使用SDM的基本路由器配置

目錄

簡介

本文說明如何使用思科安全裝置管理員(SDM)設定路由器的基本組態。這包括 IP 位址、預設路由、靜態和動態路由、靜態和動態 NAT、主機名稱、橫幅標語、secret 密碼、使用者帳戶等的組態。Cisco SDM允許您使用易於使用的基於Web的管理介面，在包括小型辦公室(Small Office Home Office，SOHO)、分支機構(Branch Office，BO)、區域辦公室、中心站點或企業總部在內的各種網路環境中配置路由器。

必要條件

需求

本檔案假設Cisco路由器已完全運行並配置為允許Cisco SDM進行配置更改。

注意： 請參閱允許SDM進行HTTPS訪問，以便允許SDM配置路由器。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 採用Cisco IOS的Cisco 3640路由器[?]軟體版本12.4(8)
- 思科安全裝置管理員(SDM)版本2.3.1

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

注意：如果您使用思科整合服務路由器(ISR)，請參閱使用思科配置專業版的基本路由器配置，瞭解具有更強大功能的類似配置詳細資訊。有關Cisco CP支援哪些路由器的資訊，請參閱*Cisco Configuration Professional 2.5*發行說明的支援的路由器部分。

慣例
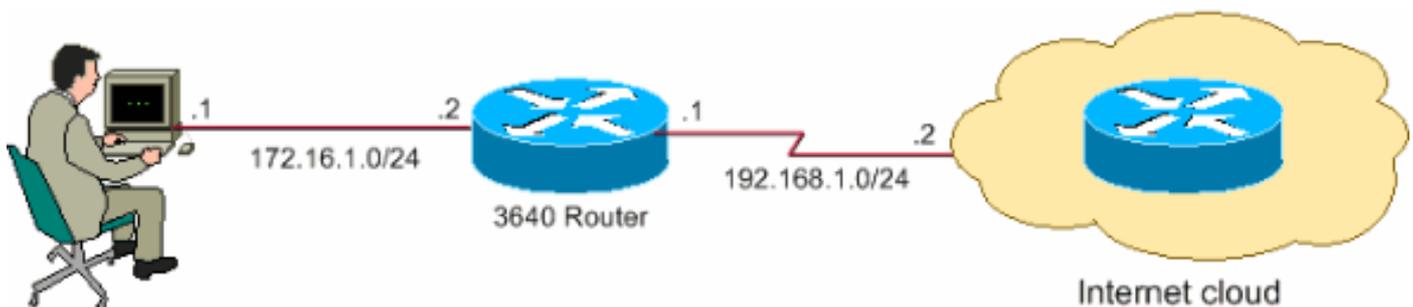
請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

設定

本節提供為網路中的路由器配置基本設定的相關資訊。

網路圖表

本檔案會使用以下網路設定：

3640 Router

172.16.1.0/24

192.168.1.0/24

Internet cloud

注意：此配置中使用的IP編址方案在Internet上不能合法路由。它們是RFC 1918，已在實驗室環境中使用。

介面組態

完成這些步驟，設定思科路由器的介面。

1. 按一下「**Home**」以轉到SDM首頁。SDM首頁提供路由器硬體和軟體、功能可用性和配置摘要等資訊。綠色圓圈顯示此路由器支援的功能，紅色圓圈顯示不支援的功能。

2. 選擇Configure > Interfaces and Connections > Create Connection以配置介面的WAN連線。例如，對於串列介面2/0，選擇Serial選項，然後按一下Create New Connection。**註：對於**其他型別的介面(如**乙太網**)，請選擇相應的介面型別，然後按一下Create New Connection**按鈕繼續**操作。
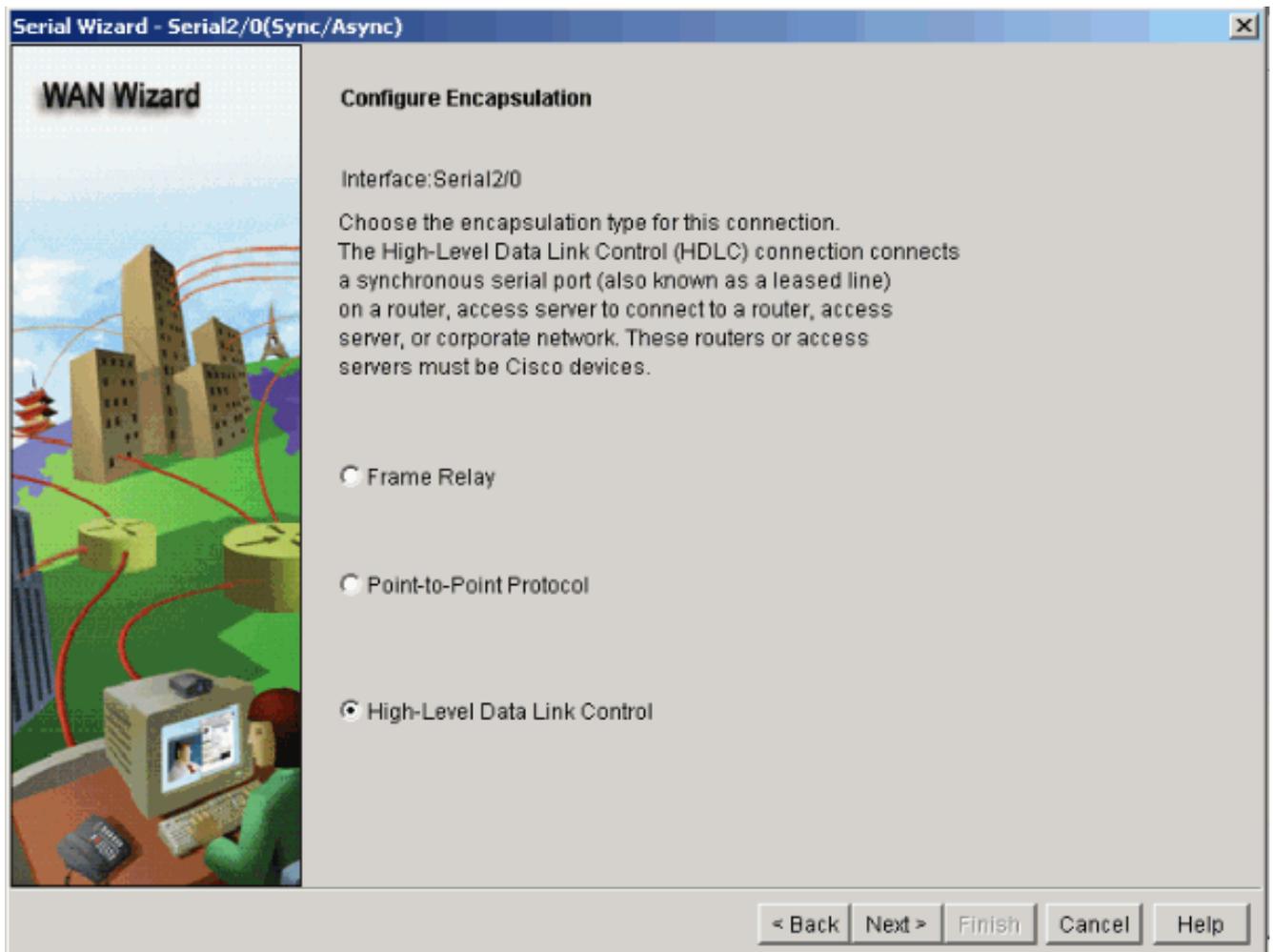
3. 按一下Next以在出現此介面後繼續。
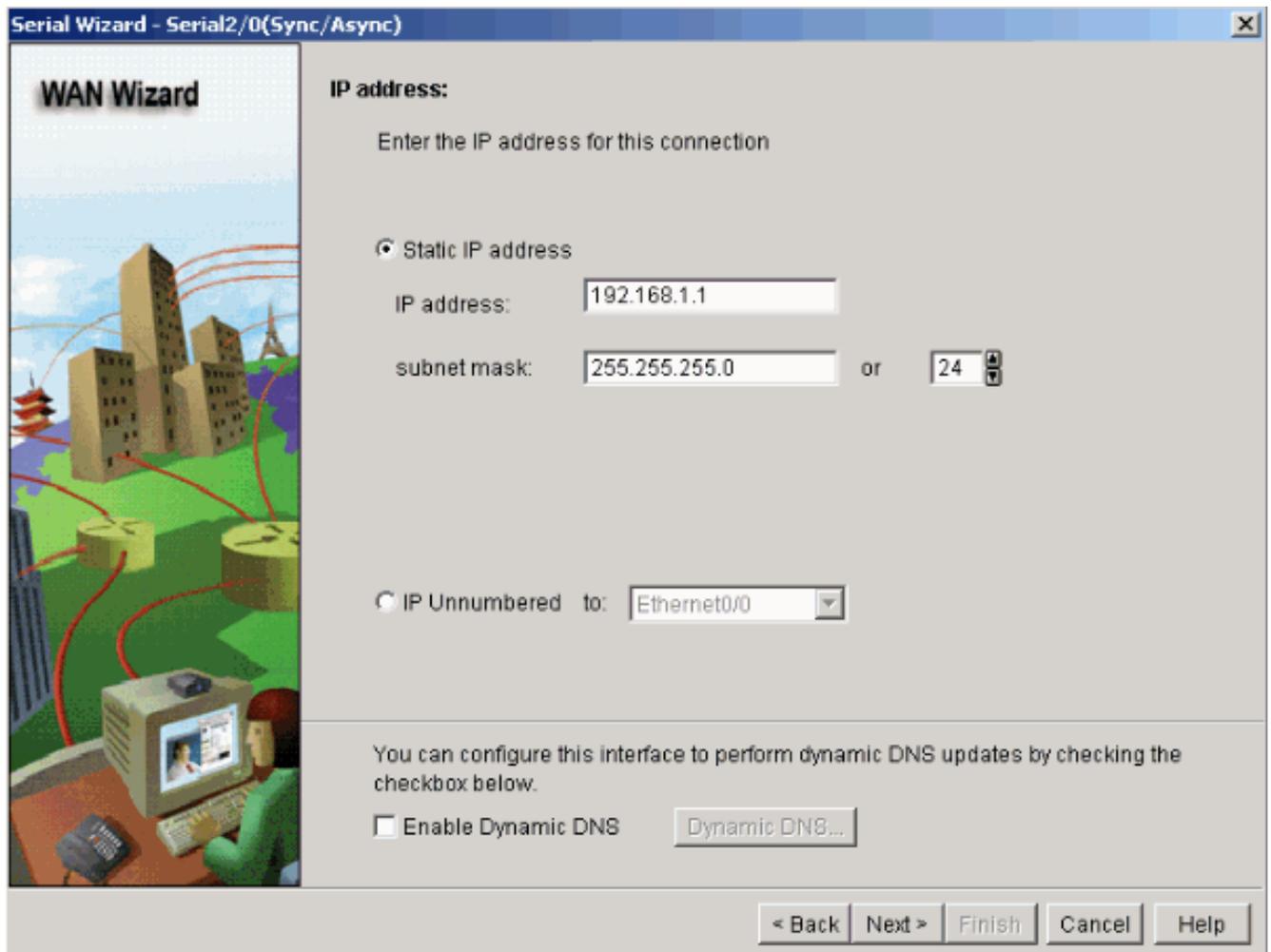
4. 從Available Interfaces選項中選擇**Serial interface 2/0（需要）**，然後按一下**Next。**
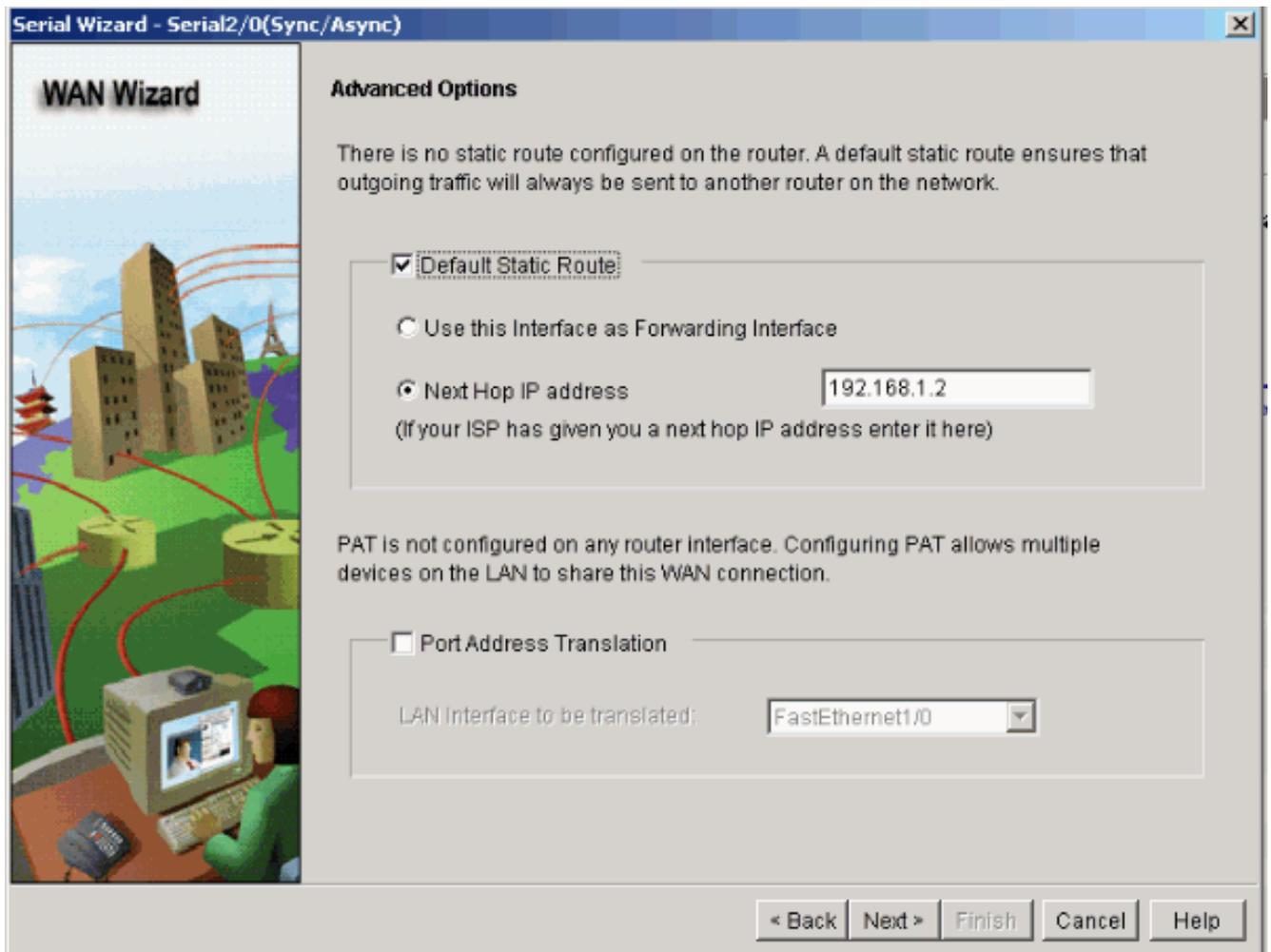
5. 選擇串列介面的封裝型別，然後按一下**Next。**
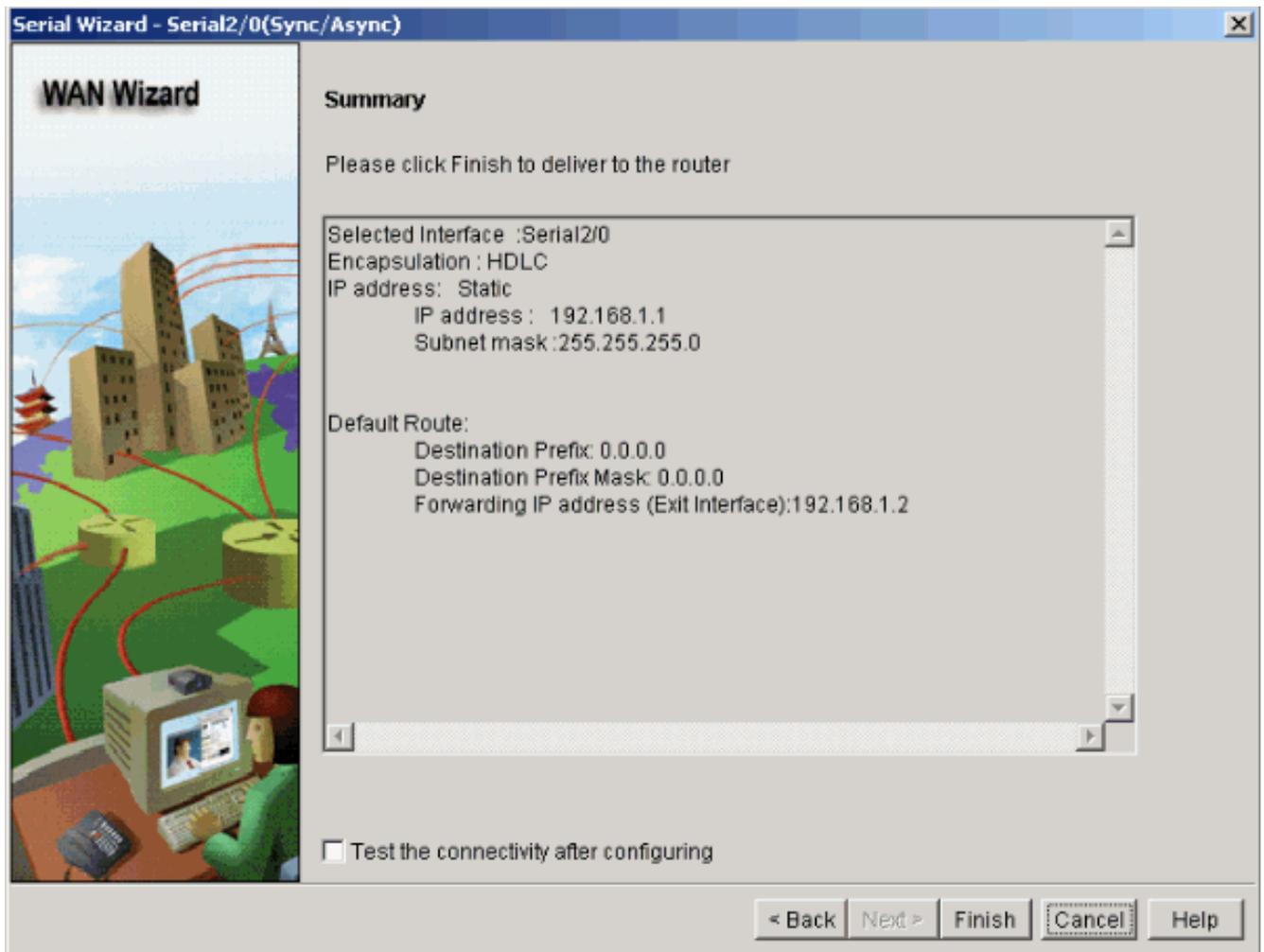
6. 使用介面的相應子網掩碼指定靜態IP地址，然後按一下下一步。
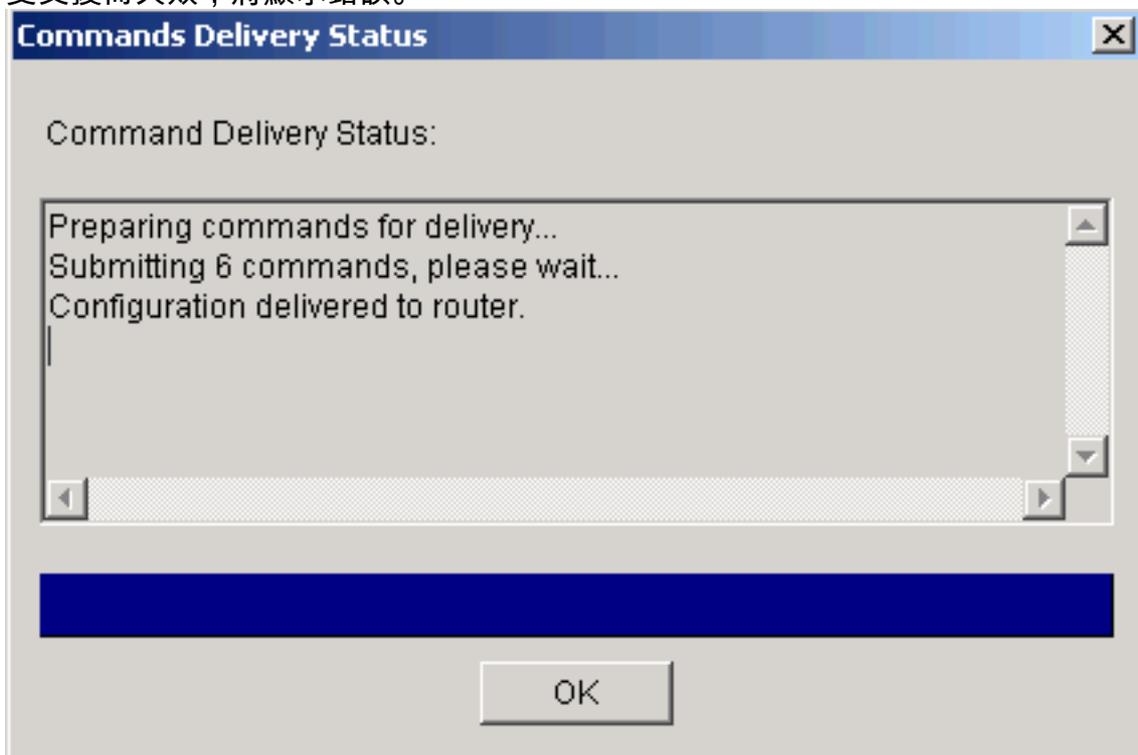
7. 使用ISP提供的可選引數(如下一跳IP地址（根據網路圖192.168.1.2）)配置預設路由，然後按一下Next。

出現此視窗並顯示使用者配置的配置摘要。按一下「Finish」（結束）。

Serial Wizard - Serial2/0(Sync/Async)

WAN Wizard

Summary

Please click Finish to deliver to the router

```
Selected Interface :Serial2/0
Encapsulation : HDLC
IP address:  Static
        IP address :  192.168.1.1
        Subnet mask :255.255.255.0


Default Route:
        Destination Prefix: 0.0.0.0
        Destination Prefix Mask: 0.0.0.0
        Forwarding IP address (Exit Interface):192.168.1.2
```

☐ Test the connectivity after configuring

< Back   Next >   Finish   Cancel   Help

出現此視窗，並顯示命令到路由器的傳送狀態。否則，如果命令交付由於不相容命令或功能不受支援而失敗，將顯示錯誤。

Commands Delivery Status

Command Delivery Status:

```
Preparing commands for delivery...
Submitting 6 commands, please wait...
Configuration delivered to router.
```

OK

8. 選擇Configure > Interfaces and Connections > Edit Interfaces/Connections以新增/編輯/刪除各種介面。

Cisco Router and Security Device Manager (SDM): 172.16.1.2

File Edit View Tools Help

| Home | Configure | Monitor | Refresh | Save | Search | Help | Cisco Sy |

Tasks

Interfaces and Connections

Create Connection | **Edit Interface/Connection**
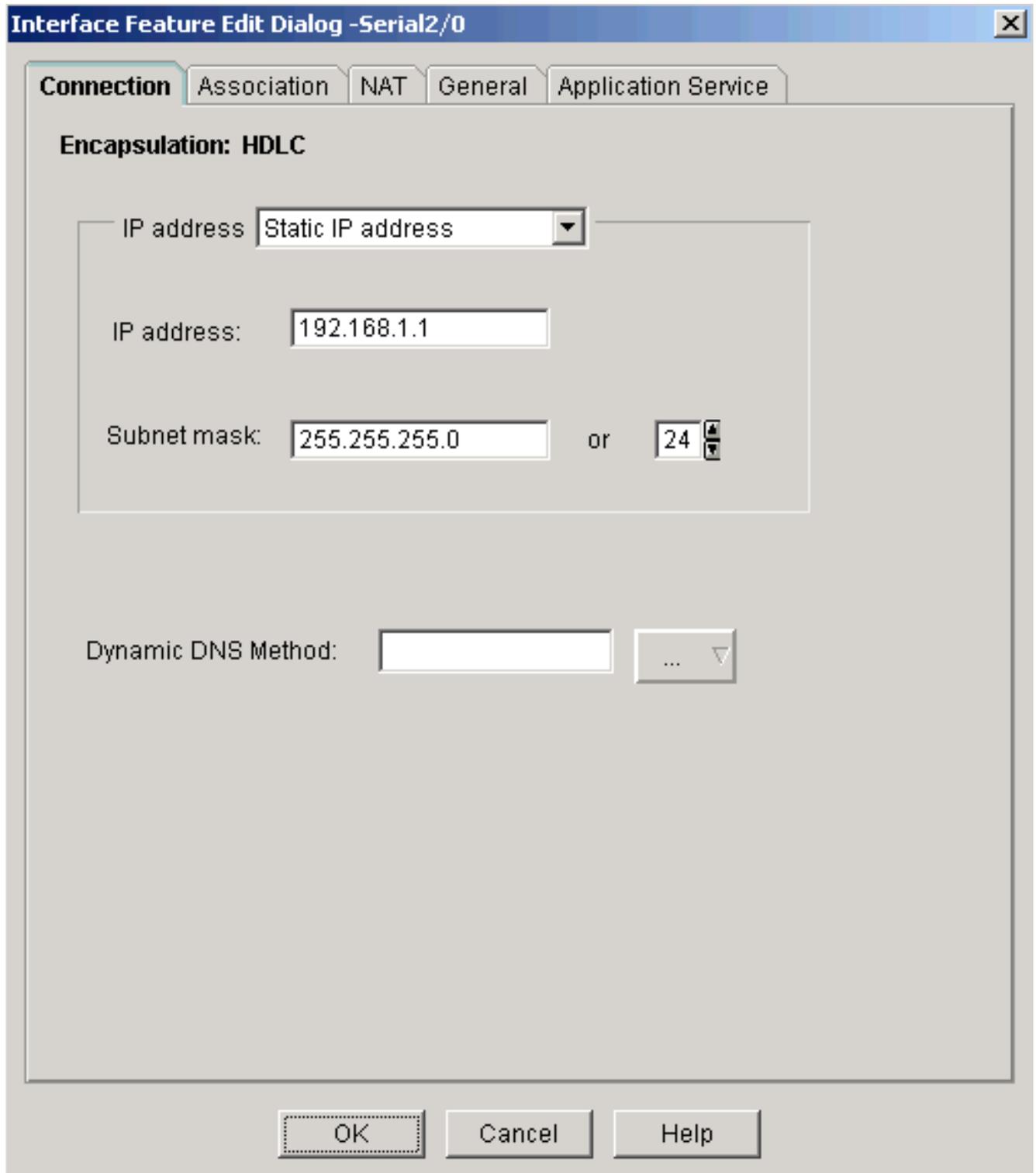
Interface List

Add ▾ | Edit | Delete | Summary | Details | Disable | Test Conne

Interface	IP	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	

Details about Interface Serial2/0   ● Administratively Up   ● Administratively Do

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>

突出顯示要更改的介面，如果要編輯或更改介面配置，請按一下**Edit**。您可以在此處更改現有的靜態IP地址。
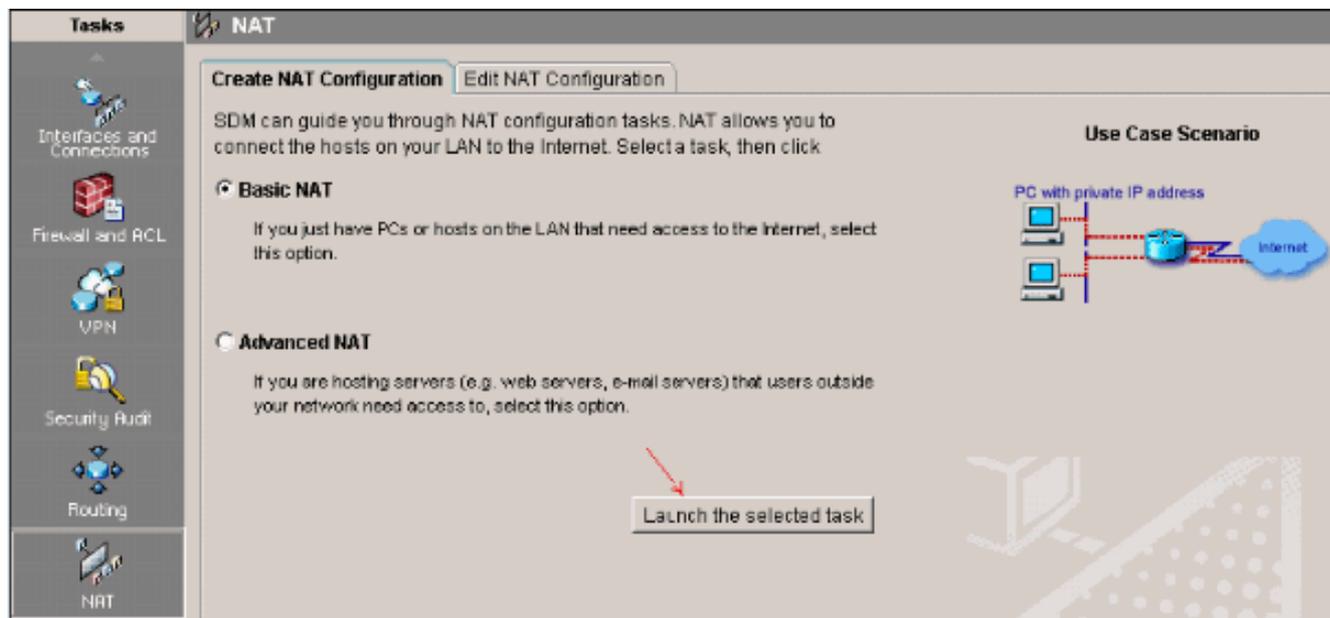
NAT配置
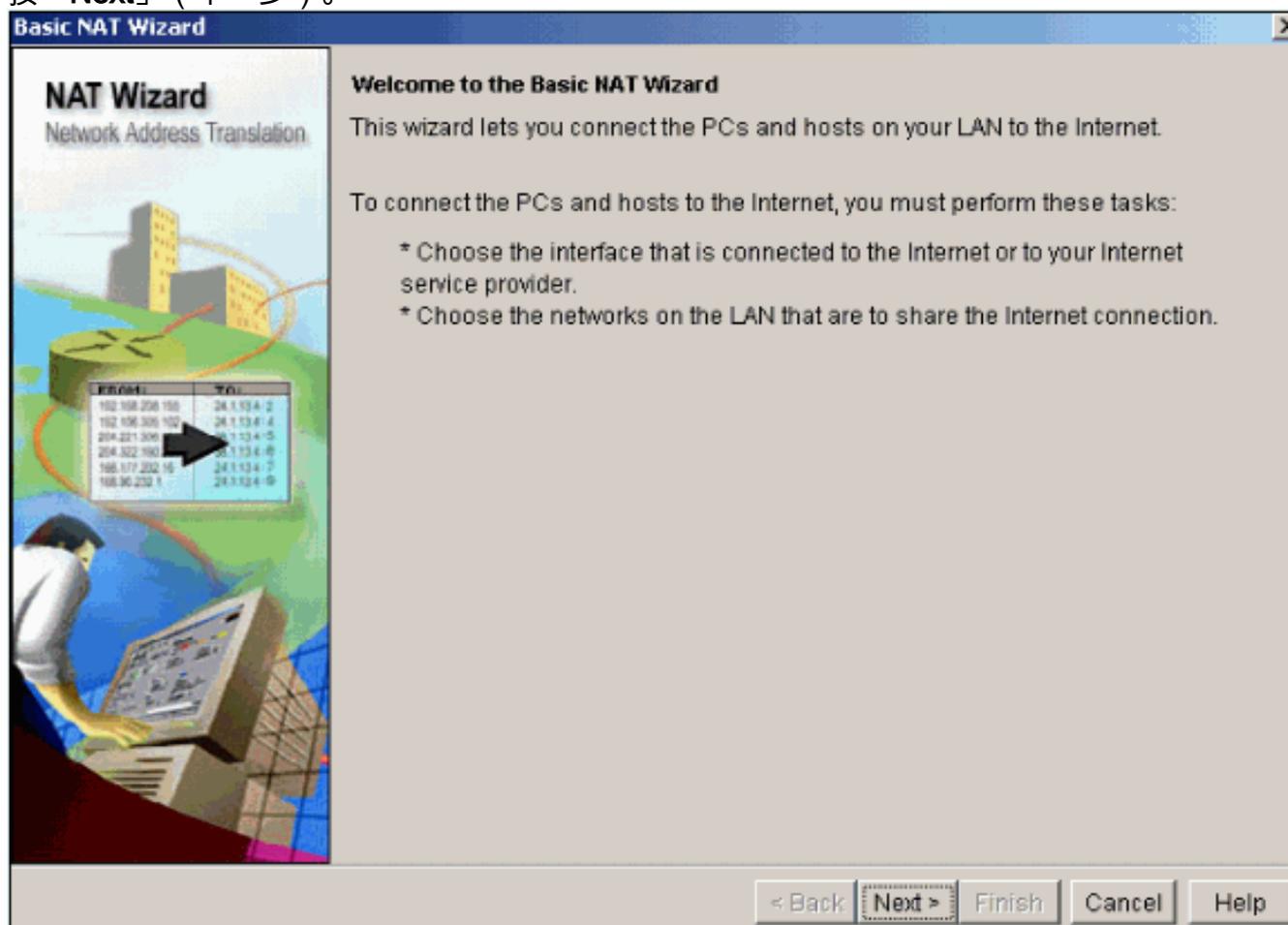
動態NAT配置

完成這些步驟，在Cisco路由器中配置動態NAT。
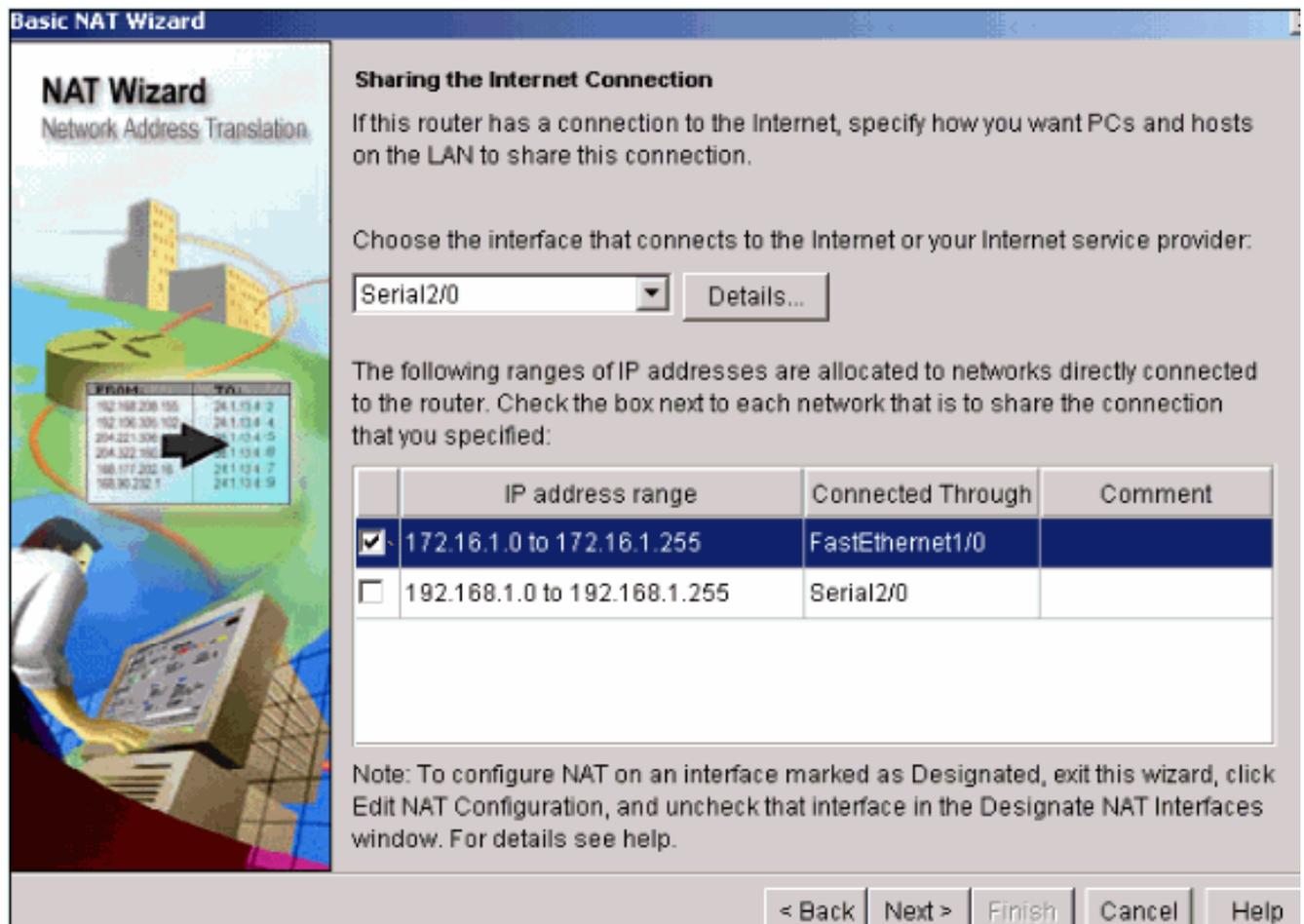
1. 選擇**Configure > NAT > Basic NAT**，然後按一下**Launch the selected task**以配置基本 NATing。
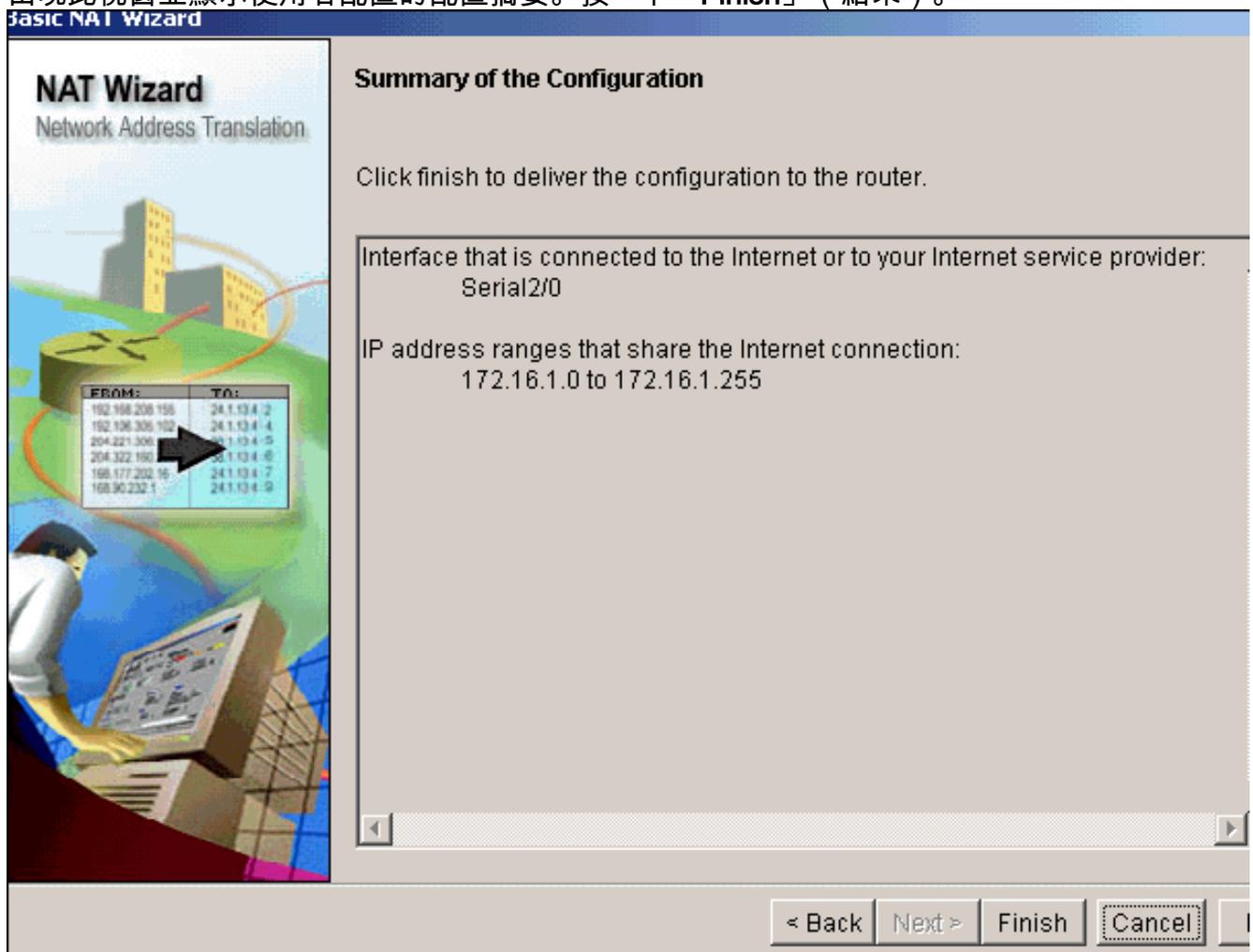
2. 按「**Next**」（下一步）。
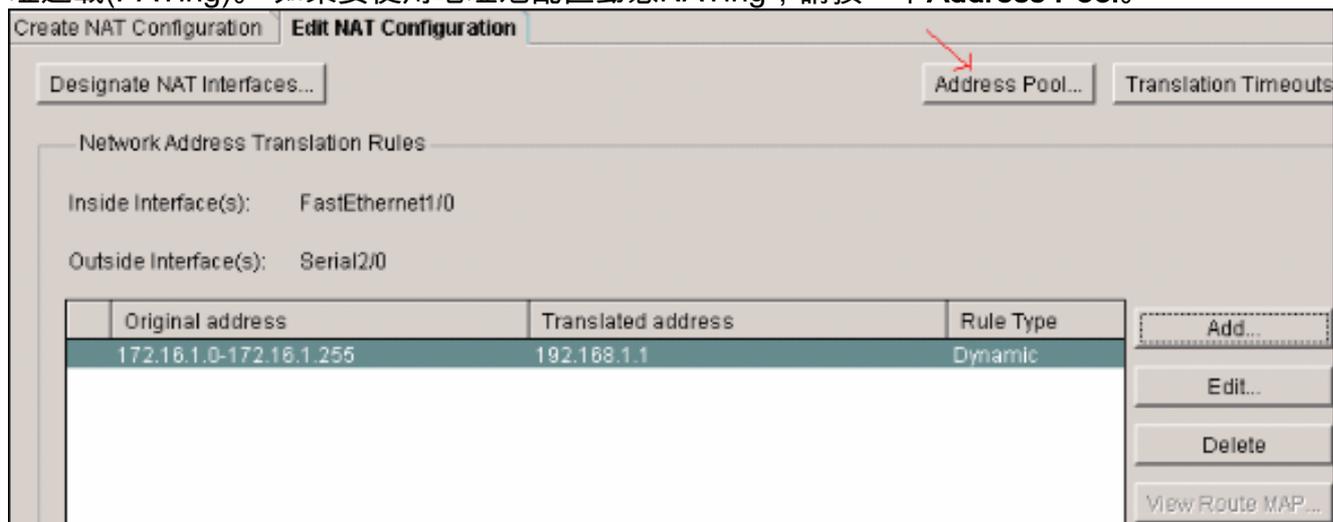
3. 選擇連線到Internet或ISP的介面，並選擇共用Internet訪問的IP地址範圍。

Basic NAT Wizard

NAT Wizard
Network Address Translation

Sharing the Internet Connection

If this router has a connection to the Internet, specify how you want PCs and hosts on the LAN to share this connection.

Choose the interface that connects to the Internet or your Internet service provider:

Serial2/0 ▼   Details...

The following ranges of IP addresses are allocated to networks directly connected to the router. Check the box next to each network that is to share the connection that you specified:

	IP address range	Connected Through	Comment
☑	172.16.1.0 to 172.16.1.255	FastEthernet1/0	
☐	192.168.1.0 to 192.168.1.255	Serial2/0	

Note: To configure NAT on an interface marked as Designated, exit this wizard, click Edit NAT Configuration, and uncheck that interface in the Designate NAT Interfaces window. For details see help.

< Back | Next > | Finish | Cancel | Help

4. 出現此視窗並顯示使用者配置的配置摘要。按一下「**Finish**」（結束）。

Basic NAT Wizard

NAT Wizard
Network Address Translation

Summary of the Configuration

Click finish to deliver the configuration to the router.

Interface that is connected to the Internet or to your Internet service provider:
        Serial2/0

IP address ranges that share the Internet connection:
        172.16.1.0 to 172.16.1.255

< Back | Next > | Finish | Cancel |

5. Edit NAT Configuration（編輯NAT配置）視窗顯示已配置的動態NAT配置，其中已轉換的IP地址過載(PATing)。 如果要使用地址池配置動態NATing，請按一下**Address Pool**。

6. 按一下「**Add**」。

此處提供了池名稱和帶網路掩碼的IP地址範圍等資訊。有時池中的大多數地址都已分配，並且IP地址池已接近耗盡。發生這種情況時，PAT可與單個IP地址配合使用，以滿足對IP地址的其他請求。如果希望路由器在地址池接近耗盡時使用PAT，請檢查**埠地址轉換(PAT)**。

Add Address Pool

Pool Name: `pool1`

☑ Port Address Translation(PAT)

IP address: `192.168.1.3` -- `192.168.1.10`

Network Mask: `255.255.255.0` or `24`

OK Cancel Help

7. 按一下「**Add**」。

Address Pools

Address Pools are used to configure Dynamic Network Address Translation addresses.

	Pool Name	Address
	pool1	192.168.1.3 - 192.168.1.10

Add...
Edit...
Delete

☐ Clone selected Entry on Add

OK Cancel Help

8. 按一下「**Edit**」。

Create NAT Configuration | **Edit NAT Configuration**

Designate NAT Interfaces...   Address Pool... Translation Timeouts
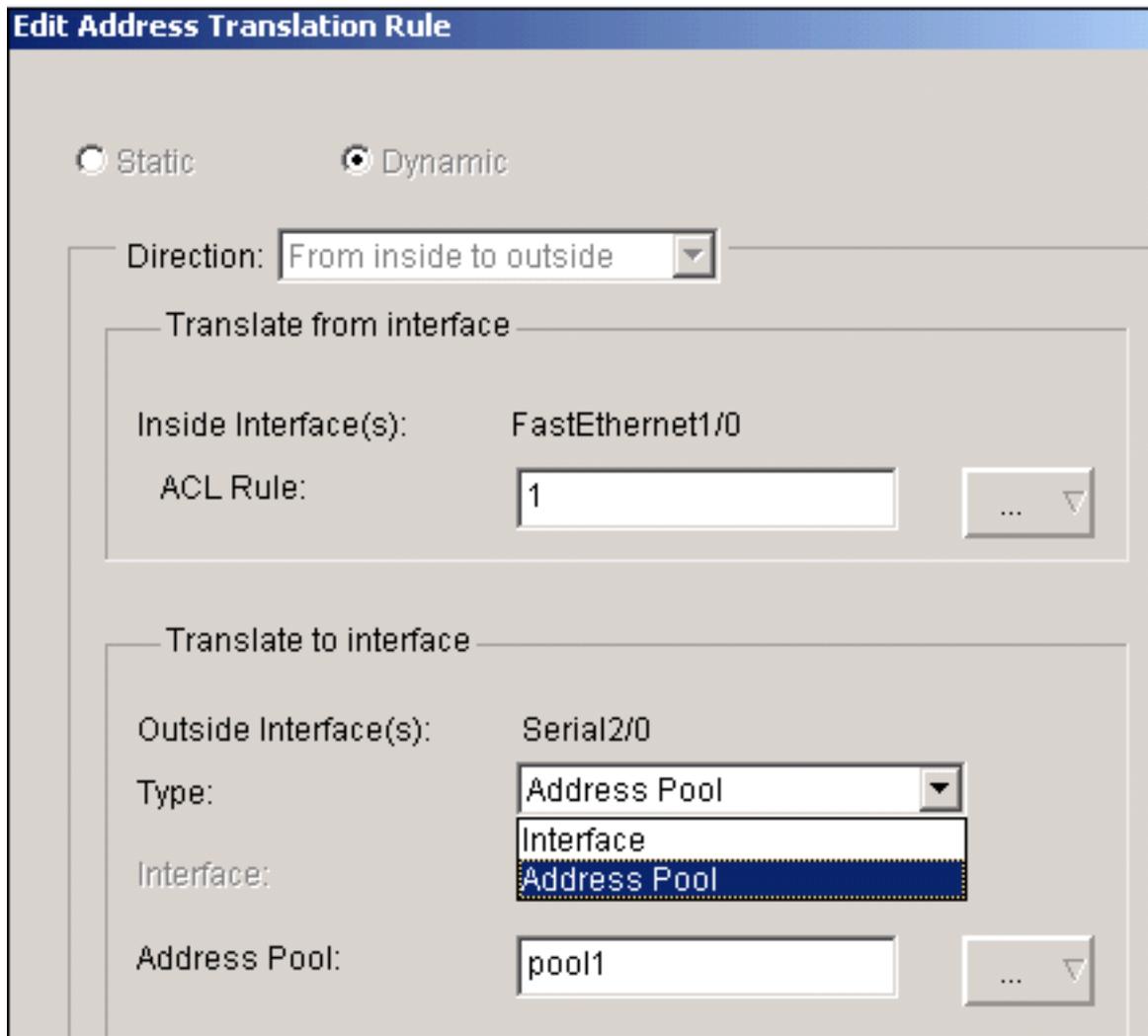
Network Address Translation Rules

Inside Interface(s): FastEthernet1/0
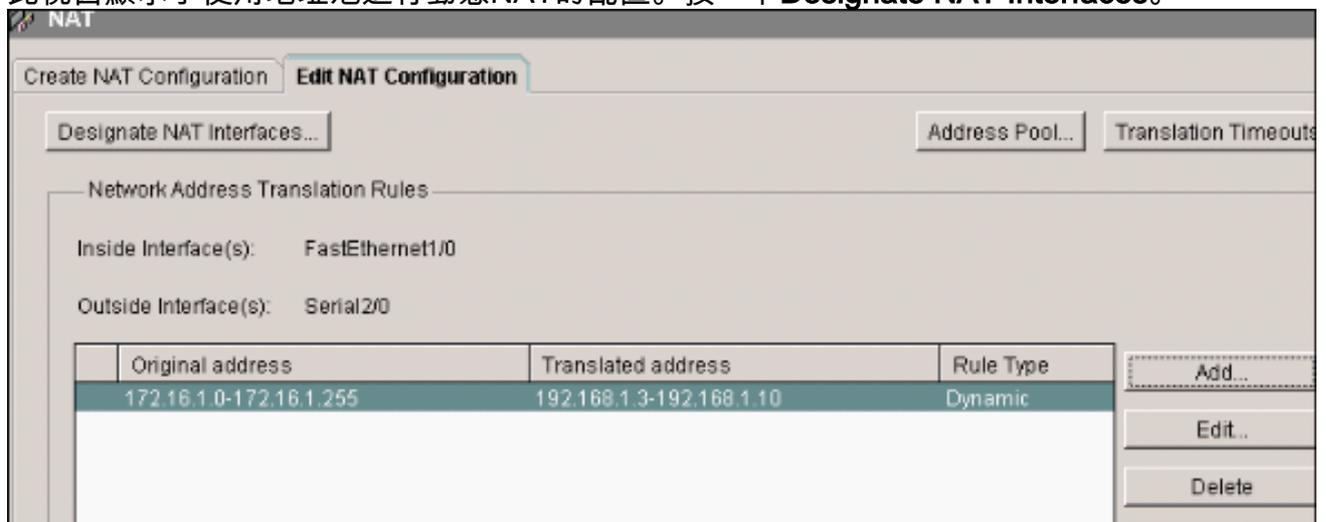
Outside Interface(s): Serial2/0

| Original address	Translated address	Rule Type
172.16.1.0-172.16.1.255	192.168.1.1	Dynamic

Add...
Edit...
Delete
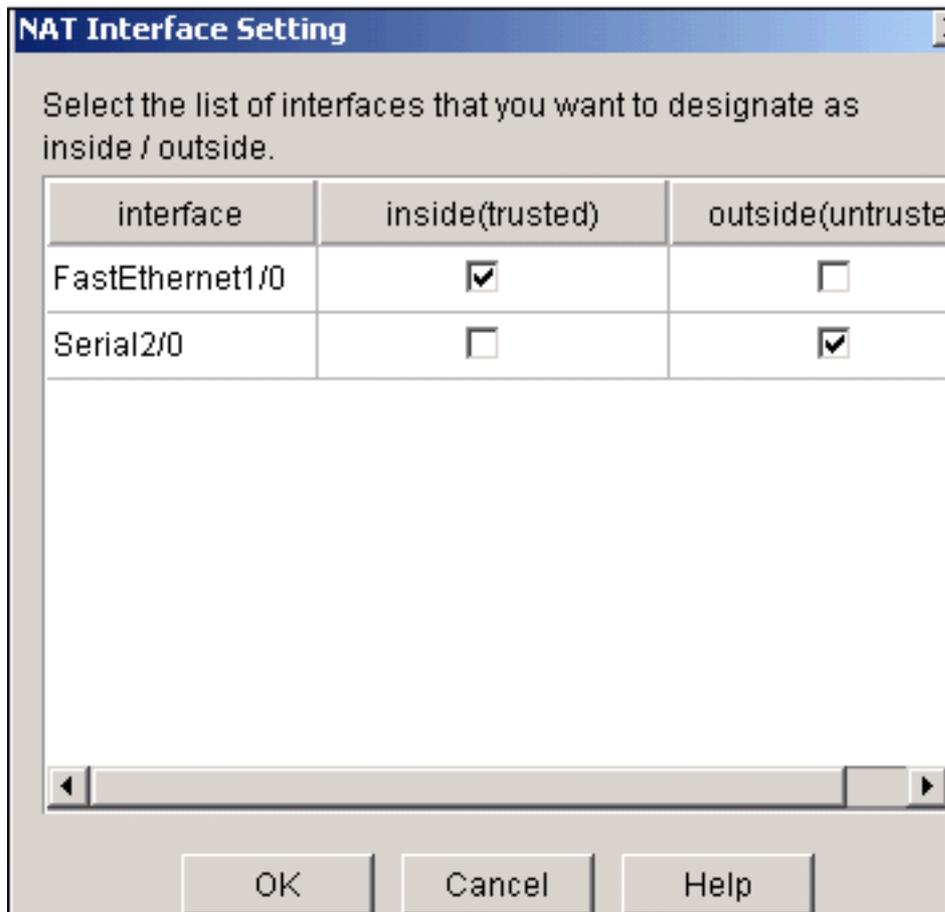
9. 在Type欄位中選擇**Address Pool**，以**pool1**的形式提供地址池的名稱，然後按一下**OK**。

10. 此視窗顯示了使用地址池進行動態NAT的配置。按一下**Designate NAT Interfaces**。
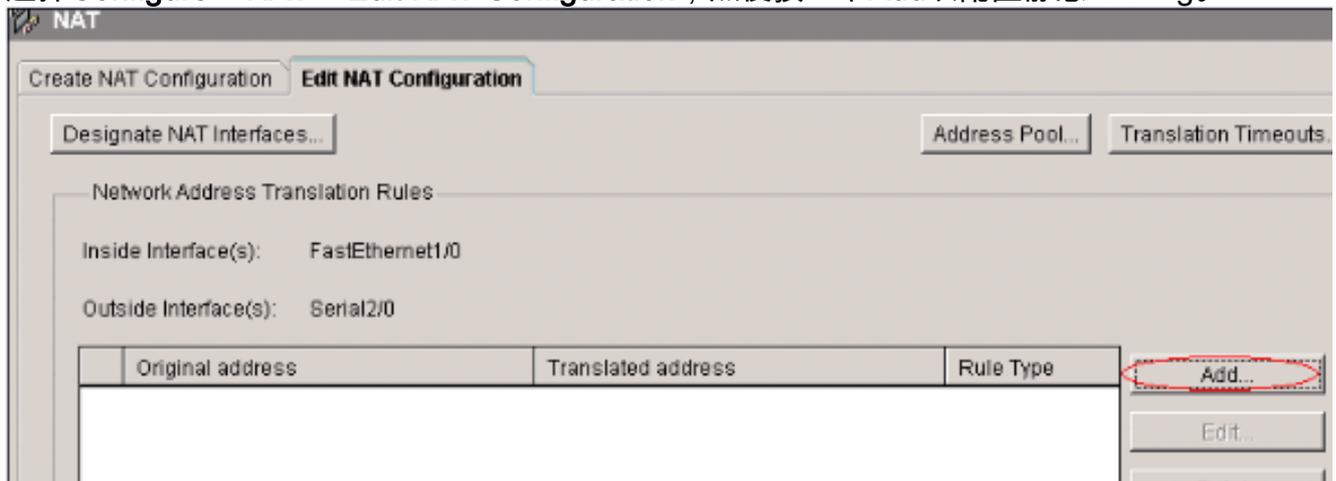
使用此視窗可以指定要在NAT轉換中使用的內部和外部介面。NAT在解釋轉換規則時使用內部和外部標識，因為轉換是從內部執行到外部，或從外部執行到內部。指定後，這些介面將用於所有NAT轉換規則。指定的介面顯示在主NAT視窗中的Translation Rules清單上方。
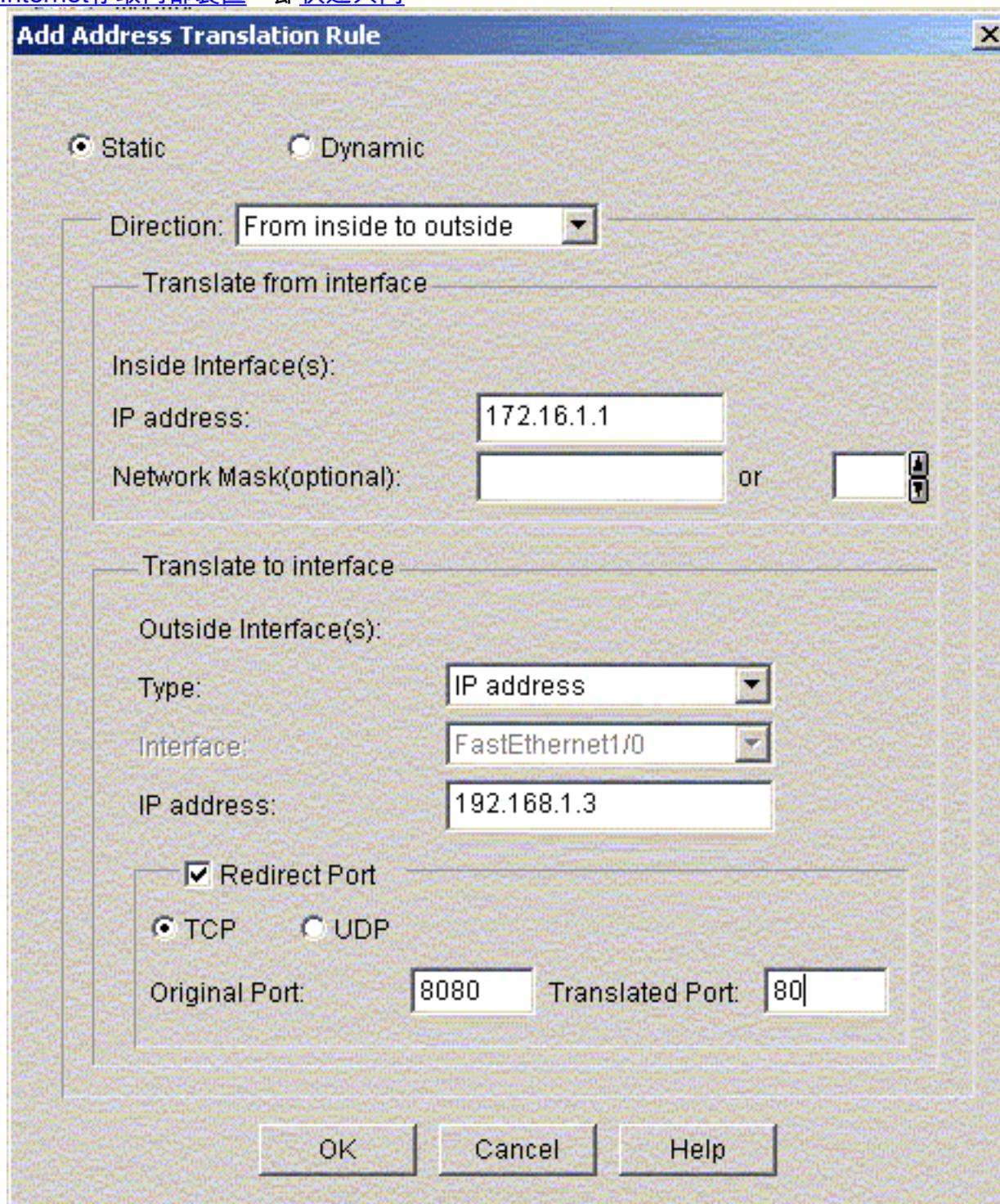
靜態NAT配置

完成這些步驟，以便在Cisco路由器中配置靜態NAT。

1. 選擇**Configure > NAT > Edit NAT Configuration**，然後按一下**Add**以配置靜態NATing。
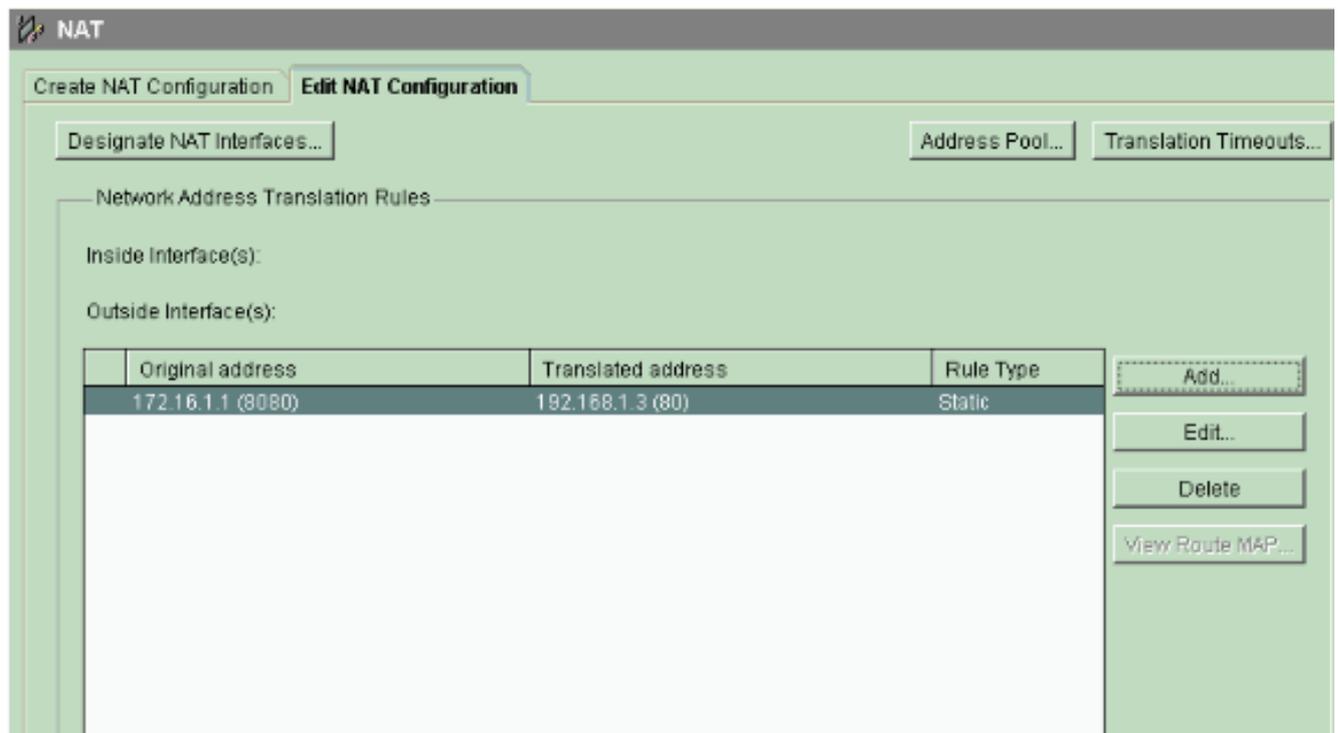
2. 選擇**Direction**（從內部到外部或從外部到內部），在**Translate from Interface**下指定要轉換的內部IP地址。在**Translate to Interface**區域中選擇Type。如果要將Translate from Address轉換為IP Address欄位中定義的IP地址，請選擇**IP Address**。如果希望**Translate from Address**使用路由器上介面的地址，請選擇**Interface**。**Translate from Address**將轉換為分配給您在Interface欄位中指定的介面的IP地址。如果您要在轉換中包括內部裝置的埠資訊，請選中**Redirect Port**。這樣，只要為每台裝置指定的埠不同，就可以對多個裝置使用相同的公共IP地址。您必須為該「轉換到」地址的每個埠對映建立一個條目。如果這是TCP埠號，請按一下**TCP**，如果是UDP埠號，請按一下**UDP**。在Original Port欄位中，輸入內部裝置上的埠號。在Translated Port欄位中，輸入路由器用於此轉換的埠號。請參閱設定網路位址轉譯：的允許

此視窗顯示了啟用了埠重定向的靜態NATing配置。
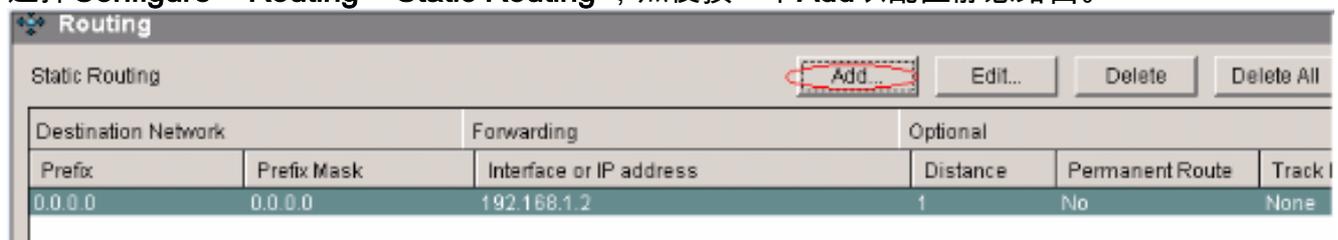
路由配置

靜態路由配置

完成這些步驟，在思科路由器中設定靜態路由。

1. 選擇Configure > Routing > Static Routing ，然後按一下Add以配置靜態路由。

2. 輸入帶有掩碼的目標網路地址，然後選擇傳出介面或下一跳IP地址。

此視窗顯示為10.1.1.0網路配置的靜態路由，其中192.168.1.2作為下一跳IP地址。

動態路由配置

完成這些步驟，在思科路由器中設定動態路由。

1. 選擇Configure > Routing > Dynamic Routing。
2. 選擇RIP，然後按一下Edit。
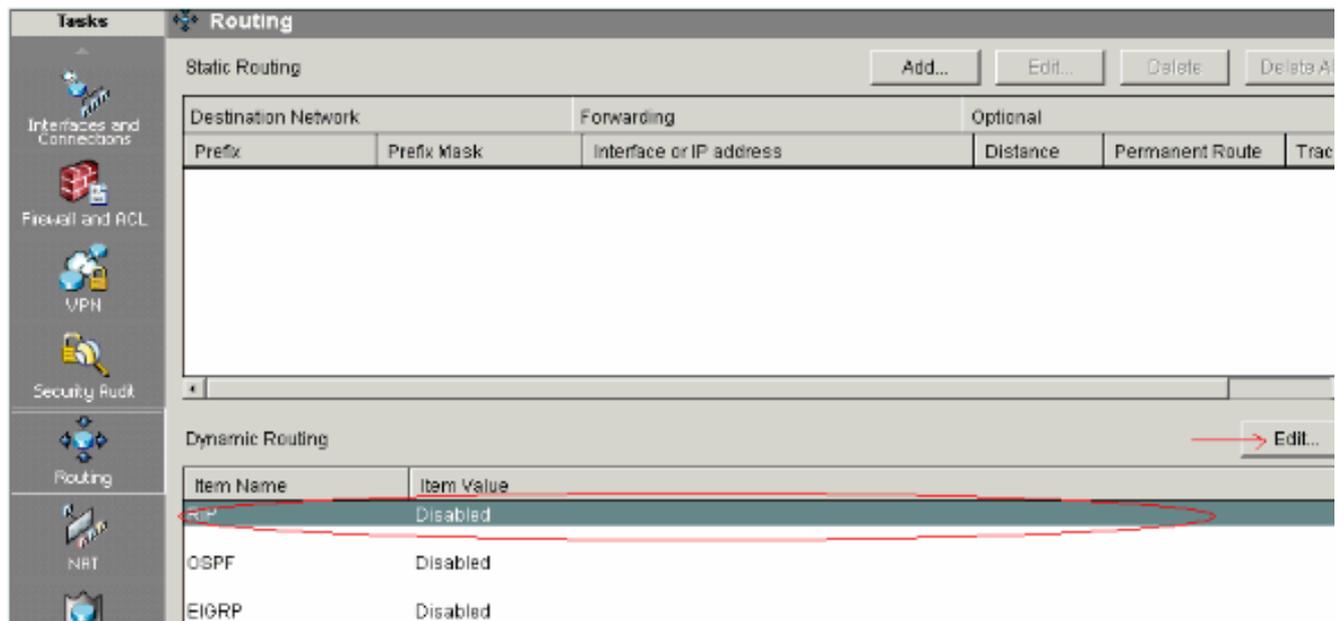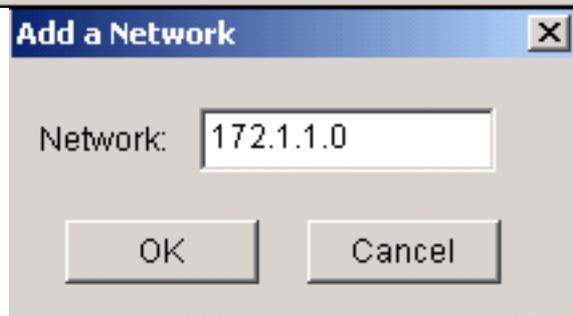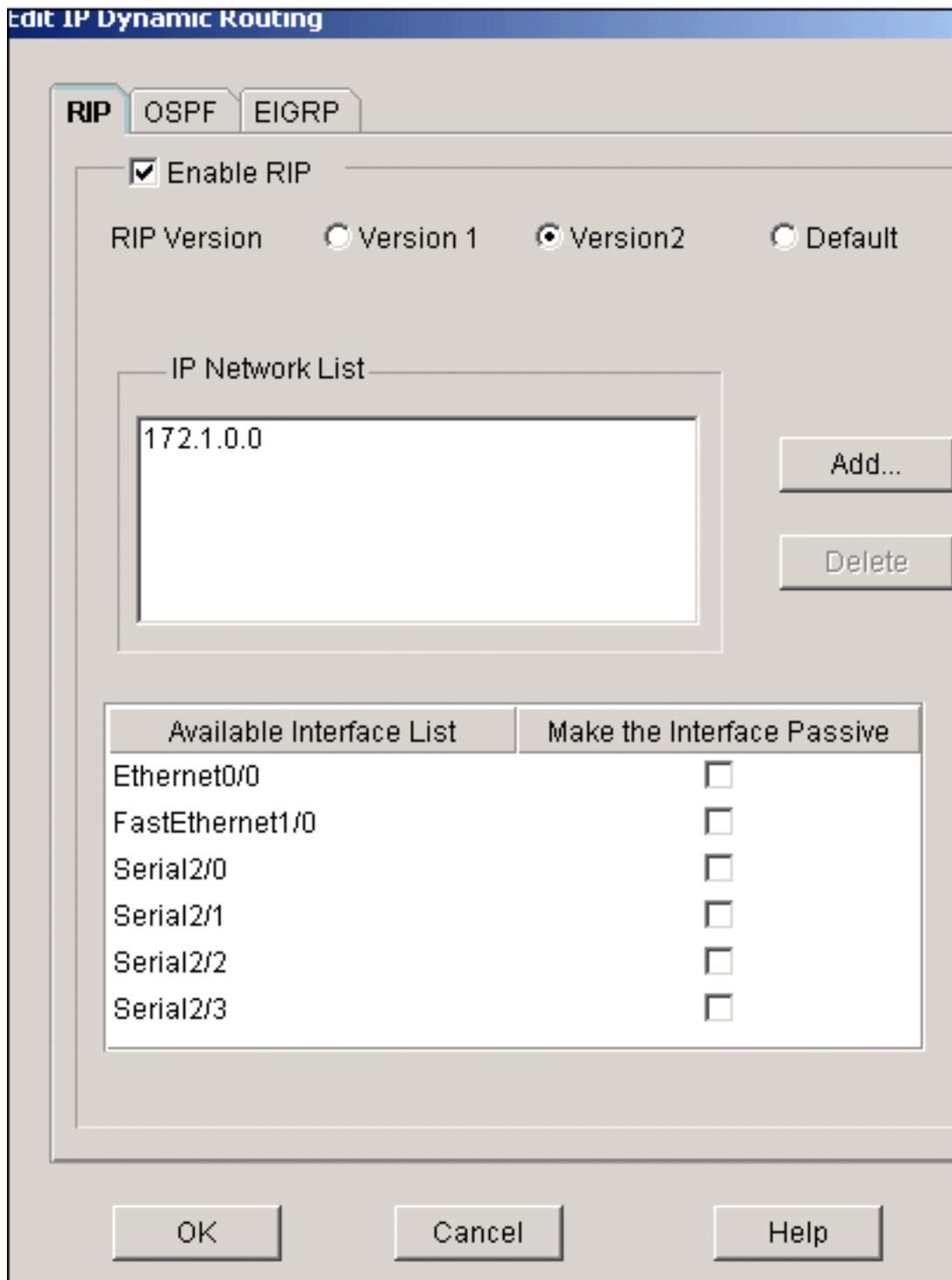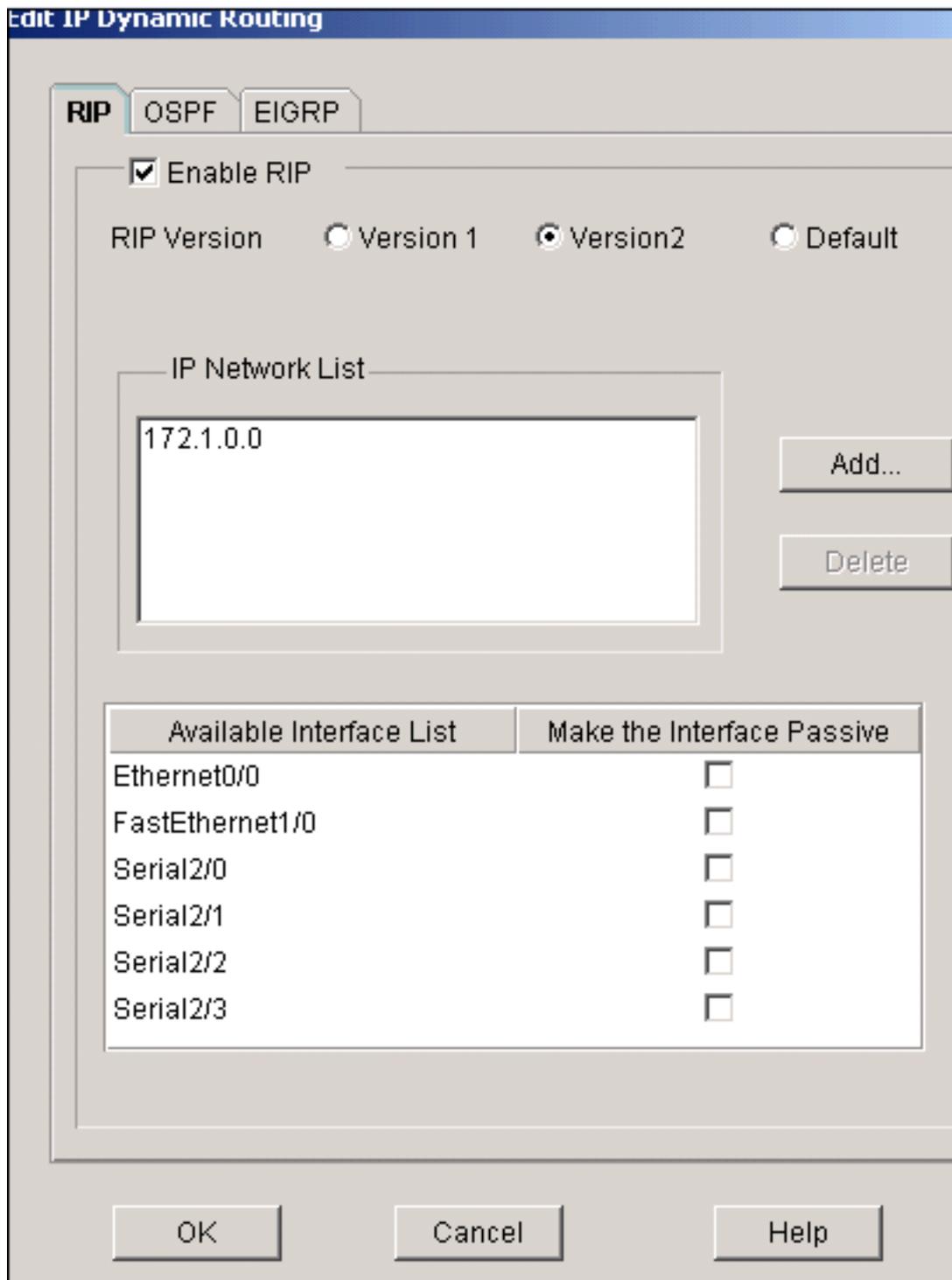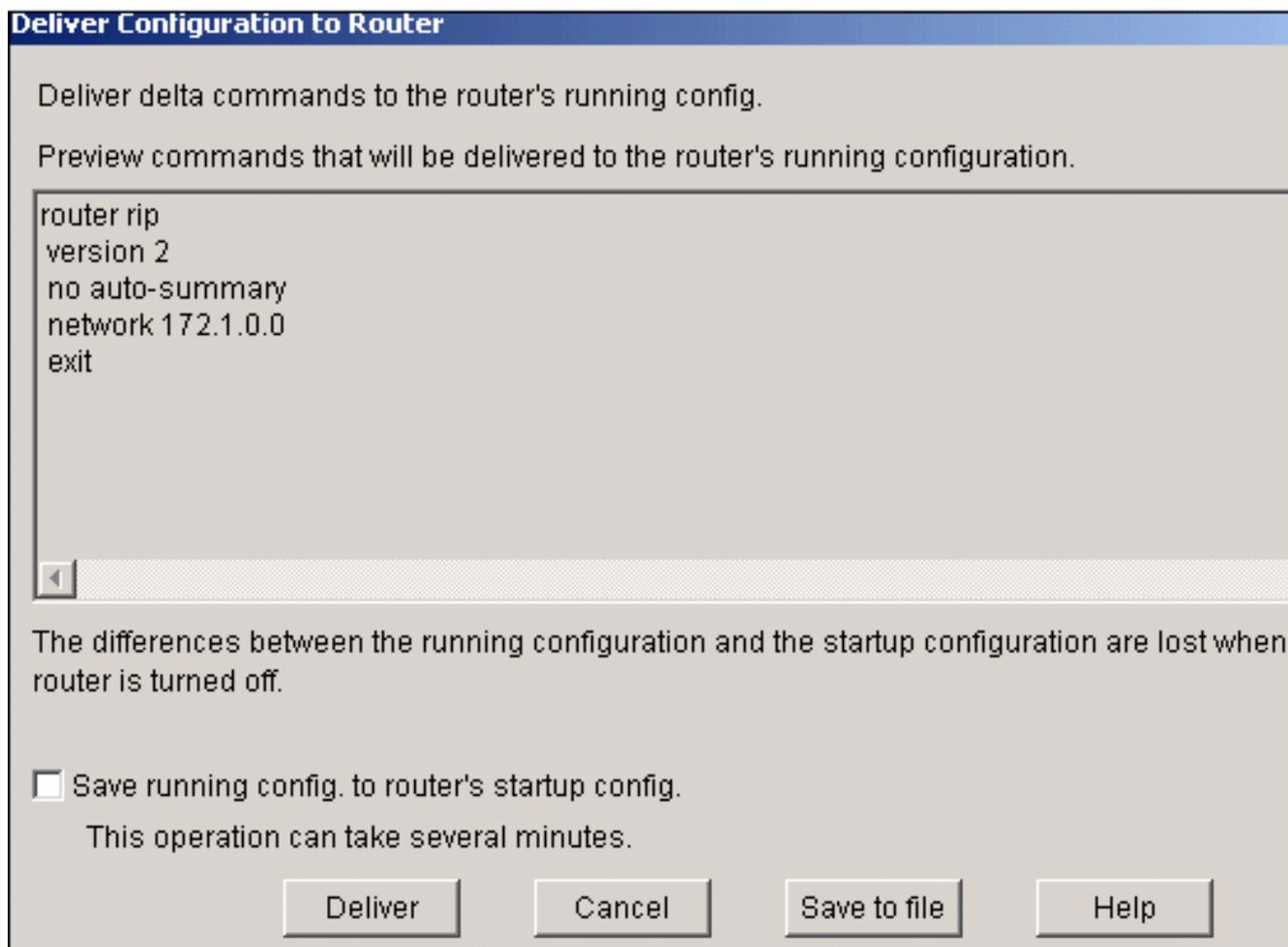
3. 選中**Enable RIP**，選擇RIP版本，然後按一下**Add**。

Edit IP Dynamic Routing

RIP | OSPF | EIGRP

☑ Enable RIP

RIP Version ○ Version 1 ● Version2 ○ Default

IP Network List

172.1.0.0

Add...

Delete

Available Interface List	Make the Interface Passive
Ethernet0/0	☐
FastEthernet1/0	☐
Serial2/0	☐
Serial2/1	☐
Serial2/2	☐
Serial2/3	☐

OK | Cancel | Help

Add a Network ✕

Network: 172.1.1.0

OK | Cancel
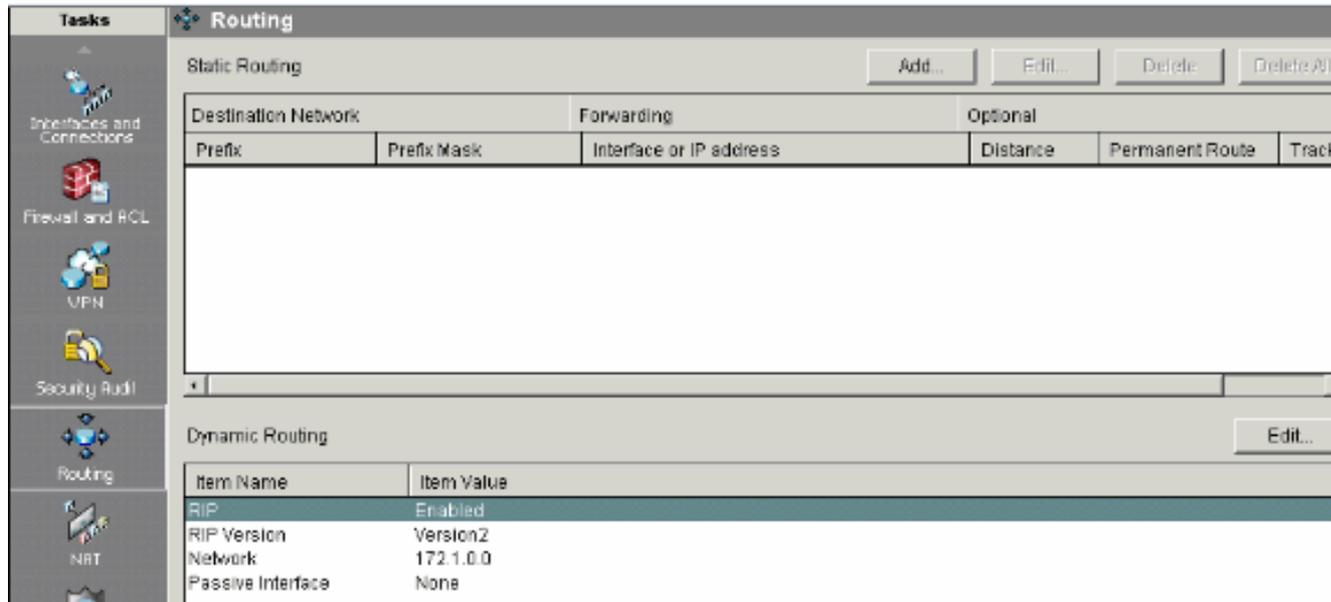
4. 指定要通告的網路地址。

5. 按一下「OK」（確定）。

6. 按一下「Deliver」將命令傳送到路由器。

Deliver Configuration to Router

Deliver delta commands to the router's running config.

Preview commands that will be delivered to the router's running configuration.

```
router rip
version 2
no auto-summary
network 172.1.0.0
exit
```

The differences between the running configuration and the startup configuration are lost when router is turned off.

☐ Save running config. to router's startup config.

This operation can take several minutes.

| Deliver | Cancel | Save to file | Help |

此視窗顯示了動態RIP路由配置。

其他配置

完成這些步驟，在思科路由器中設定其他基本設定。
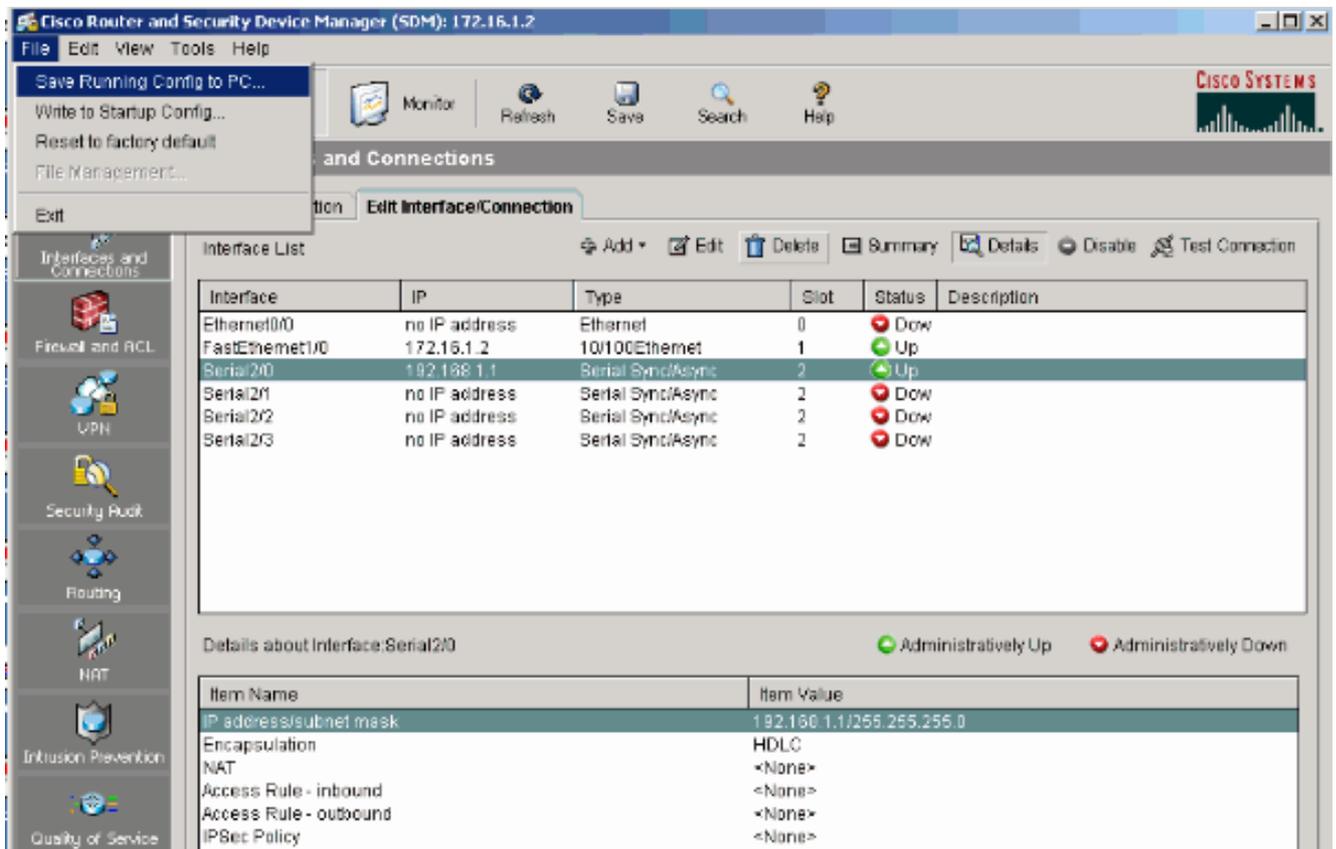
1. 如果要更改路由器的主機名、域名、標語和啟用加密口令屬性，請選擇Configure > Additional Tasks > Router Properties，然後按一下Edit。
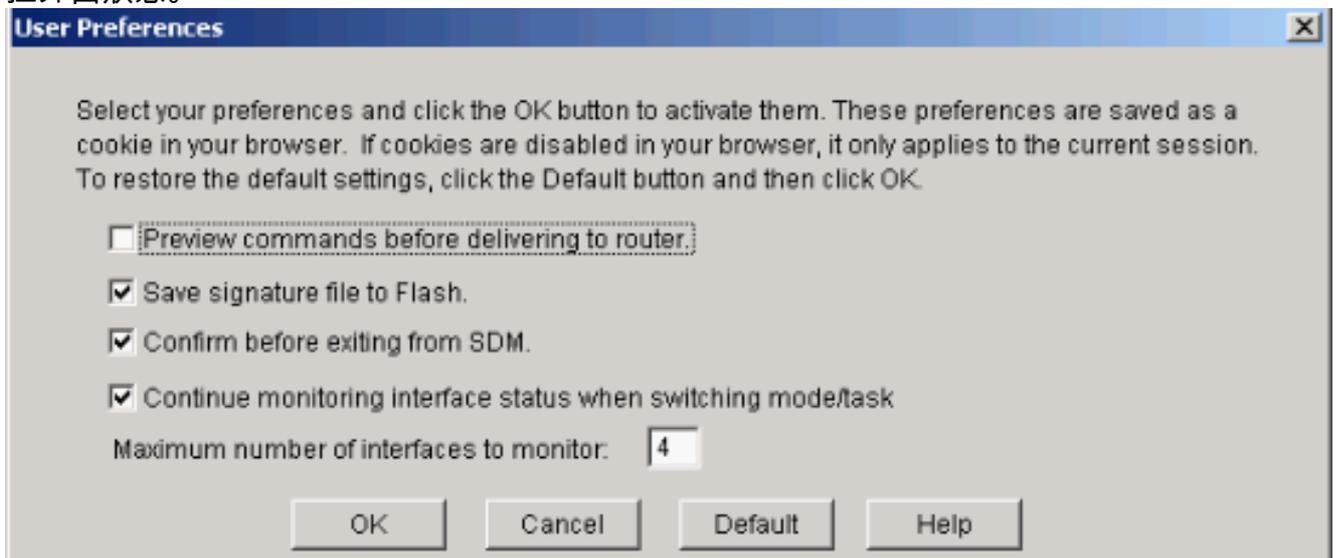
2. 選擇Configure > Additional Tasks > Router Access > User Accounts/View以向路由器新增/編輯/刪除使用者帳戶。

3. 選擇File > Save Running Config to PC...將配置儲存到路由器的NVRAM和PC並將當前配置重置為預設（工廠）設定。

4. 前往工作列並選擇**「編輯>首選項」**以啟用以下「使用者首選項」選項：在將命令傳送到路由器之前進行預覽。將簽名檔案儲存到快閃記憶體。退出SDM前確認。交換模式/任務時繼續監控介面狀態。

5. 如果您要執行以下操作，請從工作列中選擇**檢視**:檢視「首頁」、「配置」或「監控」頁。檢視路由器的運行配置。檢視各種show命令。檢視SDM預設規則。如果通過CLI與SDM配置了路由器配置，請選擇Refresh以同步路由器配置。

CLI組態

路由器配置
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
  0DD0BE16 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 Translation (NAT).* **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 match access list 1 !--- are NATed to the address pool named pool1.* 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**
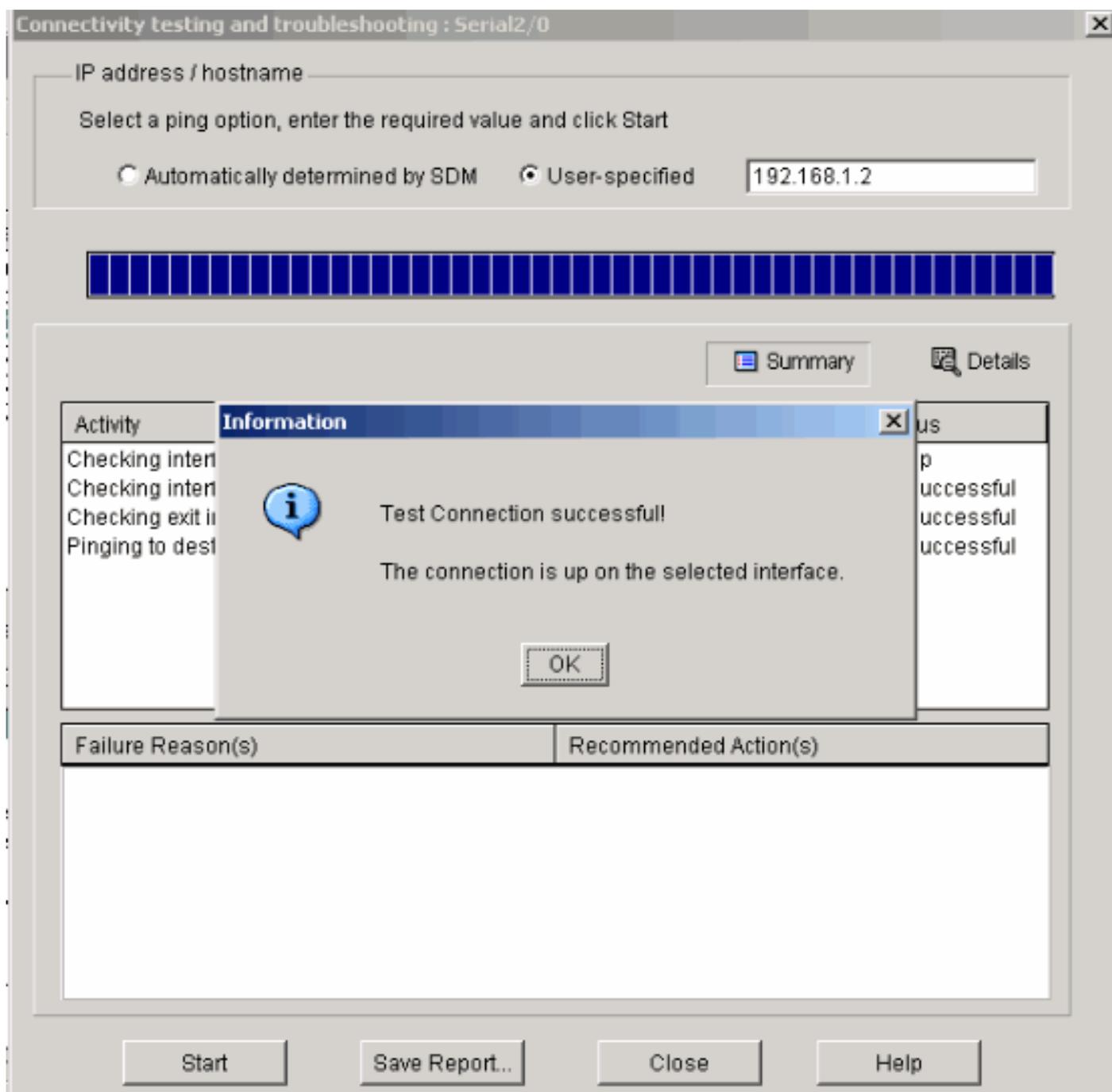
!--- In order to translate the packets between the real IP address 172.16.1.1 with TCP !--- port 80 and the mapped IP address 192.168.1.1 with TCP port 500. **ip nat inside source static tcp 172.16.1.1 80 192.168.1.3 500 extendable**
```
!
!

!
```

```
!
!--- The default route is configured and points to
192.168.1.2. ip route 0.0.0.0 0.0.0.0 192.168.1.2 ! ! !-
-- The static route is configured and points to
192.168.1.2. ip route 10.1.1.0 255.255.255.0 192.168.1.2
! ! control-plane ! ! ! ! ! ! ! ! ! ! line con 0 line
aux 0 !--- Telnet enabled with password as sdmsdm. line
vty 0 4 password sdmsdm login ! ! end
```

驗證

選擇Configure > Interface & Connections > Edit Interface Connections > Test Connection以測試端到端連線。如果按一下User-specified單選按鈕，則可以指定遠端終端IP地址。
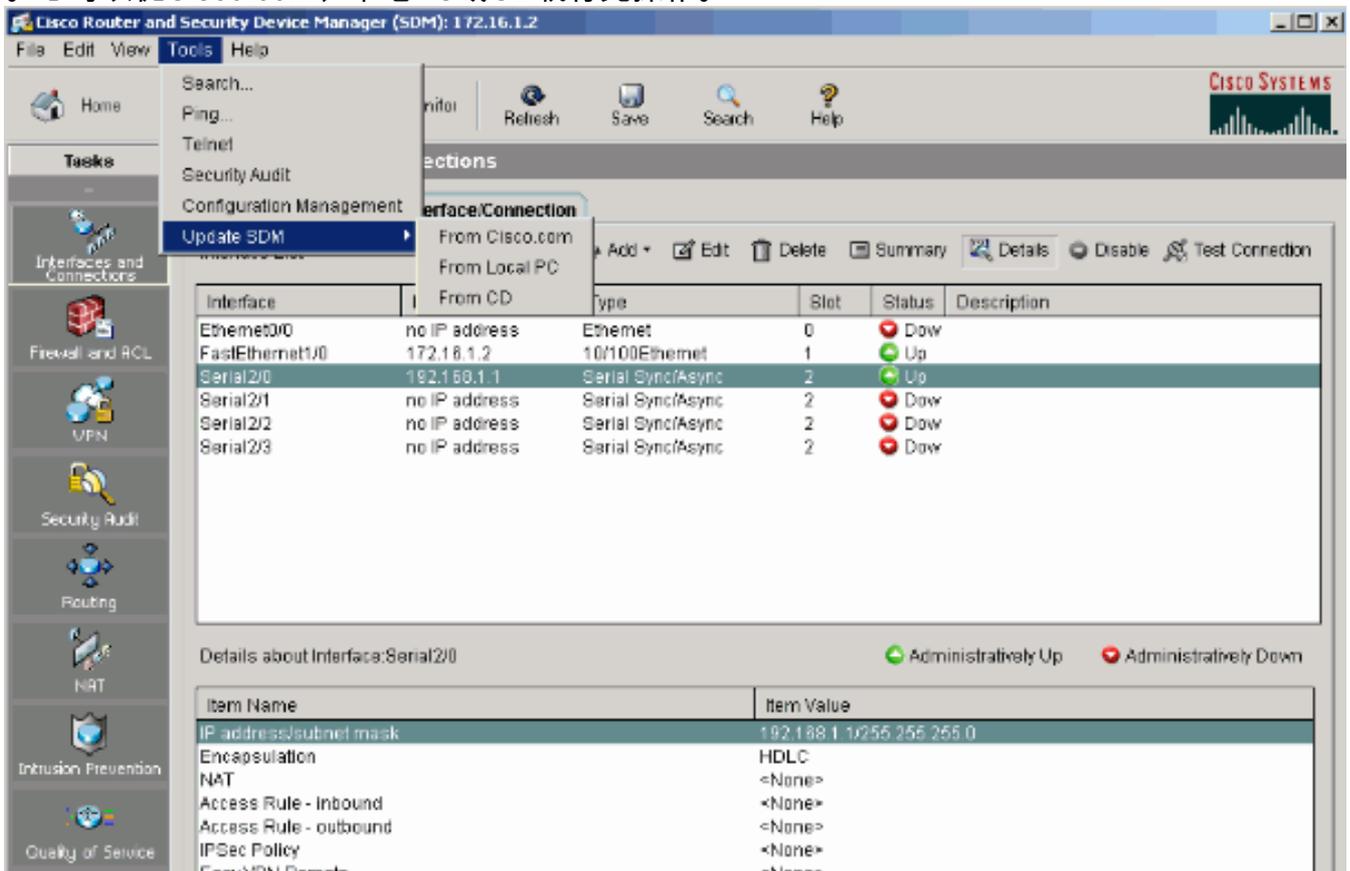
疑難排解

[輸出直譯器工具](僅供[已註冊]客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。
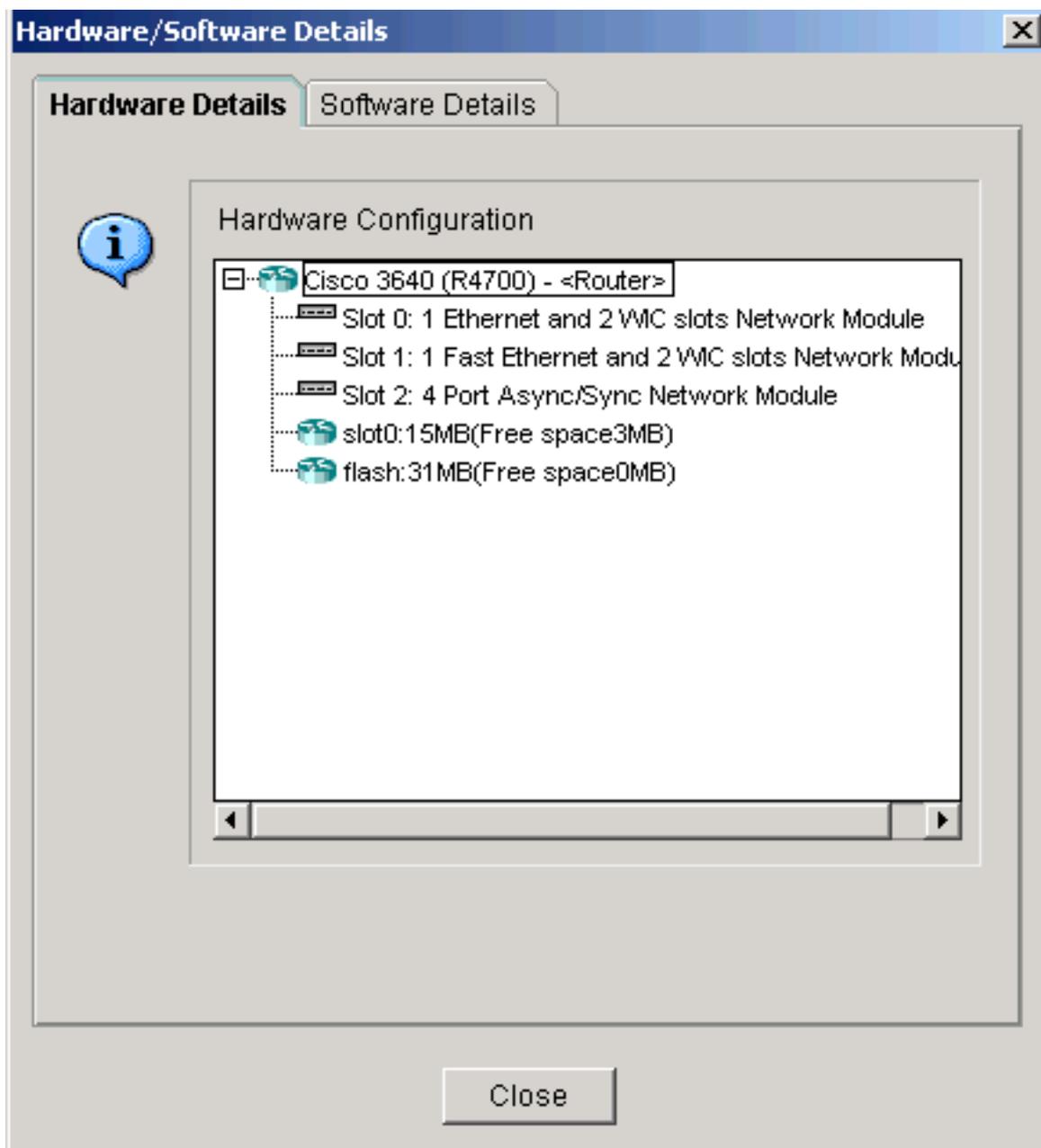
註:在發出debug命令前[,請先參閱]有關Debug命令的重要資訊。

您可以使用以下選項進行疑難排解:

- 從工作列中選擇「**Tools > Update SDM**」,以執行ping、Telnet操作並將SDM升級到最新版本。您可以從Cisco.com、本地PC或CD執行此操作。

- 選擇**Help > About this Router**,以檢視有關路由器硬體配置的資訊。

Hardware/Software Details

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
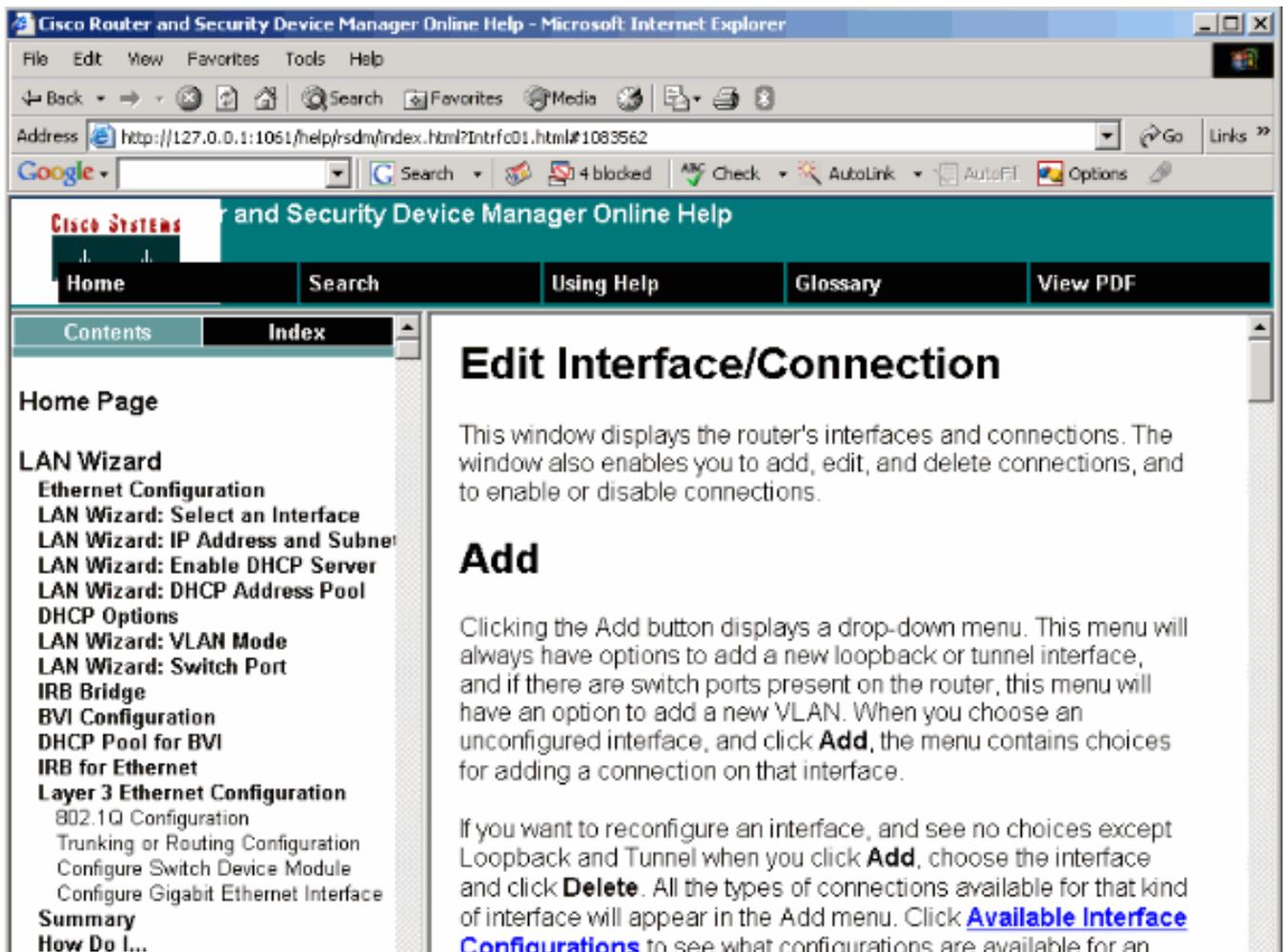
此視窗顯示有關路由器中儲存的IOS映像的資訊。

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]

- **Help**選項提供有關SDM中用於配置路由器的各種可用選項的資訊。

SDM與64位作業系統的相容性

具有64位作業系統的電腦上不支援SDM。您應該在路由器上安裝SDM，並通過Web瀏覽器訪問它。

請參閱任務4:安裝SDM檔案，瞭解有關在路由器上安裝SDM檔案的詳細資訊。

無法通過Web瀏覽器啟動SDM

問題

通過Web瀏覽器使用SDM時，會出現SDM start up錯誤消息。

解決方案1

問題可能出在Java的版本上。Java更新可能與SDM版本不相容。如果Java的版本是Java 6更新12，則解除安裝該版**本，然後安裝Java 6更新3**。這樣可解決該問題。有關相容性的詳細資訊，請參閱SDM 2.5發行說明的Web瀏覽器版本和Java運行時環境版本一節。SDM版本2.5在Java版本6的更新2和3下運行。

解決方案2

啟用**Allow active content to run in files on My Computer** on Internet Explorer選項以解決問題。

1. 開啟Internet Explorer並選擇「工具」>「Internet選項」>「高級」。

2. 在「安全」部分下，確保選中**允許活動內容在我的電腦上的檔案中運行**和**允許活動內容安裝軟體（即使簽名無效）**選項旁邊的複選框。
3. 現在，按一下**OK**並重新啟動瀏覽器以使更改生效。

錯誤：java.bling堆疊溢位

問題

我無法連線到SDM，收到以下錯誤消息：

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

解決方案

此問題通常發生在使用Java代碼版本1.5.0_06時。有關如何解決此問題的資訊，請參閱使用者無法連線到安全裝置管理器(SDM)並收到java.bling stack over flow錯誤消息。

相關資訊

- 思科安全裝置管理器安裝指南
- 思科產品支援頁面 — 路由器
- 思科組態專業版支援頁面
- NAT支援頁面
- 技術支援與文件 - Cisco Systems