local, ou du CD.

The screenshot shows the Cisco Router and Security Device Manager (SDM) interface. The main window displays a table of interfaces with the following data:

Interface	IP address	Type	Slot	Status	Description
Ethernet0/0	no IP address	Ethernet	0	Dow	
FastEthernet1/0	172.16.1.2	10/100Ethernet	1	Up	
Serial2/0	192.168.1.1	Serial Sync/Async	2	Up	
Serial2/1	no IP address	Serial Sync/Async	2	Dow	
Serial2/2	no IP address	Serial Sync/Async	2	Dow	
Serial2/3	no IP address	Serial Sync/Async	2	Dow	

Below the table, the details for the selected interface (Serial2/0) are shown:

Item Name	Item Value
IP address/subnet mask	192.168.1.1/255.255.255.0
Encapsulation	HDLC
NAT	<None>
Access Rule - Inbound	<None>
Access Rule - outbound	<None>
IPSec Policy	<None>
Face/VPN Remote	<None>

- Choisissez Help > About this Router afin d'afficher les informations sur la configuration matérielle du router.

Hardware Details

Software Details



Hardware Configuration

- [-] Cisco 3640 (R4700) - <Router>
 - Slot 0: 1 Ethernet and 2 WIC slots Network Module
 - Slot 1: 1 Fast Ethernet and 2 WIC slots Network Modu
 - Slot 2: 4 Port Async/Sync Network Module
 - slot0:15MB(Free space3MB)
 - flash:31MB(Free space0MB)

Close

Cette fenêtre montre des informations sur l'image de l'IOS enregistrée dans le routeur.

Hardware/Software Details



Hardware Details

Software Details



IOS Image Name: c3640-ik9s-mz.124-8.bin

IOS Version: 12.4(8)

Boot From: flash

Feature Sets:

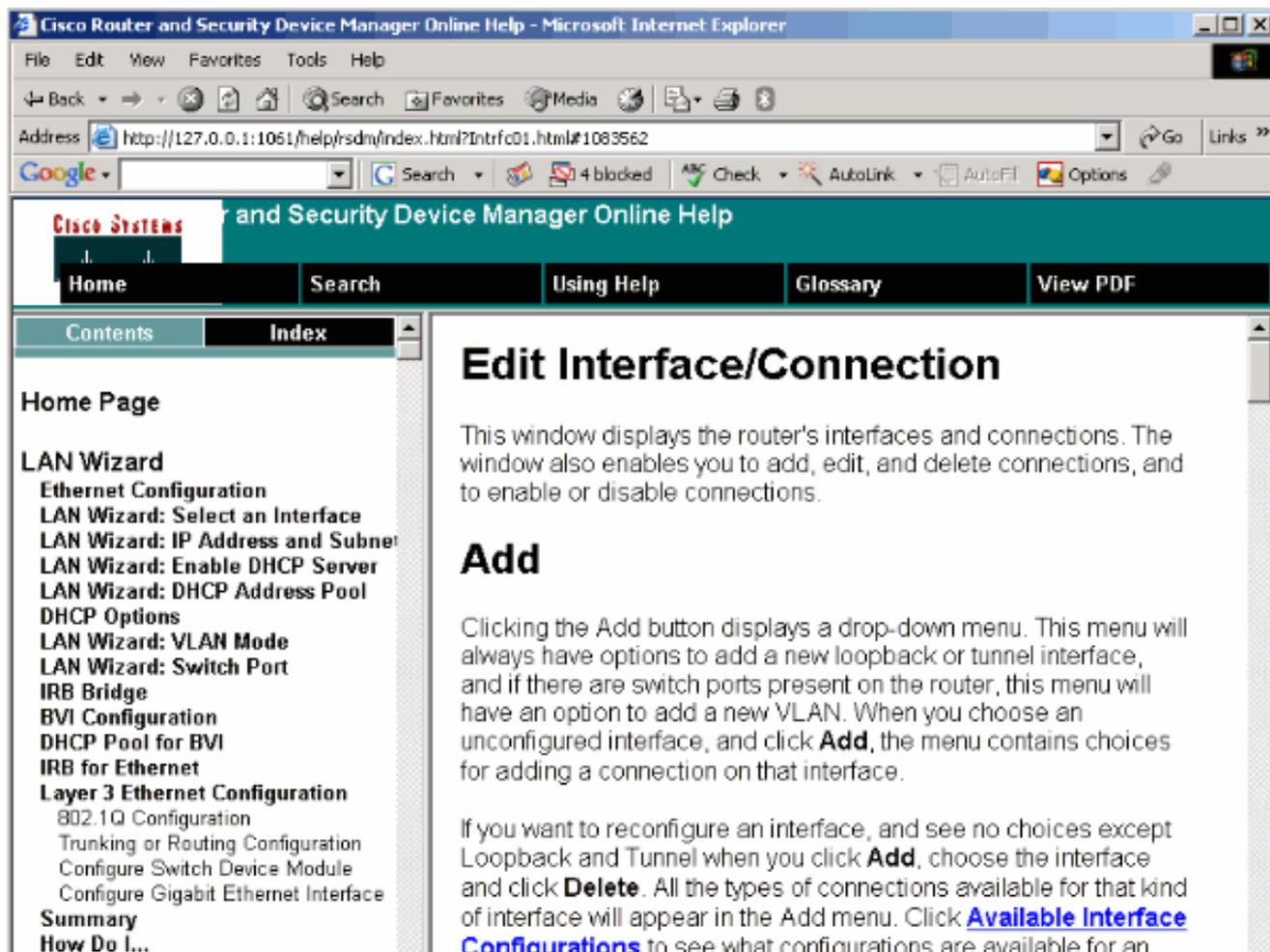
✓ IP (Internet Protocol)

✓ VPN (DES, AES, 3DES, SEAL)

SDM Version: 2.1

Close

- L'option Help fournit des informations au sujet des diverses options disponibles dans le SDM pour la configuration des routeurs.



Compatibilité de SDM avec un système d'exploitation 64 bits

SDM n'est pas pris en charge sur les ordinateurs avec système d'exploitation 64 bits. Vous devez installer le SDM sur le routeur et y accéder via le navigateur Web.

Référez-vous à [Tâche 4 : Installer les fichiers SDM](#) pour plus d'informations sur l'installation des fichiers SDM sur le routeur.

Impossible de lancer le SDM à travers le navigateur Web

Problème

Quand vous utilisez le SDM via le navigateur Web, un message d'erreur du démarrage du SDM apparaît.

Solution 1

Le problème peut être lié à la version de Java. La mise à jour de Java peut ne pas être compatible avec la version du SDM. Si la version de Java est Java 6 Update 12, alors désinstallez cette version et installez Java 6 Update 3. Cela résout le problème. Référez-vous à la section [Versions du navigateur Web et versions de Java Runtime Environment de la note d'édition SDM 2.5 pour plus d'informations sur la compatibilité](#). SDM version 2.5 fonctionne sous les mises à jour 2 et 3 de Java version 6.

Solution 2

Activez Autoriser l'exécution du contenu actif dans les fichiers du Poste de travail dans les options d'Internet Explorer afin de résoudre le problème.

1. Ouvrez Internet Explorer et choisissez Outils > Options Internet > Avancé.
2. Sous la section Sécurité, assurez-vous que les cases à cocher en regard des options Autoriser l'exécution du contenu actif dans les fichiers de mon ordinateur et Autoriser l'installation du logiciel par le contenu actif même si la signature n'est pas valide sont cochées.
3. Cliquez maintenant sur OK et redémarrez le navigateur afin que les modifications prennent effet.

Erreur : dépassement de pile java.bling

Problème

Je ne parviens pas à me connecter au SDM et je reçois le message d'erreur suivant :

```
java.bling stack over flow
```

Solution

Ce problème se produit généralement lorsque le code Java version 1.5.0_06 est utilisé. Pour plus d'informations sur la façon de résoudre ce problème, référez-vous à [L'utilisateur ne peut pas se connecter à Security Device Manager \(SDM\) et reçoit le message d'erreur java.bling stack over flow](#).

Informations connexes

- [Guide d'installation de Cisco Security Device Manager](#)
- [Page d'assistance de produit Cisco - Routeurs](#)
- [Page d'assistance Cisco Configuration Professional](#)
- [Page de support NAT](#)
- [Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.