

SDM によるルータ設定の基礎

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[ネットワーク図](#)

[インターフェイス設定](#)

[NAT 設定](#)

[ルーティング設定](#)

[その他の設定](#)

[CLI での設定](#)

[確認](#)

[トラブルシューティング](#)

[SDM の 64 ビット OS との互換性](#)

[Web ブラウザから SDM を起動できない](#)

[エラー:java.bling のスタック オーバーフロー](#)

[関連情報](#)

概要

このドキュメントでは、[Cisco Security Device Manager \(SDM \)](#) を使用して、[ルータの基本的な設定を行う方法について説明します](#)。基本的な設定には、IP アドレス、デフォルト ルーティング、スタティック ルーティングおよびダイナミック ルーティング、スタティック NAT およびダイナミック NAT、ホスト名、バナー、シークレット パスワード、ユーザ アカウントなどの設定が含まれます。Cisco SDM では、使いやすい Web ベースの管理インターフェイスを使用して、Small Office Home Office (SOHO)、Branch Office (BO; 営業所)、支店、中央サイト、本社など、さまざまなネットワーク環境内のルータを設定できます。

前提条件

要件

このドキュメントでは、Cisco ルータが完全に動作しており、Cisco SDM で設定変更できるように設定されていることを想定しています。

注：ルータをSDMで設定するには、[『SDM用のHTTPSアクセスの許可』](#)を参照してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco IOS²ソフトウェア リリース 12.4(8) が稼働中の Cisco 3640 ルータ
- Cisco Security Device Manager (SDM) バージョン 2.3.1

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

注：Ciscoサービス統合型ルータ(ISR)を使用する場合は、より強力な機能を備えた同様の設定の詳細については、[『Cisco Configuration Professionalを使用した基本的なルータ設定』](#)を参照してください。Cisco CP でサポートされているルータについては、『*Release Notes for Cisco Configuration Professional 2.5*』の「[Supported Routers](#)」の項を参照してください。

表記法

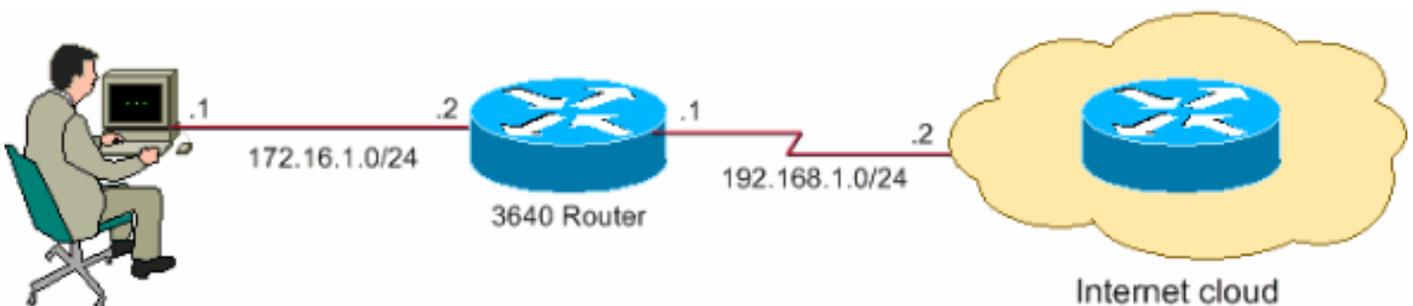
ドキュメント表記の詳細については、『[シスコテクニカルティップスの表記法](#)』を参照してください。

設定

このセクションでは、ネットワーク内にあるルータの基本的な設定を行うための情報を提供します。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



注：この設定で使用されるIPアドレッシング方式は、インターネット上で正式にルーティング可能なものではありません。これらは、ラボ環境で使用された [RFC 1918](#) のアドレスです。

インターフェイス設定

Cisco ルータのインターフェイスを設定するには、次の手順を実行します。

1. [Home] をクリックして、[SDM Home] ページに移動します。SDM Home ページでは、ルータのハードウェアやソフトウェア、機能の可用性、および設定の概略などの情報が提供されています。緑色の円はこのルータでサポートされている機能、赤色の円はサポートされていない機能を示しています。

Cisco Router and Security Device Manager (SDM): 172.16.1.2

File Edit View Tools Help

Home Configure Monitor Refresh Save Search Help

About Your Router Host Name: Router



Cisco 3640

Hardware	More...	Software	More...
Model Type:	Cisco 3640	IOS Version:	12.4(8)
Available / Total Memory(MB):	48/128 MB	SDM Version:	2.1
Total Flash Capacity:	48 MB		

Feature Availability: IP Firewall VPN IPS NAC

Configuration Overview View Running Config

Interfaces and Connections Up (1) Down (5)

Total Supported LAN:	2	Total Supported WAN:	4(Serial Sync/Async)
Configured LAN Interface:	1	Total WAN Connections:	1(HDLC)
DHCP Server:	Not Configured		

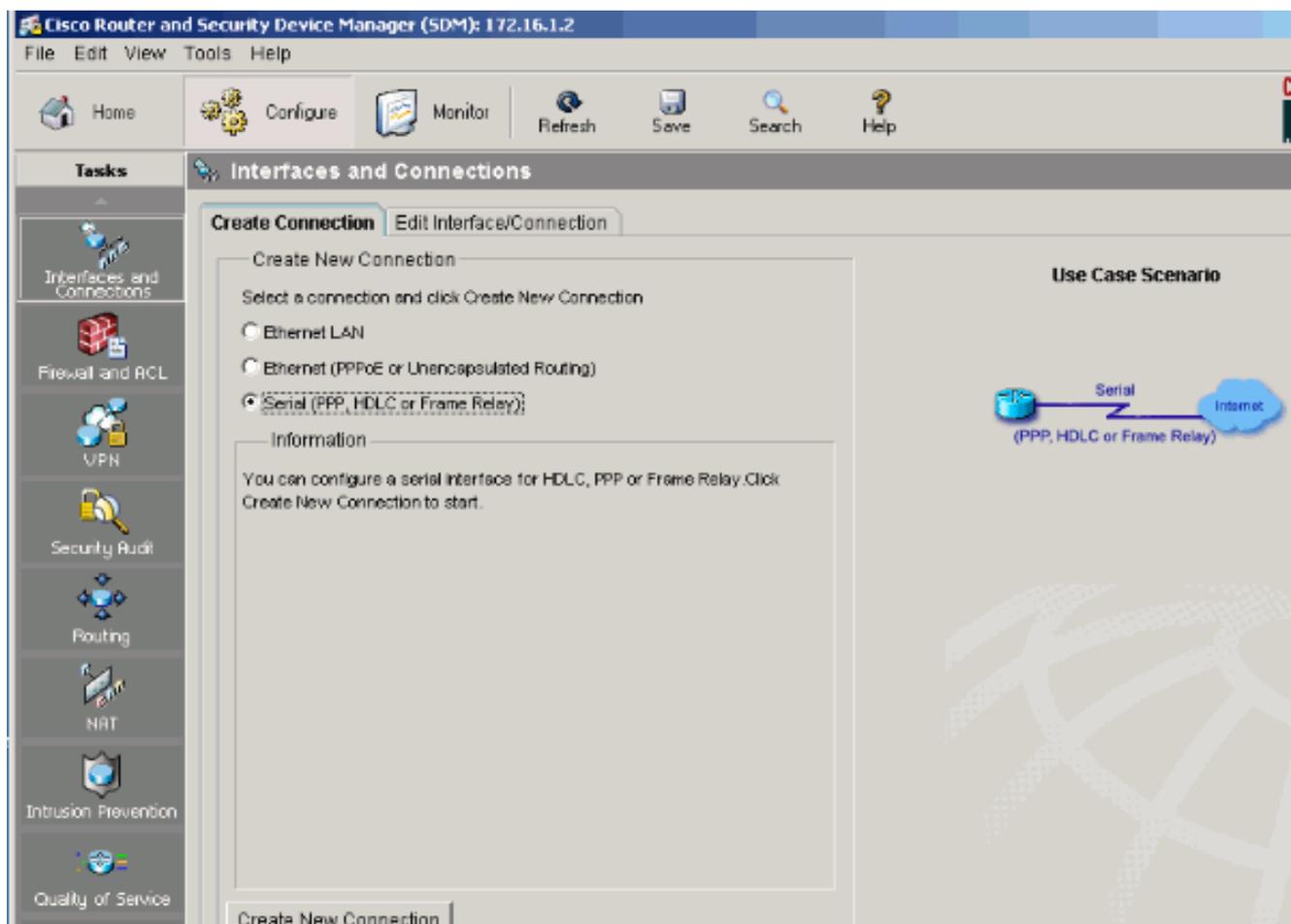
VPN Up (0)

IPSec (Site-to-Site):	0	GRE over IPSec:	0
Xauth Login Required:	0	Easy VPN Remote:	0
No. of DMVPN Clients:	0	No. of Active VPN Clients:	0

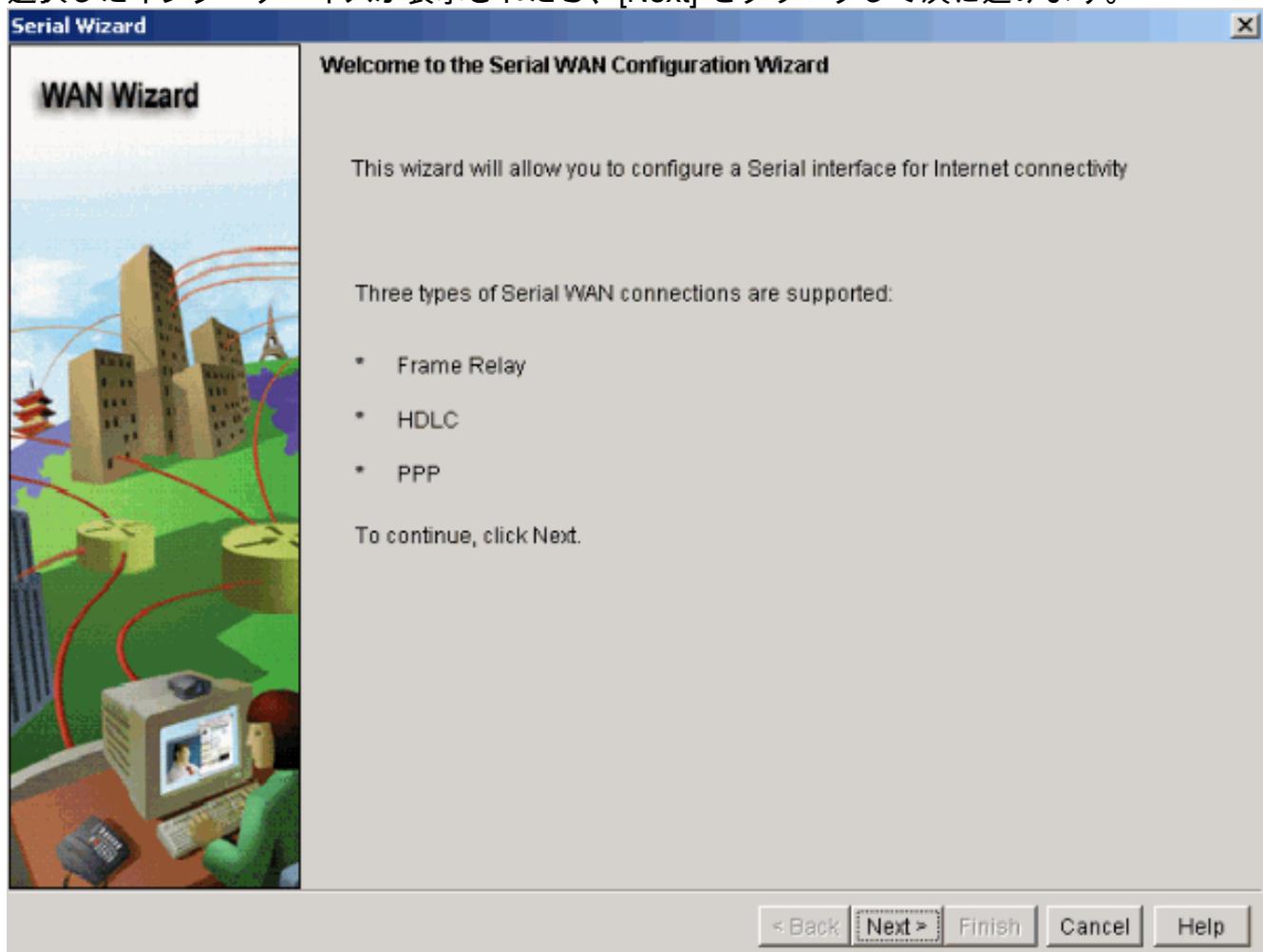
Routing

No. of Static Route:	0
Dynamic Routing Protocols:	None

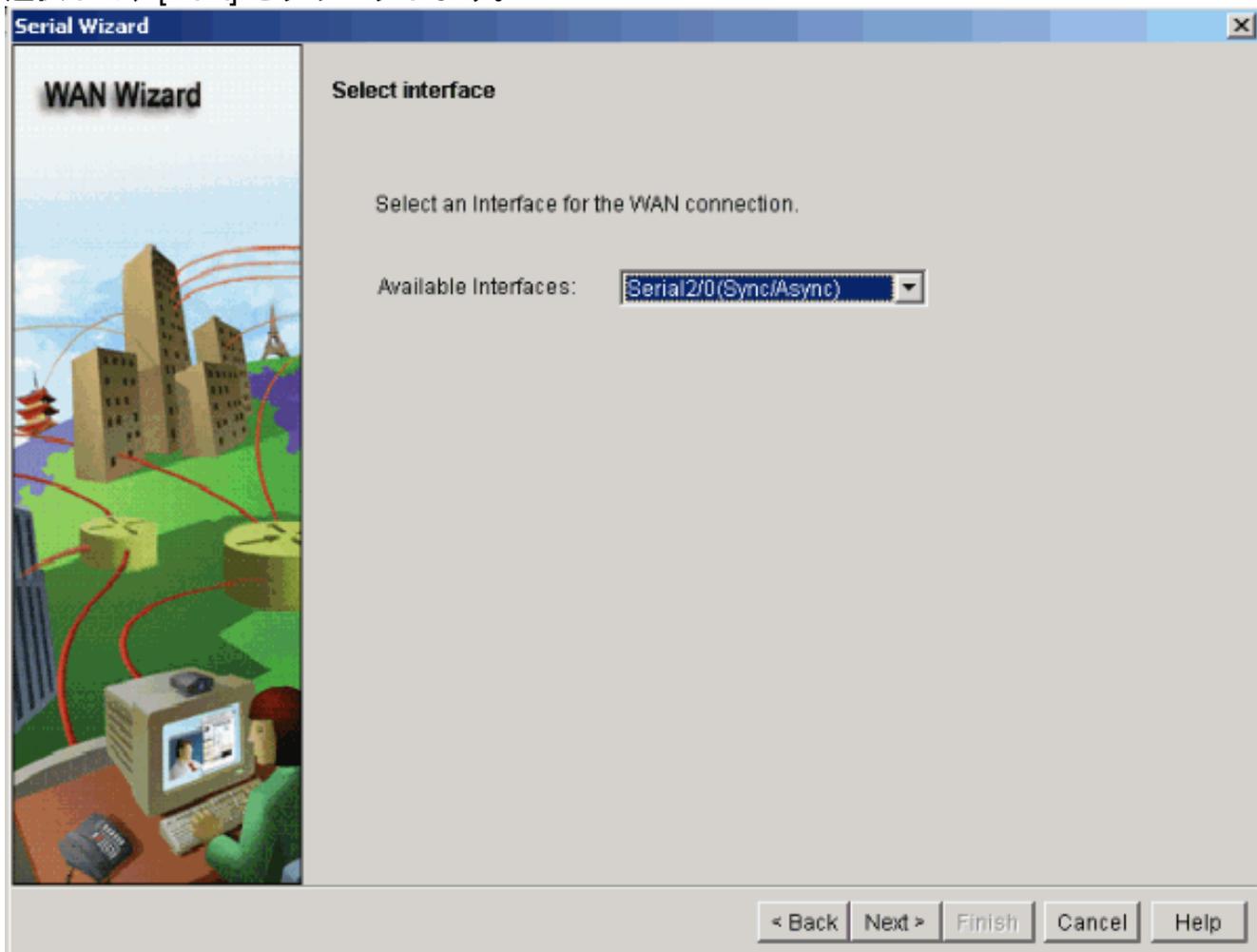
2. [Configure] > [Interfaces and Connections] > [Create Connection] を選択して、インターフェイスの WAN 接続を設定します。例として、シリアルインターフェイス 2/0 の場合は、[Serial] オプションを選択して [Create New Connection] をクリックします。注：イーサネットなどの他のタイプのインターフェイスの場合は、各インターフェイスタイプを選択し、[Create New Connection] ボタンをクリックして続行します。



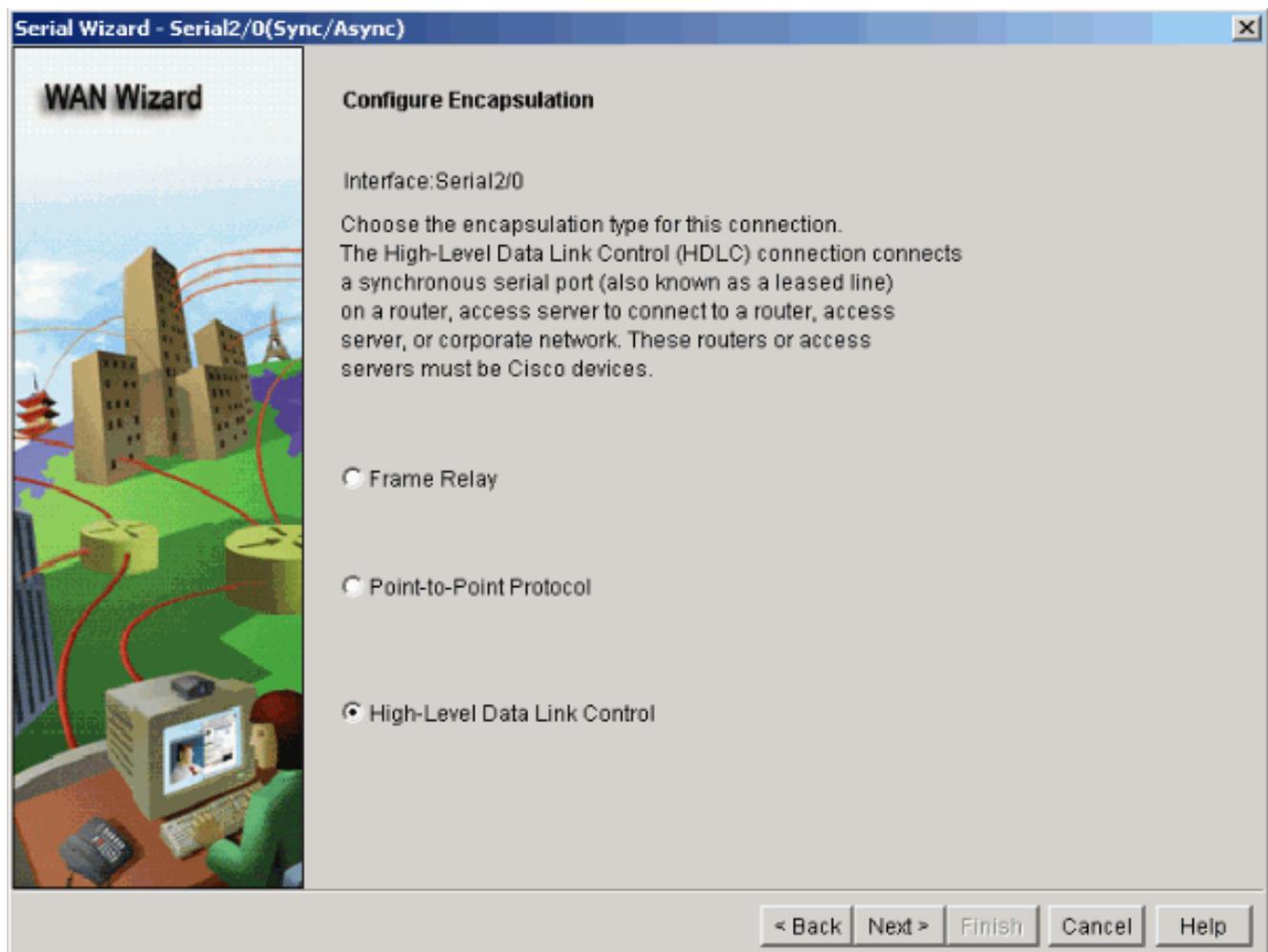
3. 選択したインターフェイスが表示されたら、[Next] をクリックして次に進みます。



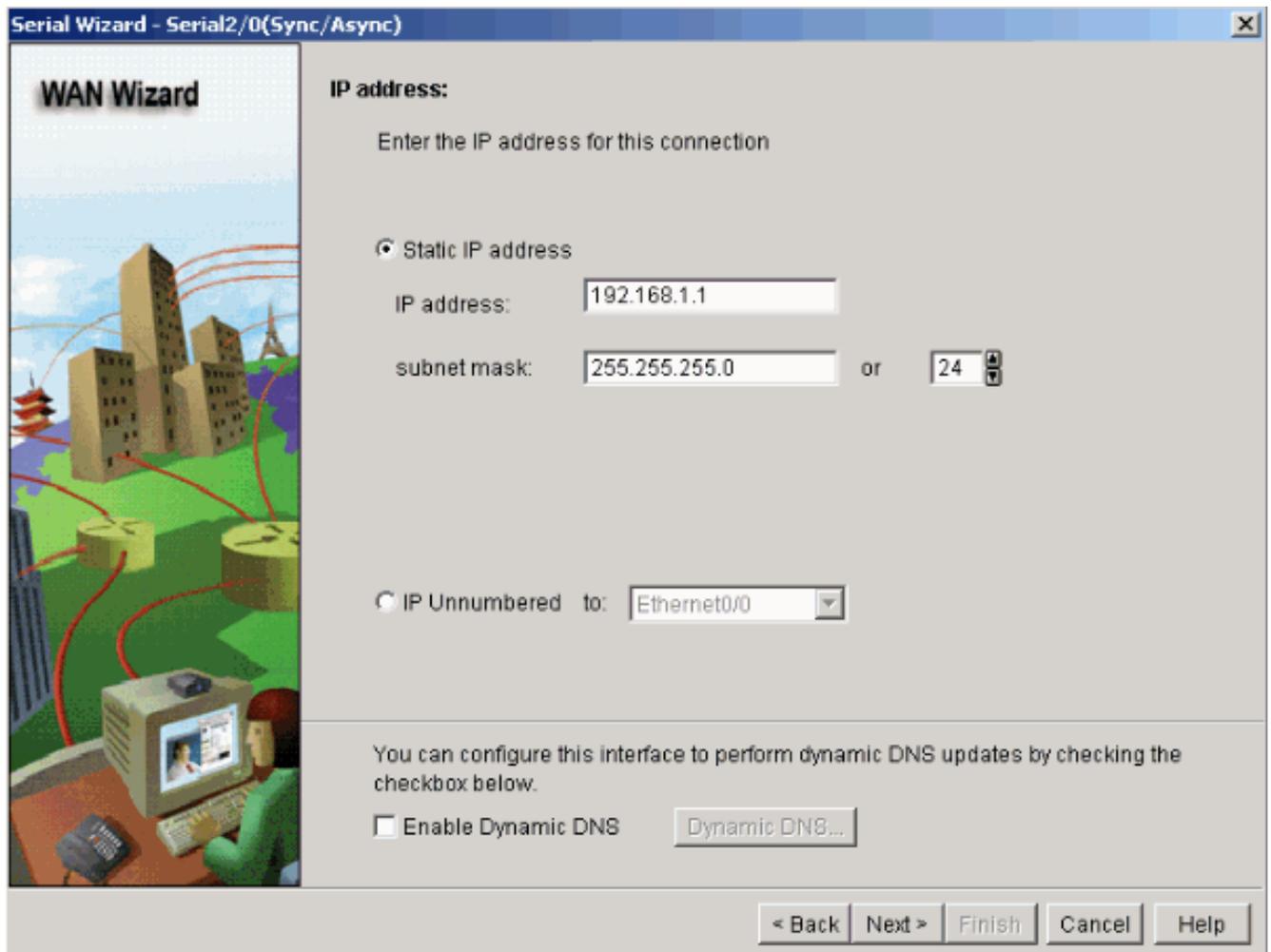
4. [Available Interfaces] のオプションから [Serial interface 2/0] (目的のインターフェイス) を選択して、[Next] をクリックします。



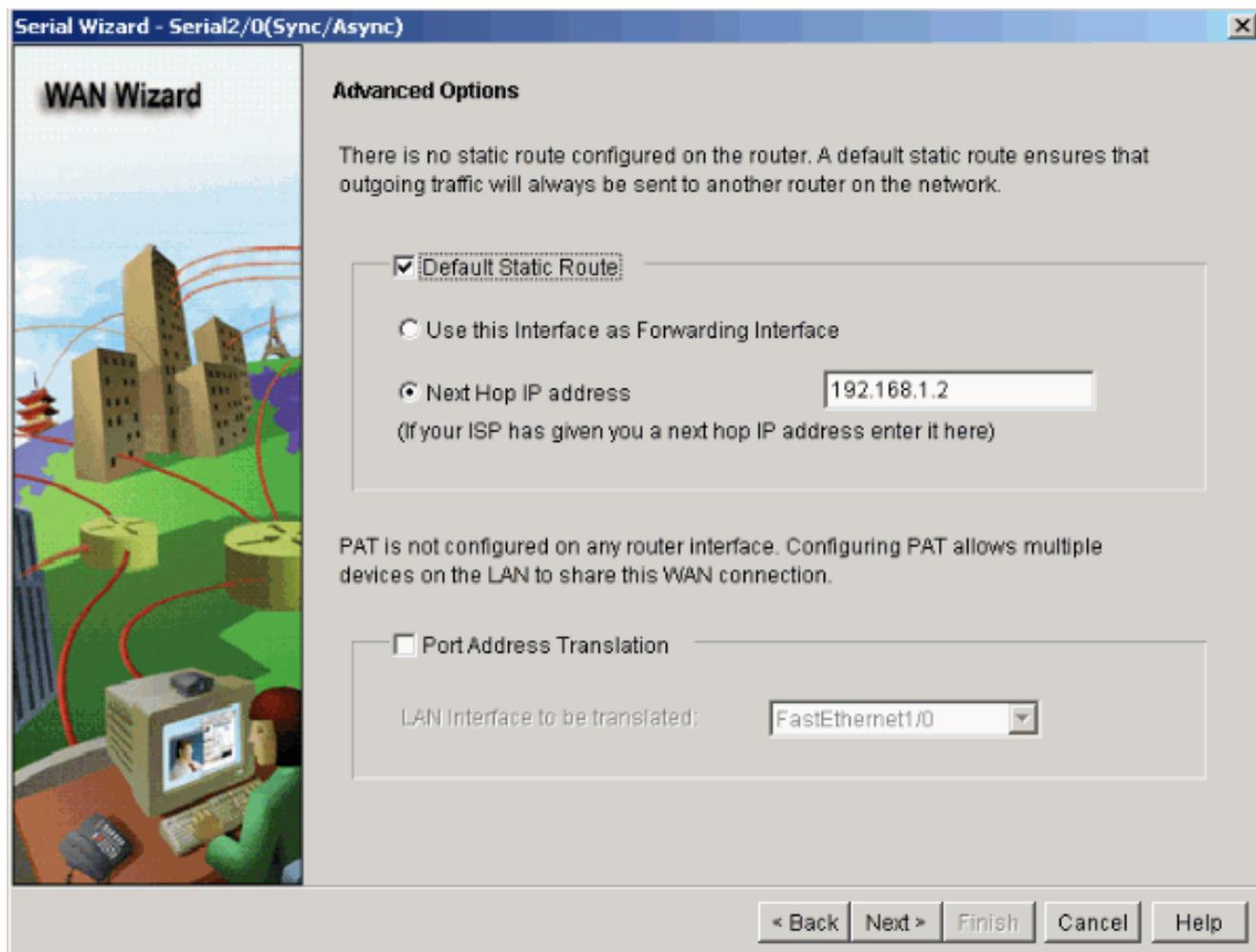
5. シリアル インターフェイスのカプセル化の種類を選択して、[Next] をクリックします。



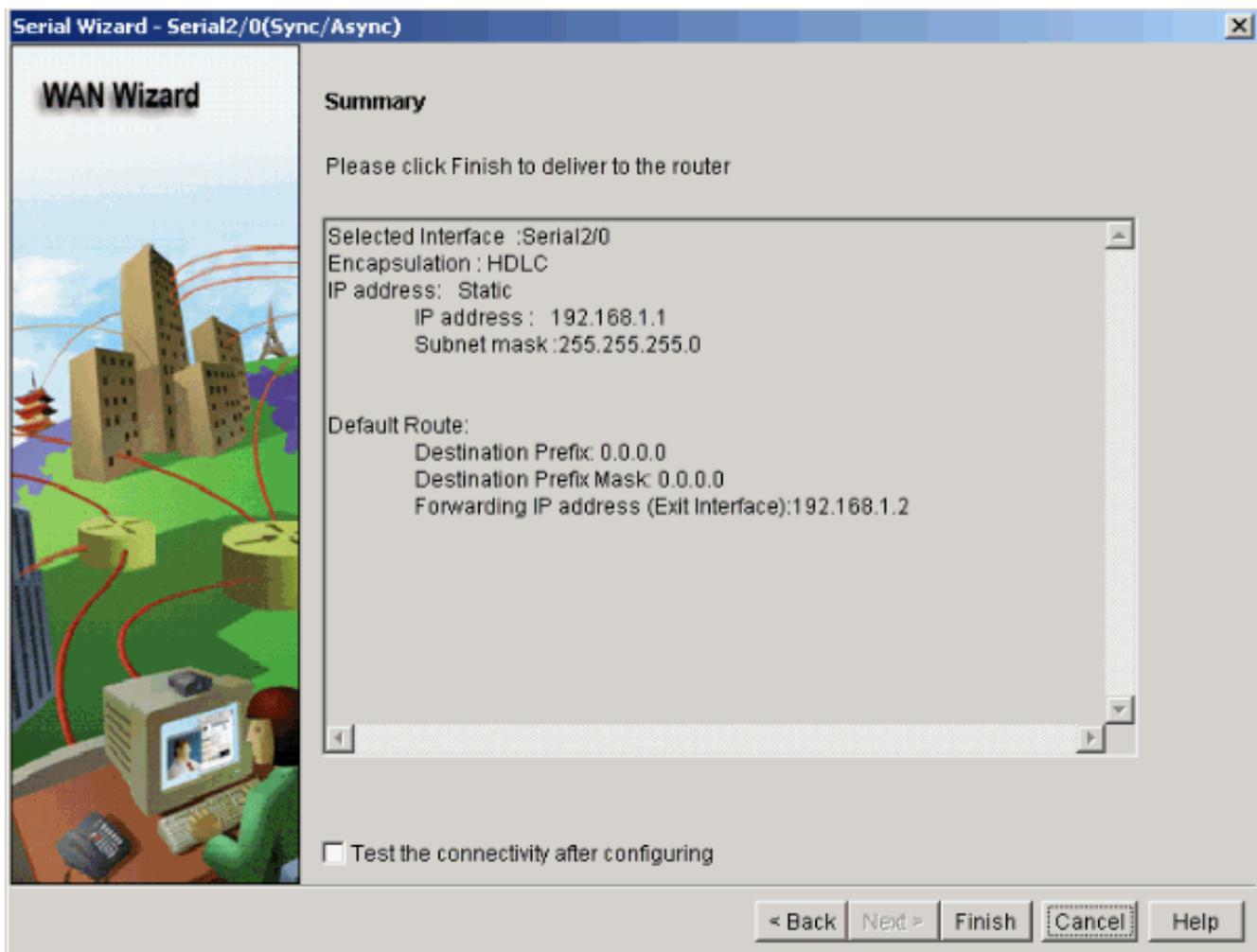
6. インターフェイスの固定 IP アドレスと対応するサブネット マスクを指定して、[Next] をクリックします。



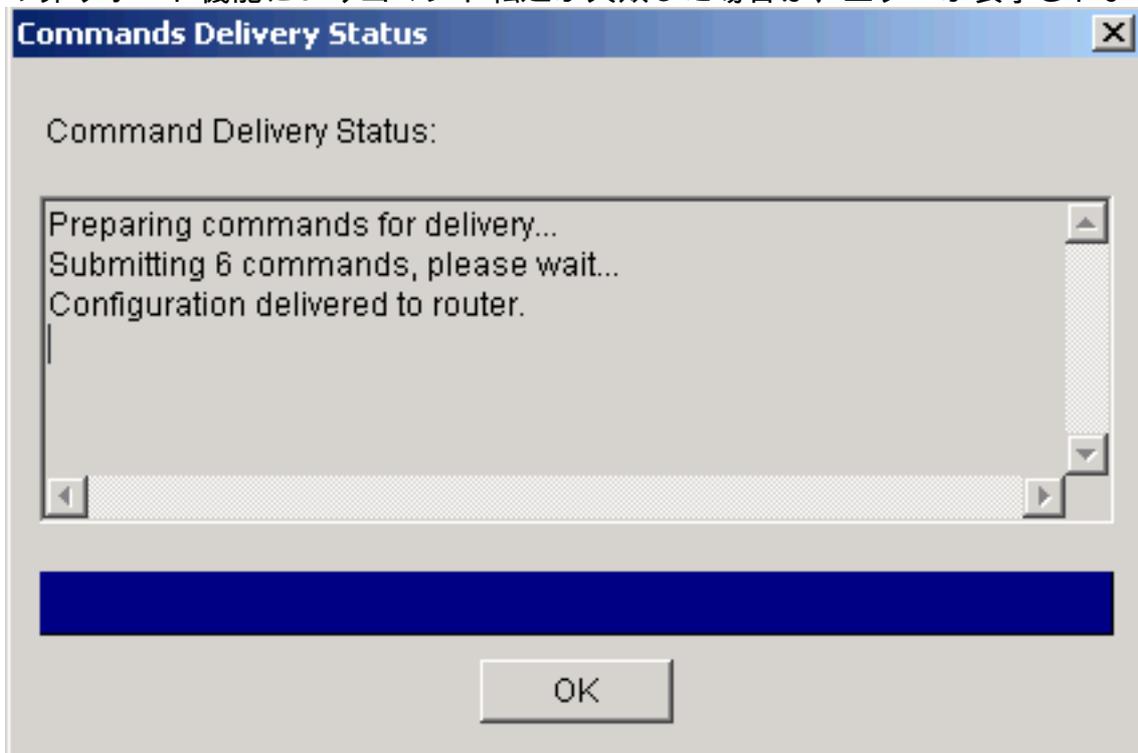
7. ISP から提供されるネクストホップ IP アドレス (ネットワーク ダイアグラムでは、192.168.1.2) などのオプション パラメータを使用してデフォルト ルーティングを設定し、[Next] をクリックします。



次のウィンドウが表示され、ユーザが行った設定の要約が表示されます。[Finish] をクリックします。



次のウィンドウが表示され、ルータへのコマンド転送状況が表示されます。非互換コマンドや非サポート機能によりコマンド転送が失敗した場合は、エラーが表示されます。



8. [Configure] > [Interfaces and Connections] > [Edit Interfaces/Connections] を選択して、さまざまなインターフェイスの追加/編集/削除を行います。

Cisco Router and Security Device Manager (SDM): 172.16.1.2

File Edit View Tools Help

Home Configure Monitor Refresh Save Search Help

Tasks

Interfaces and Connections

Create Connection Edit Interface/Connection

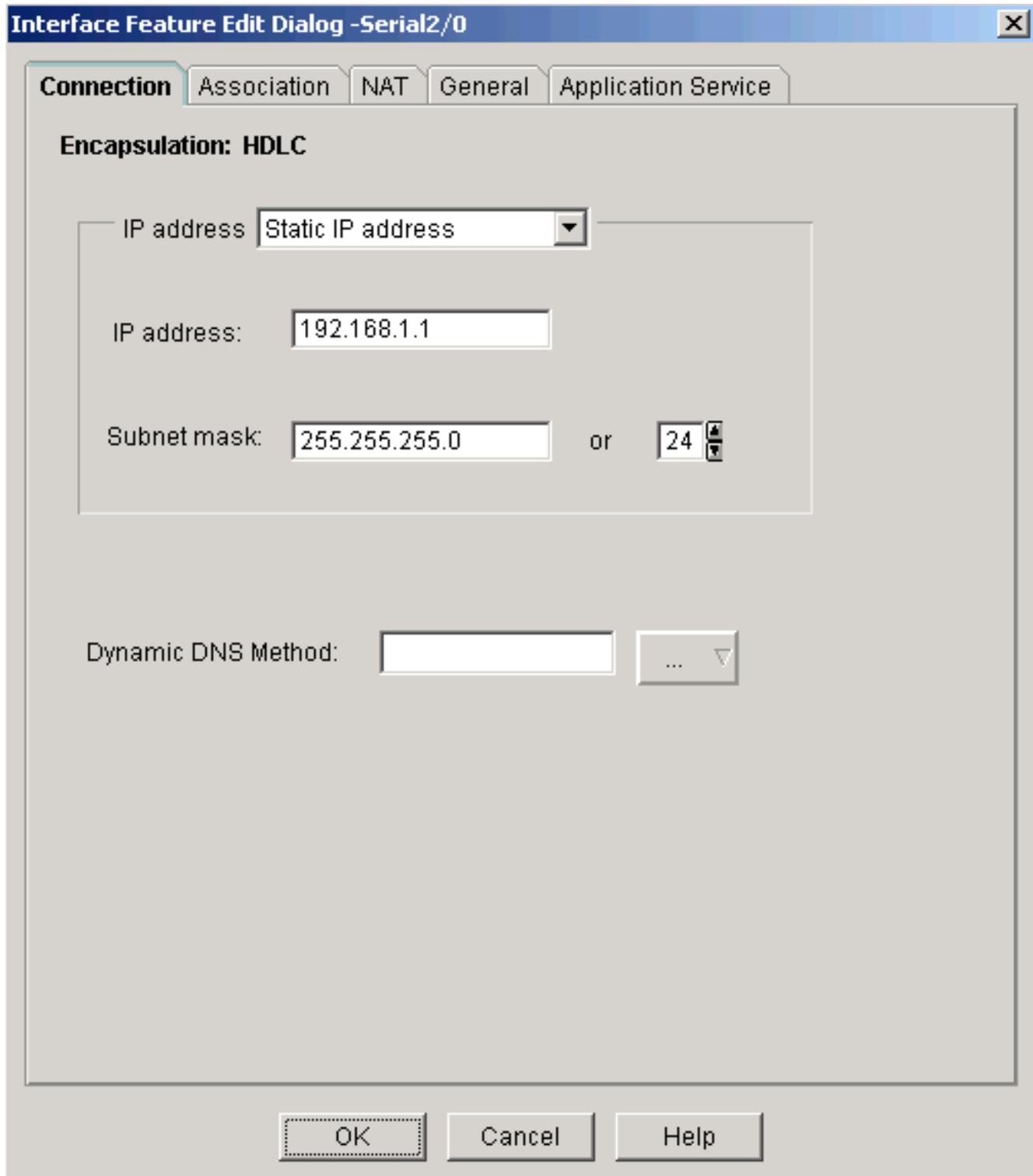
Interface List Add Edit Delete Summary Details Disable Test Connection

Interface	IP	Type	Slot	Status	Description
Ethernet0/0	no IP address	Ethernet	0	Down	
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	Down	
Serial2/2	no IP address	Serial Sync/Async	2	Down	
Serial2/3	no IP address	Serial Sync/Async	2	Down	

Details about Interface: Serial2/0 Administratively Up Administratively Down

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>

インターフェイスの設定を編集または変更するには、変更するインターフェイスを強調表示して [Edit] をクリックします。ここでは既存の固定 IP アドレスを変更できます。

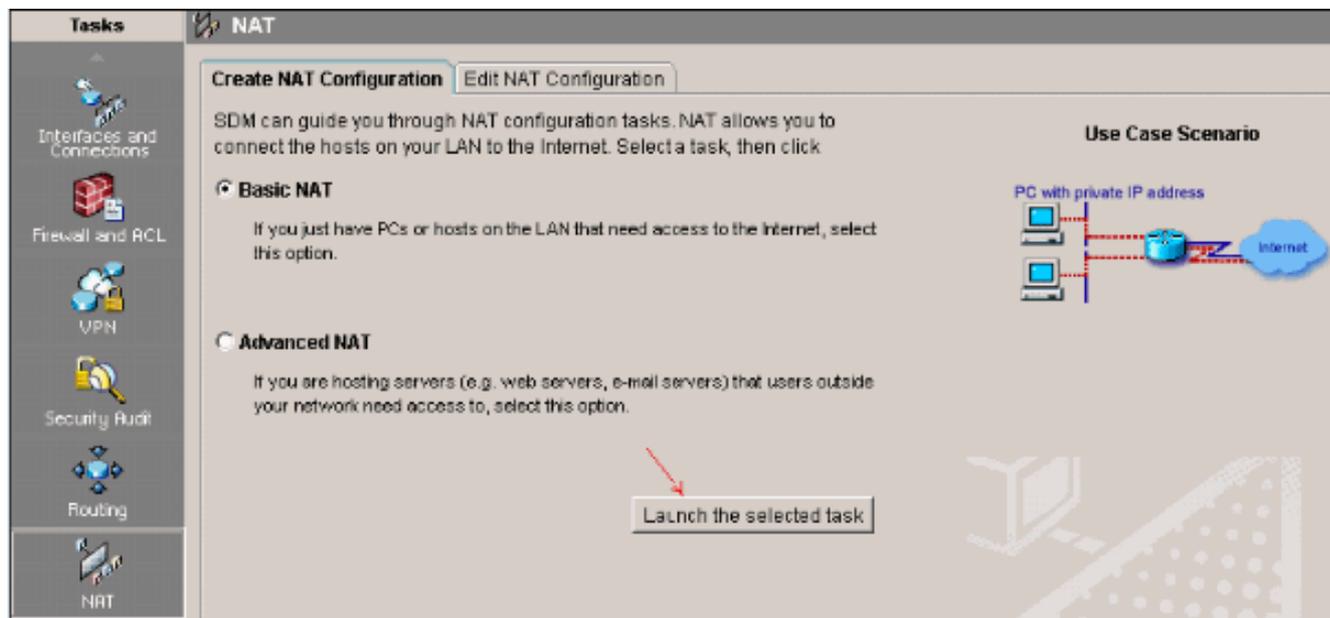


[NAT 設定](#)

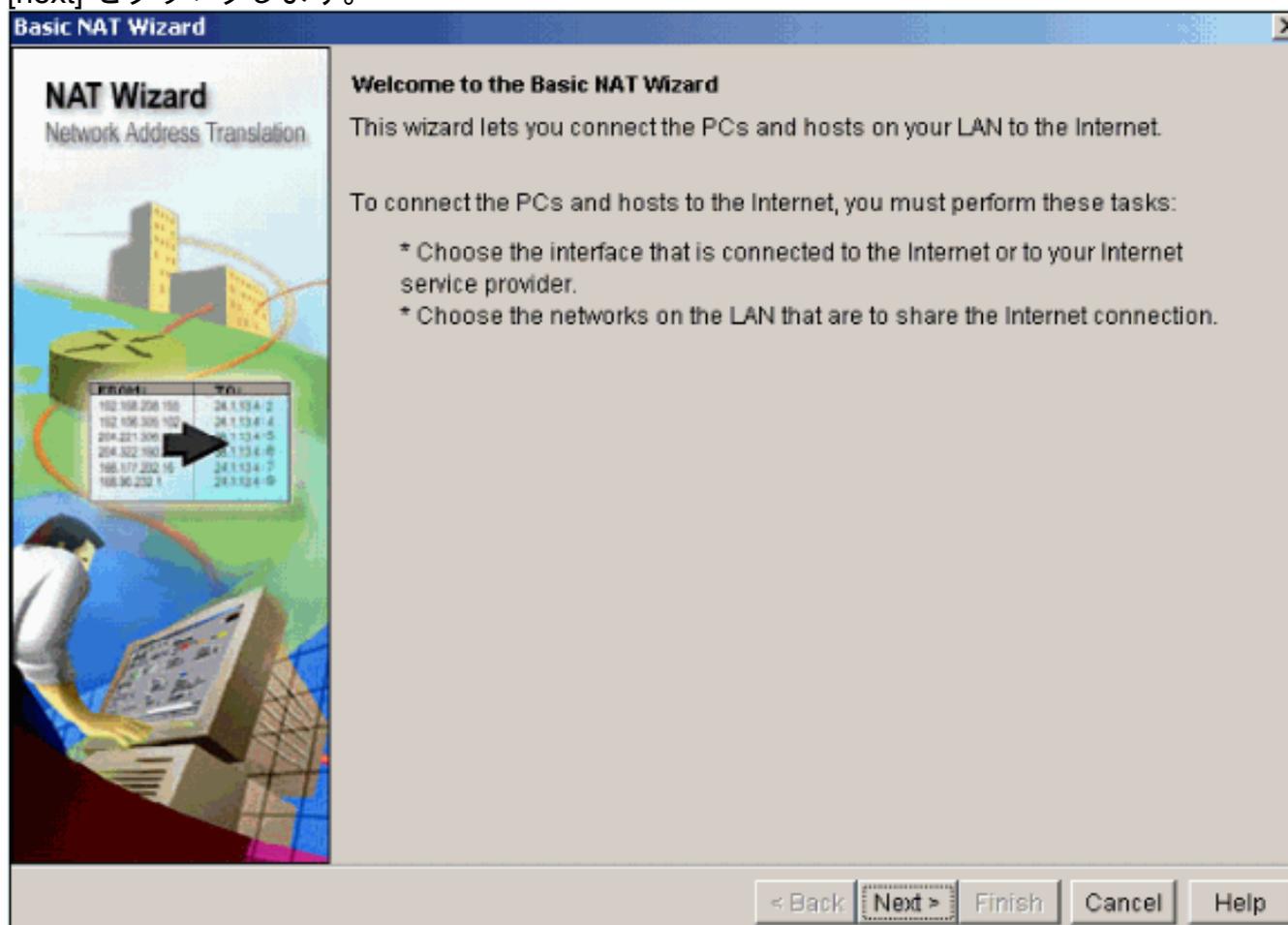
[ダイナミックNAT の設定](#)

Cisco ルータでダイナミック NAT を設定するには、次の手順を実行します。

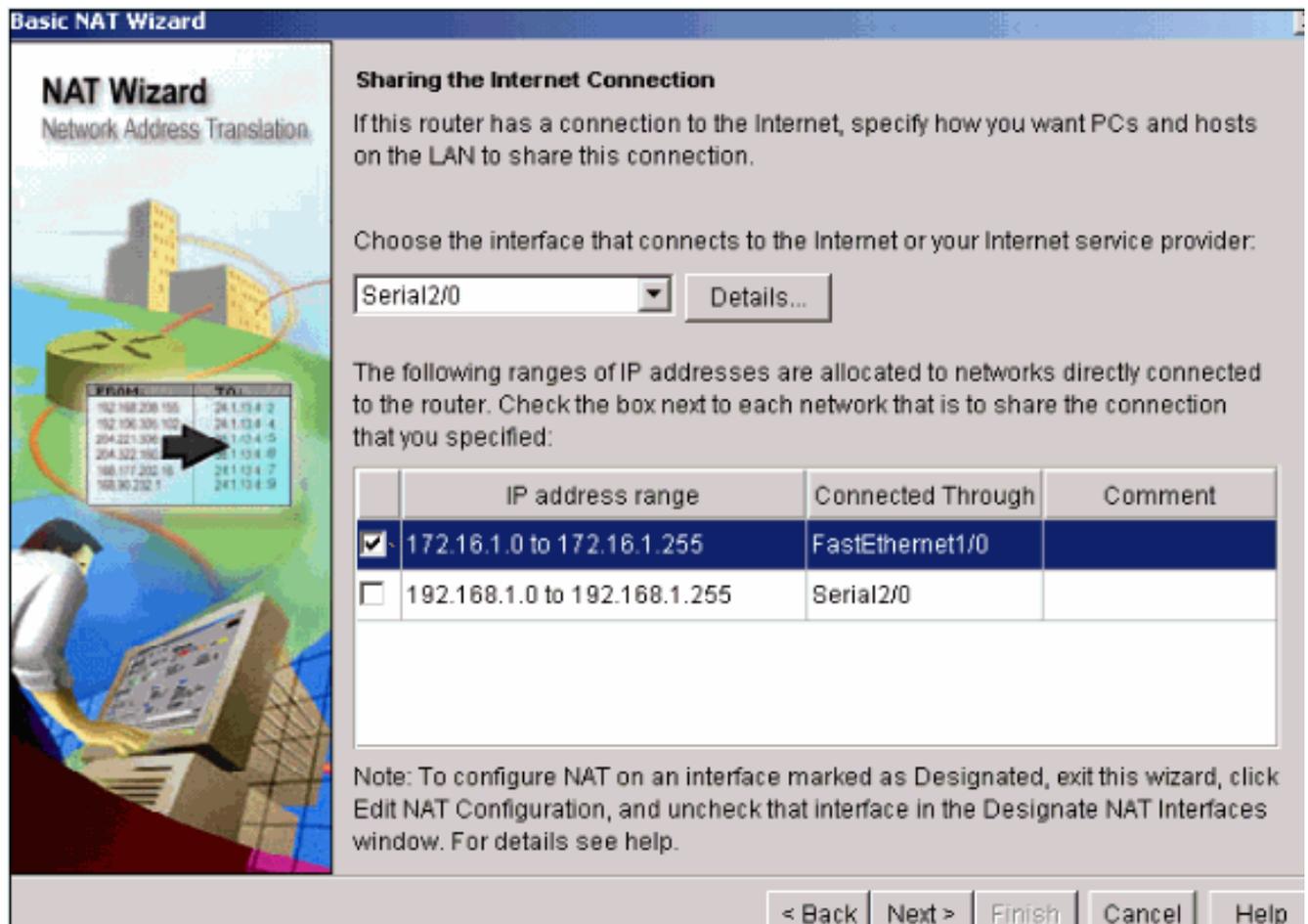
1. [Configure] > [NAT] > [Basic NAT] を選択し、[Launch the selected task] をクリックして、基本的な NAT を設定します。



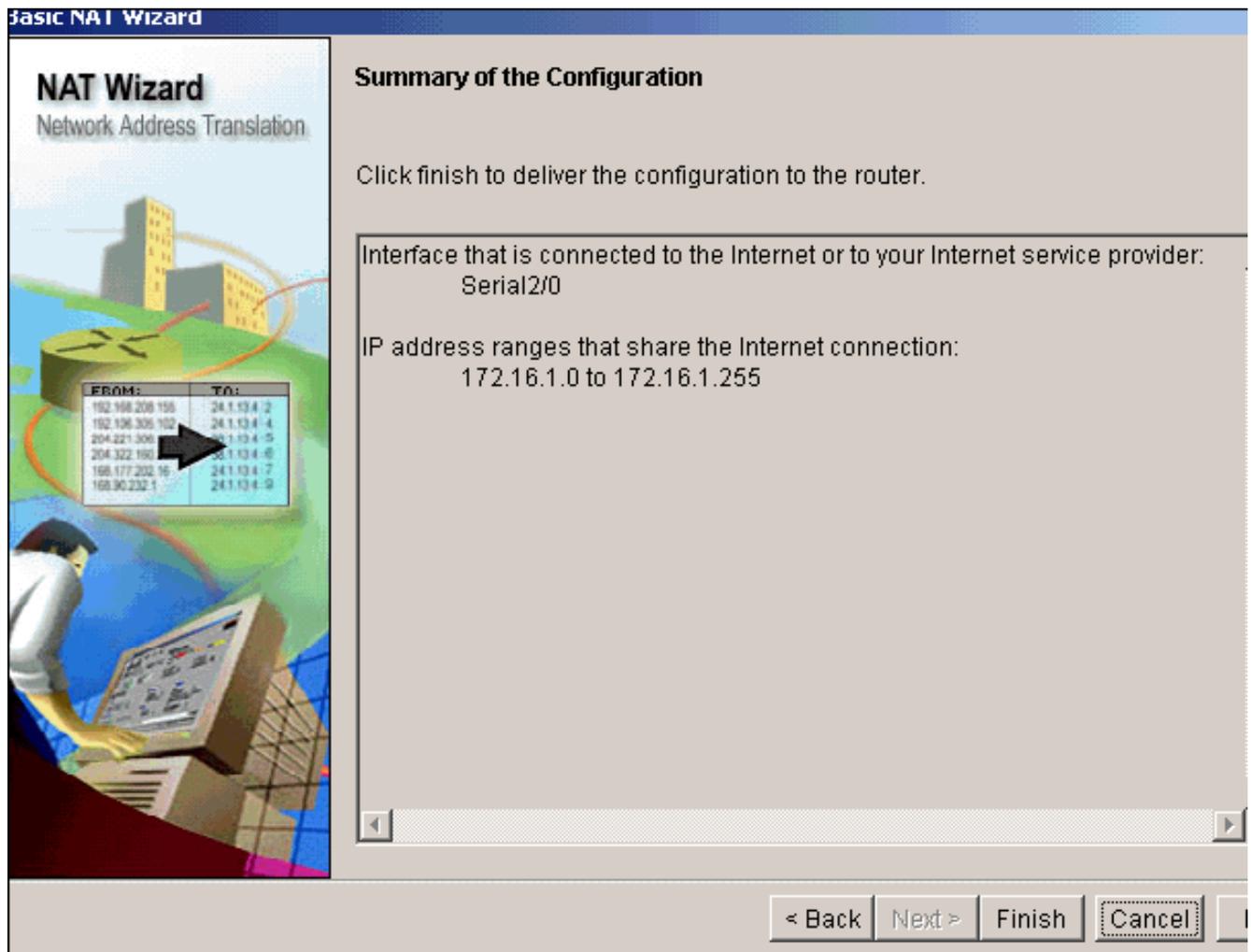
2. [next] をクリックします。



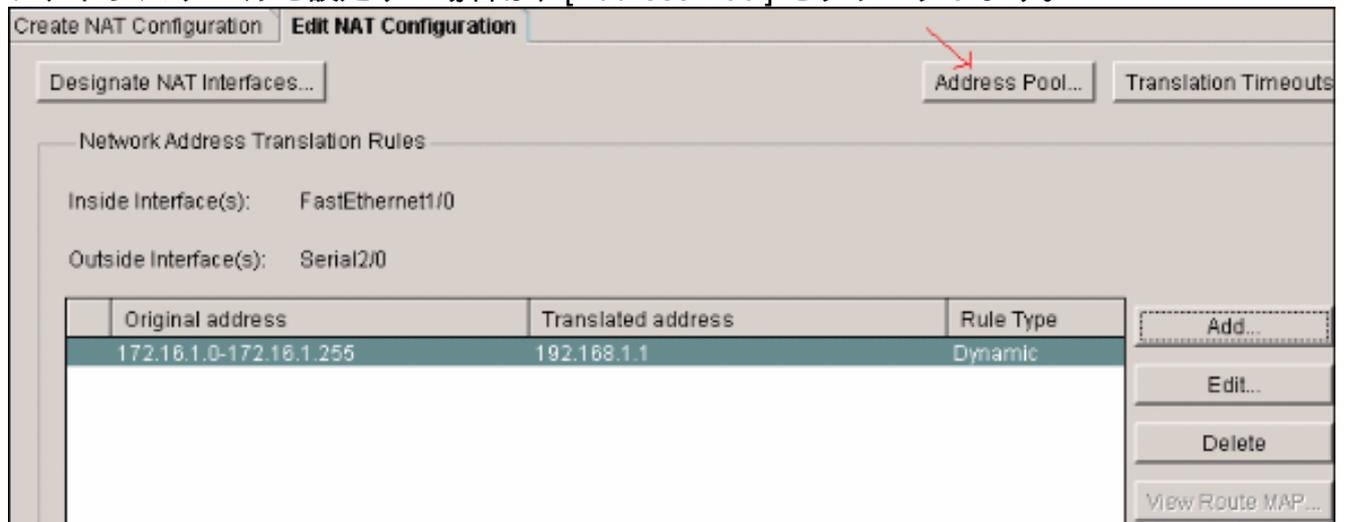
3. インターネットまたは ISP に接続するインターフェイスを選択し、インターネット アクセスで共有する IP アドレス範囲を選択します。



4. 次のウィンドウが表示され、ユーザが行った設定の要約が表示されます。[Finish] をクリックします。



5. Edit NAT Configuration ウィンドウが表示され、設定されたダイナミック NAT 設定と、オーバーロード変換 (PAT) された変換後の IP アドレスが表示されます。ダイナミック NAT にアドレスプールを設定する場合は、[Address Pool] をクリックします。



6. [Add] をクリックします。

Address Pools [X]

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

Pool Name	Address

Clone selected Entry on Add

ここでは

、プール名、IP アドレス範囲、ネットマスクなどの情報を指定します。プール内のほとんどのアドレスが割り当てられ、IP アドレスプールをほぼ使い果たしてしまうことがあります。このような場合には、PAT を使用して1つの IP アドレスで複数の IP アドレス要求に対応することができます。アドレスプールが枯渇しそうになったときにルータで PAT が使用されるようにするには、[Port Address Translation (PAT)] にチェックマークを入れます。

Add Address Pool [X]

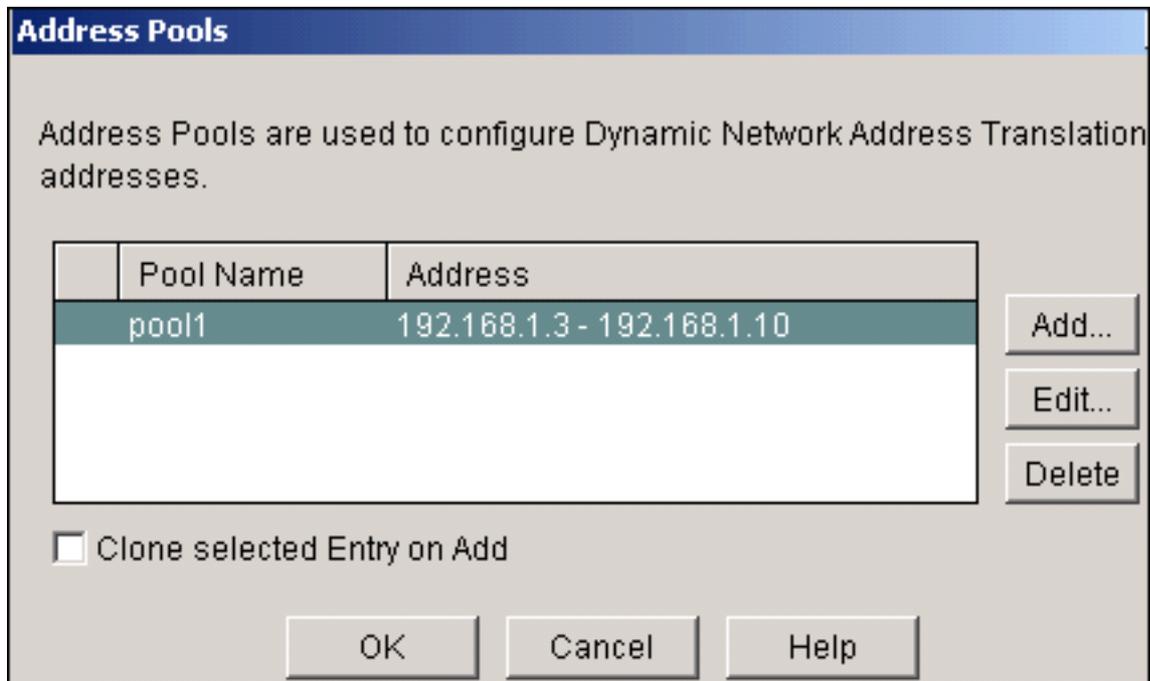
Pool Name:

Port Address Translation(PAT)

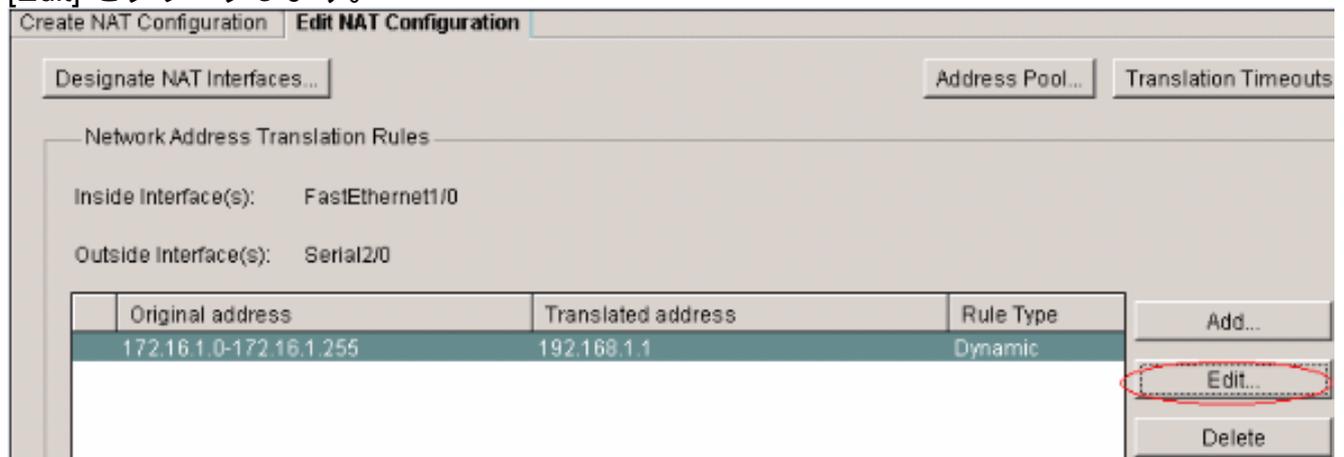
IP address: --

Network Mask: or

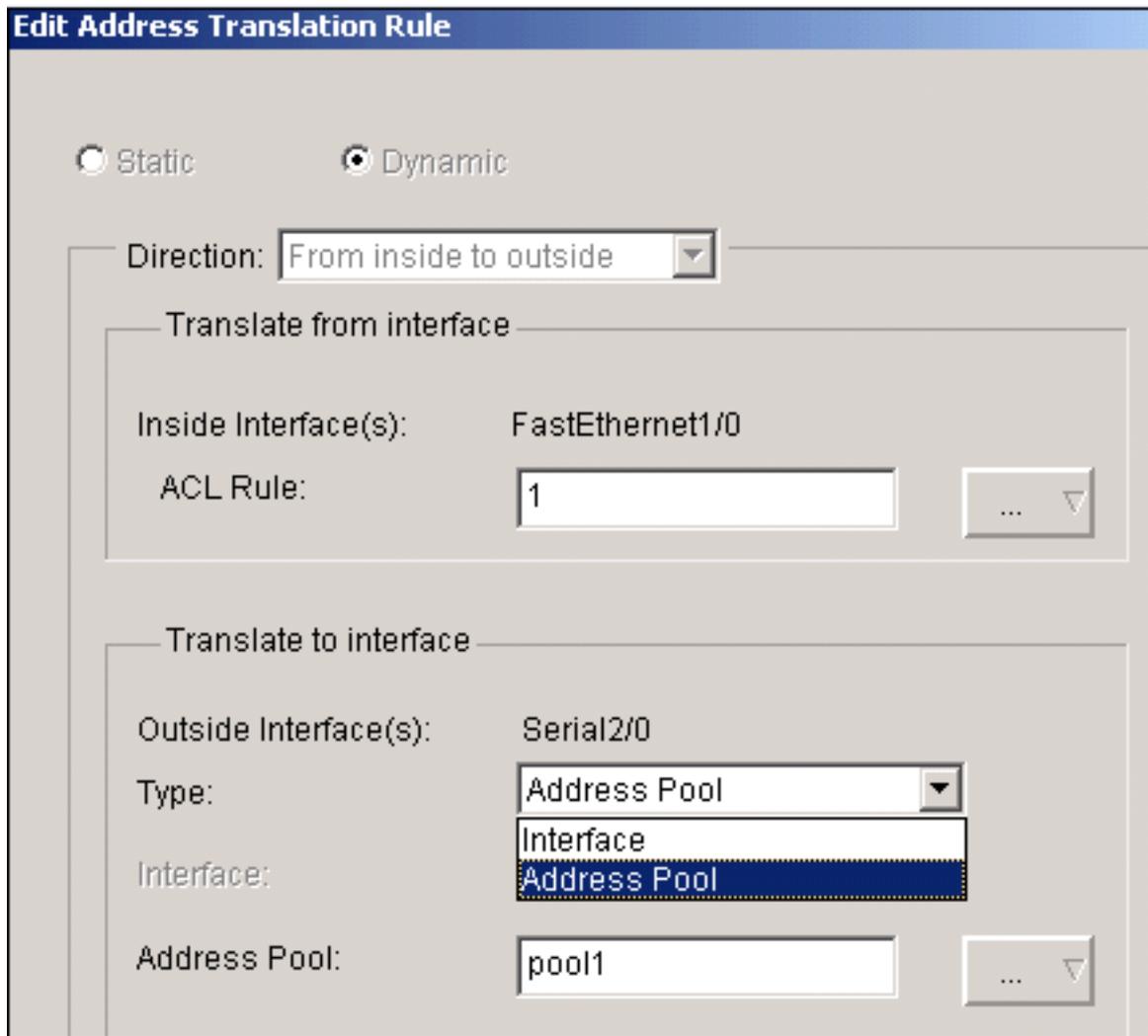
7. [Add] をクリックします。



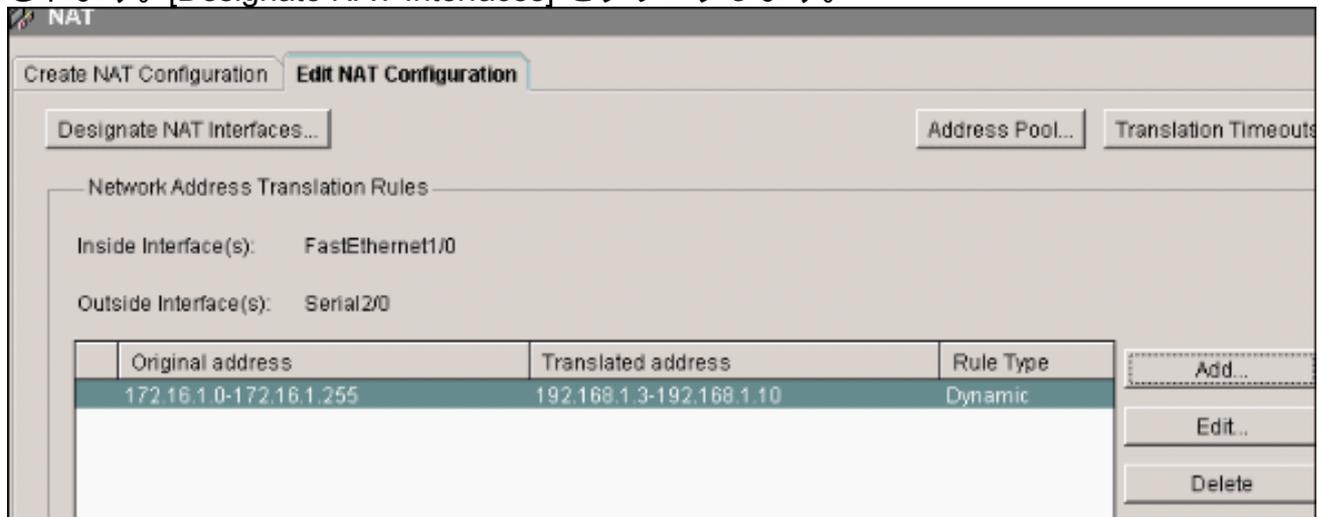
8. [Edit] をクリックします。



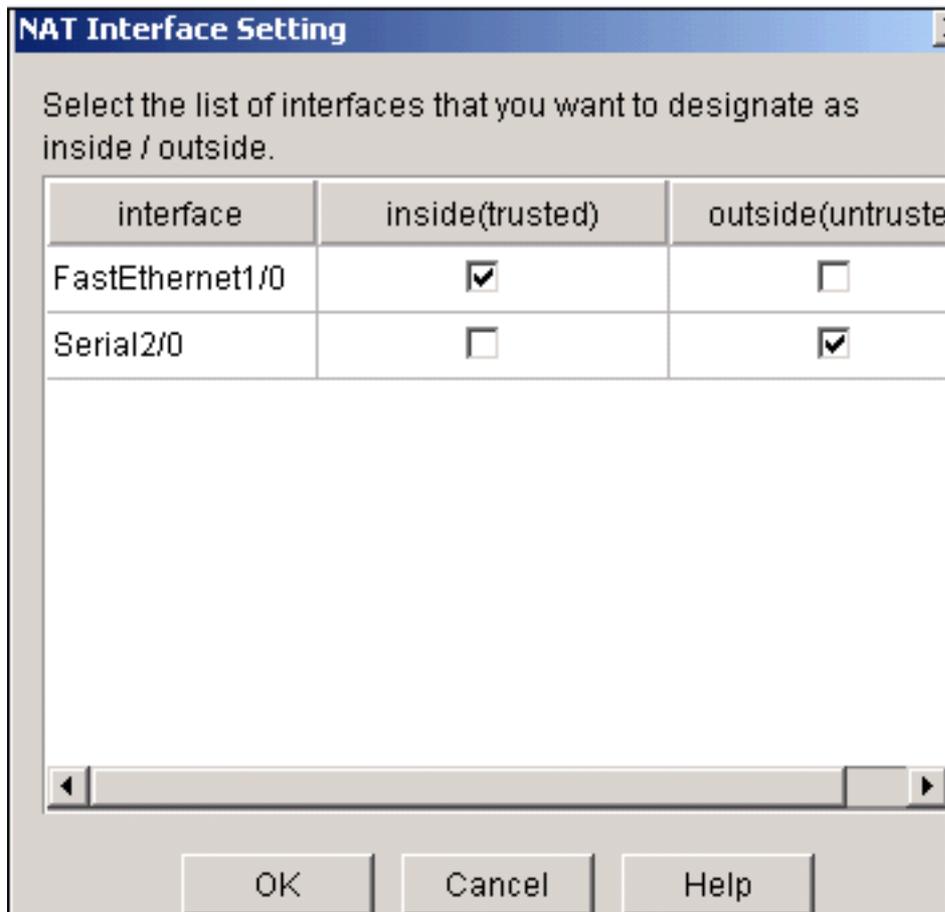
9. [Type] フィールドで [Address Pool] を選択し、[Address Pool] に pool1 という名前を入力して [OK] をクリックします。



10. 次のウィンドウが表示され、アドレスプールを使用したダイナミック NAT の設定が表示されます。[Designate NAT Interfaces] をクリックします。



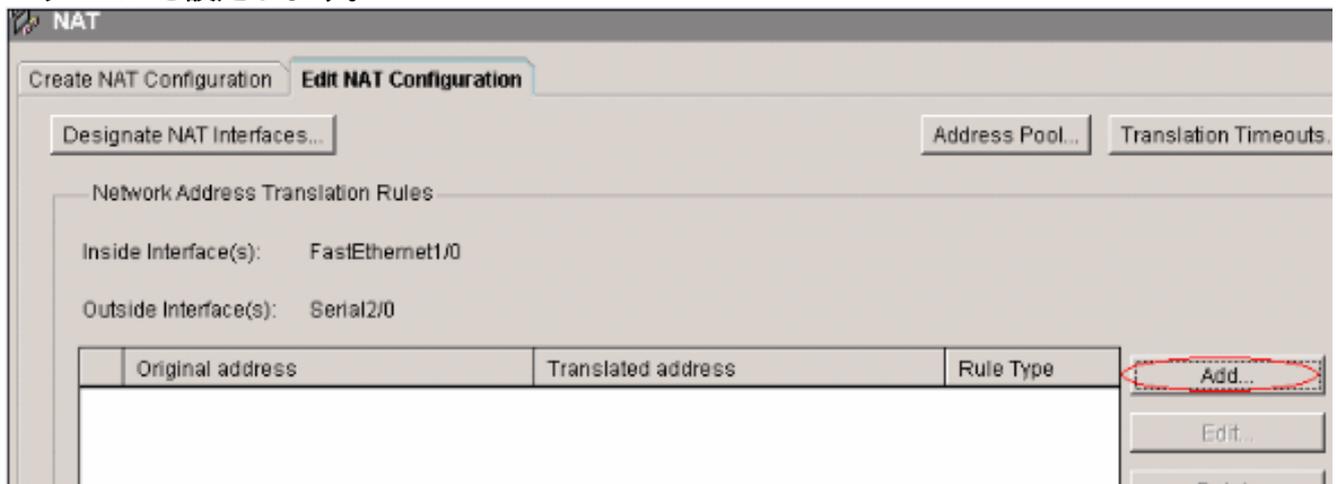
次のウィンドウを使用して、NAT 変換で使用する内部インターフェイスと外部インターフェイスを指定します。NAT では変換ルールを解釈する際に、内部と外部の指定を参照します。これは、変換が内部から外部、外部から内部の両方向で行われるためです。指定すると、すべての NAT 変換ルールでこれらのインターフェイスが使用されます。指定したインターフェイスは、メインの NAT ウィンドウの変換ルール リストの上部に表示されます。



スタティック NAT の設定

Cisco ルータでスタティック NAT を設定するには、次の手順を実行します。

1. [Configure] > [NAT] > [Edit NAT Configuration] を選択し、[Add] をクリックして、スタティック NAT を設定します。



2. [Direction] で、[From inside to outside] または [From outside to inside] を選択し、[Translate from Interface] で変換する内部 IP アドレスを指定します。[Translate to Interface] エリアで、タイプを選択します。変換元のアドレスを [IP Address] フィールドで指定した IP アドレスに変換する場合は、[IP Address] を選択します。変換元のアドレスで、ルータのインターフェイスのアドレスが使用されるようにするには、[Interface] を選択します。変換元のアドレスが、[Interface] フィールドで指定したインターフェイスに割り当てられている IP アドレスに変換されます。変換に内部デバイスのポート情報を含めるには、[Redirect Port] にチェックマークを入れます。これにより、各デバイスに指定されたポートが同一でない限り、複

数のデバイスで1つのパブリック IP アドレスを使用できるようになります。この変換先アドレスの各ポート マッピングについて、エントリを作成する必要があります。TCP ポート番号の場合は [TCP]、UDP ポート番号の場合は [UDP] をクリックします。Original Port フィールドに、内部デバイスのポート番号を入力します。Translated Port フィールドに、ルータがこの変換で使用するポート番号を入力します。「[インターネットから内部デバイスにアクセスできるようにする場合](#)」セクション (『[ネットワーク アドレス変換の設定 : スタートアップ ガイド](#)』を参照してください)。

Add Address Translation Rule

Static Dynamic

Direction: **From inside to outside**

Translate from interface

Inside Interface(s):

IP address:

Network Mask(optional): or

Translate to interface

Outside Interface(s):

Type:

Interface:

IP address:

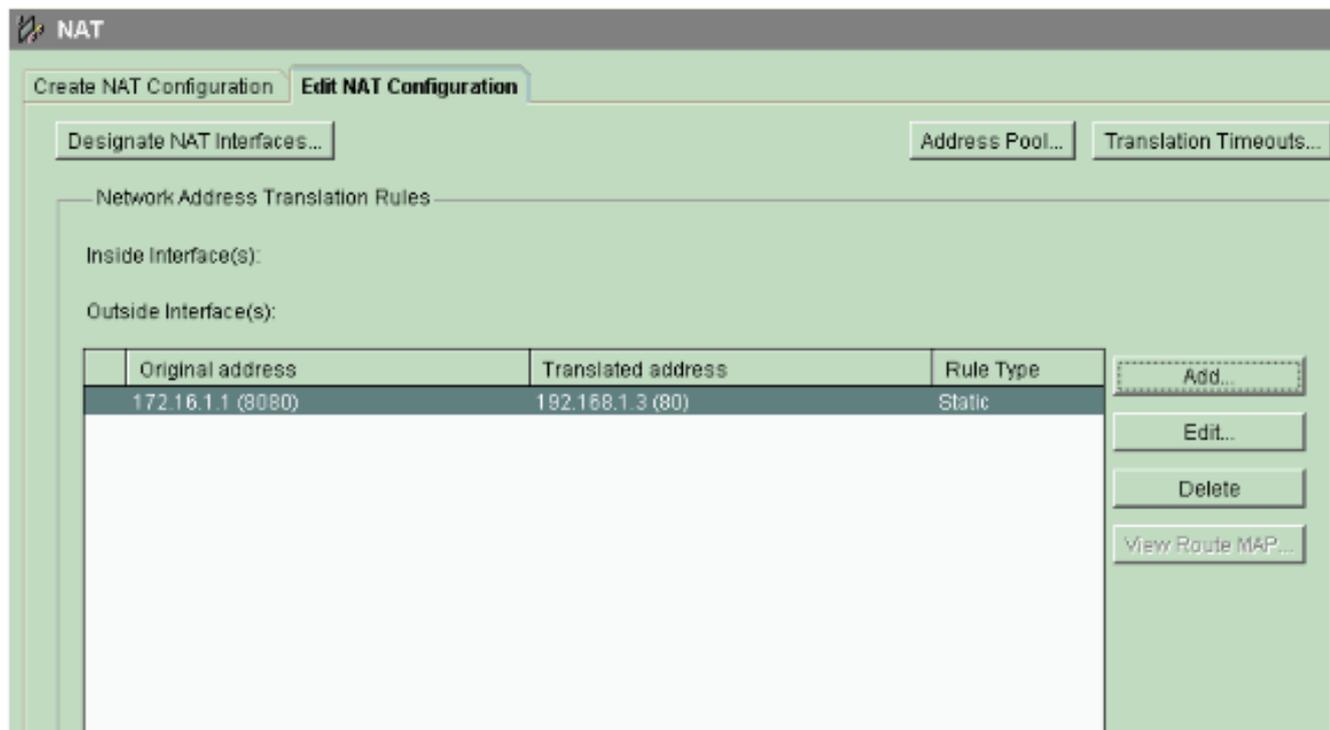
Redirect Port

TCP UDP

Original Port: Translated Port:

OK Cancel Help

次のウインドウに、ポート リダイレクトをイネーブルにしたスタティック NAT の設定が表示されます。

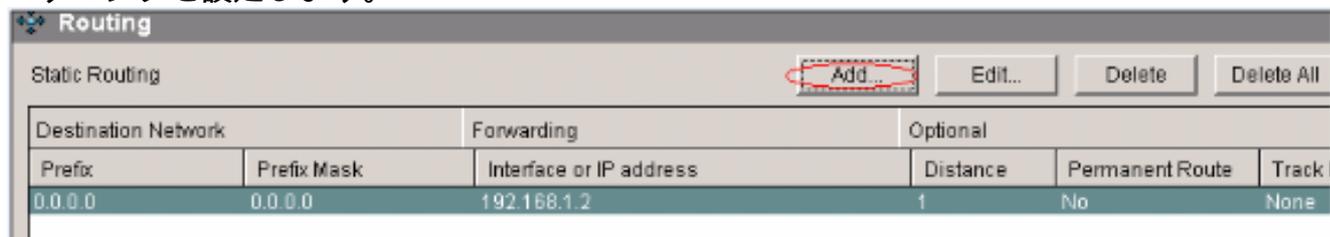


[ルーティング設定](#)

[スタティック ルーティングの設定](#)

Cisco ルータでスタティック ルーティングを設定するには、次の手順を実行します。

1. [Configure] > [Routing] > [Static Routing] を選択し、[Add] をクリックして、スタティック ルーティングを設定します。



2. 宛先ネットワークアドレスとマスクを入力し、発信インターフェイスまたはネクストホップ IP アドレスのいずれかを選択します。

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

次のウィンドウに、

10.1.1.0 ネットワークへのスタティックルートが表示されています。ネクストホップ IP アドレスは 192.168.1.2 です。

Routing

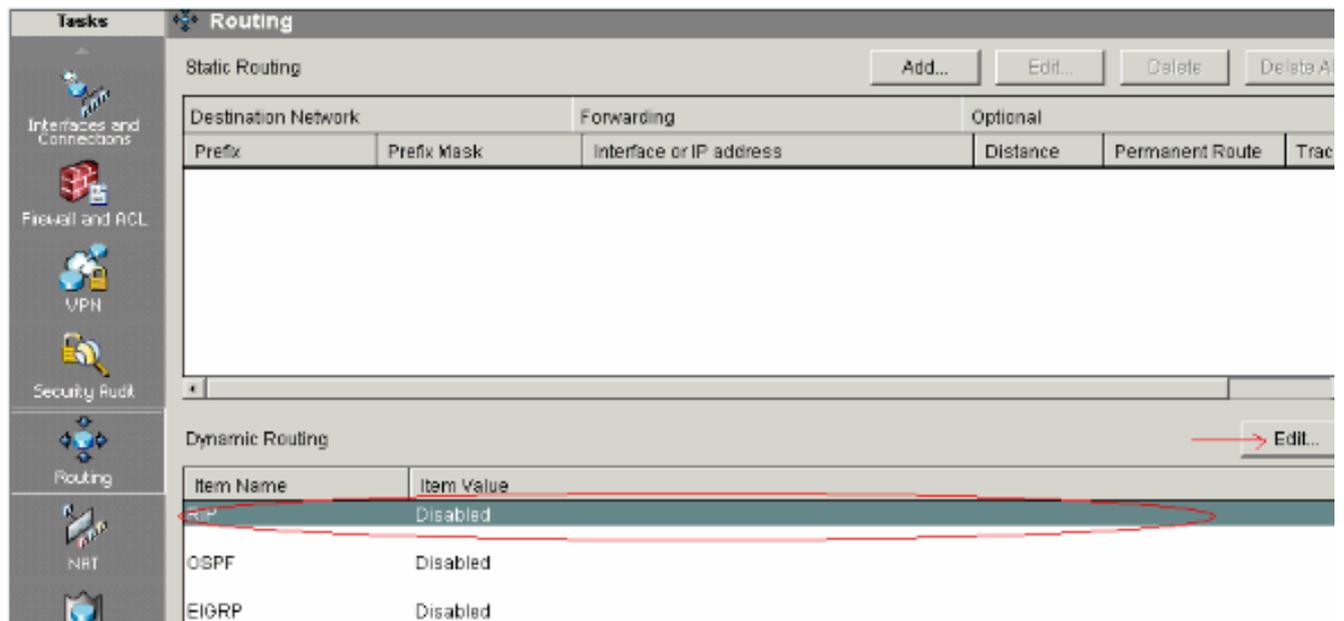
Static Routing

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

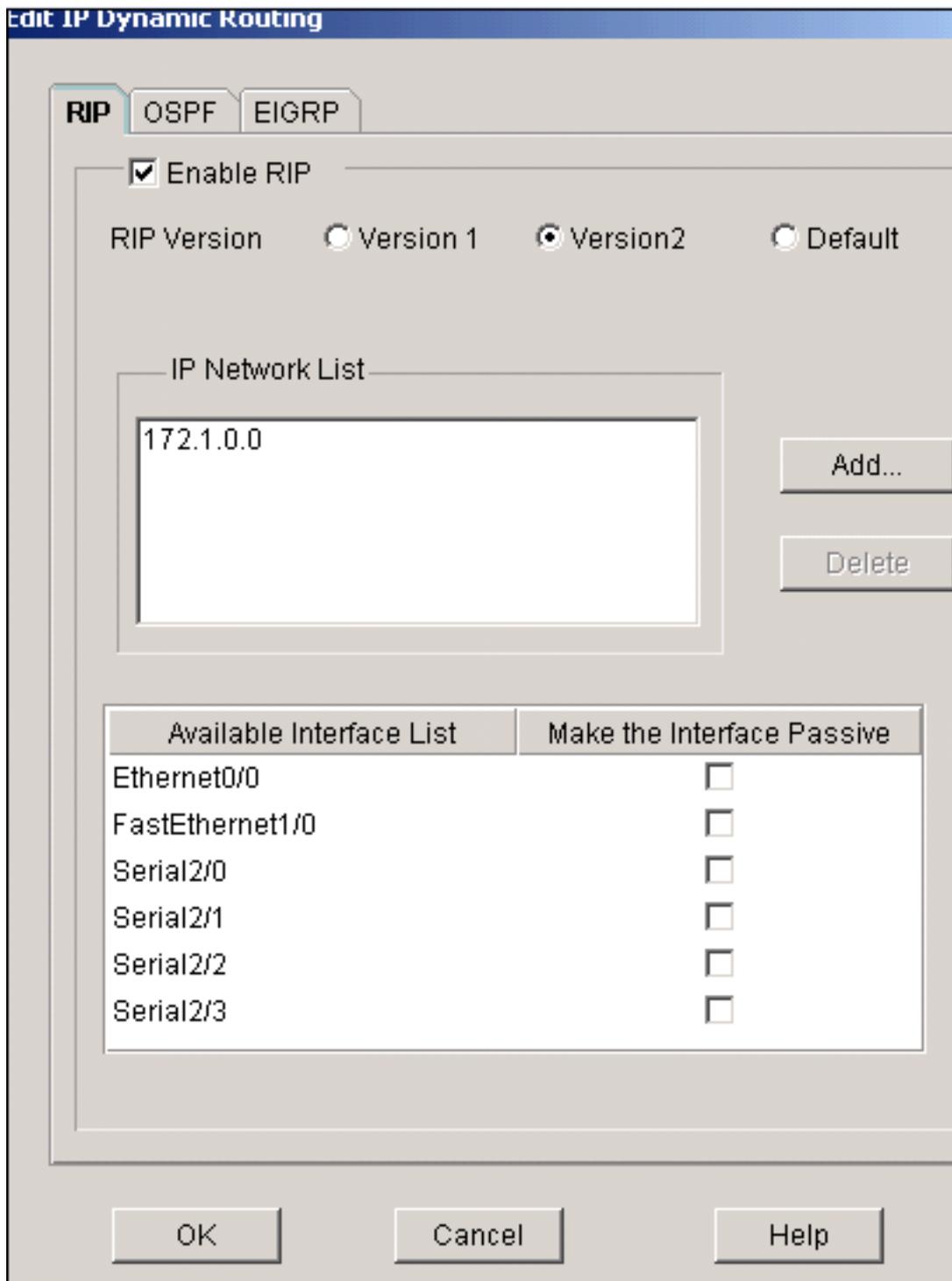
ダイナミックルーティングの設定

Cisco ルータでダイナミックルーティングを設定するには、次の手順を実行します。

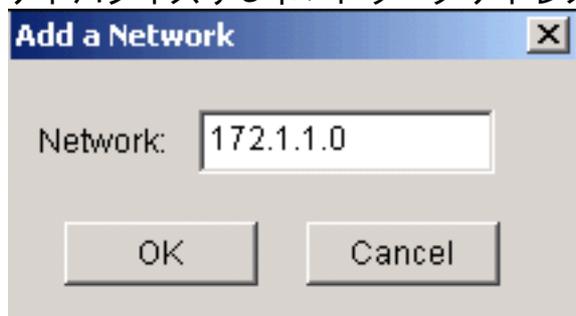
1. [Configure] > [Routing] > [Dynamic Routing] を選択します。
2. [RIP] を選択し、[Edit] をクリックします。



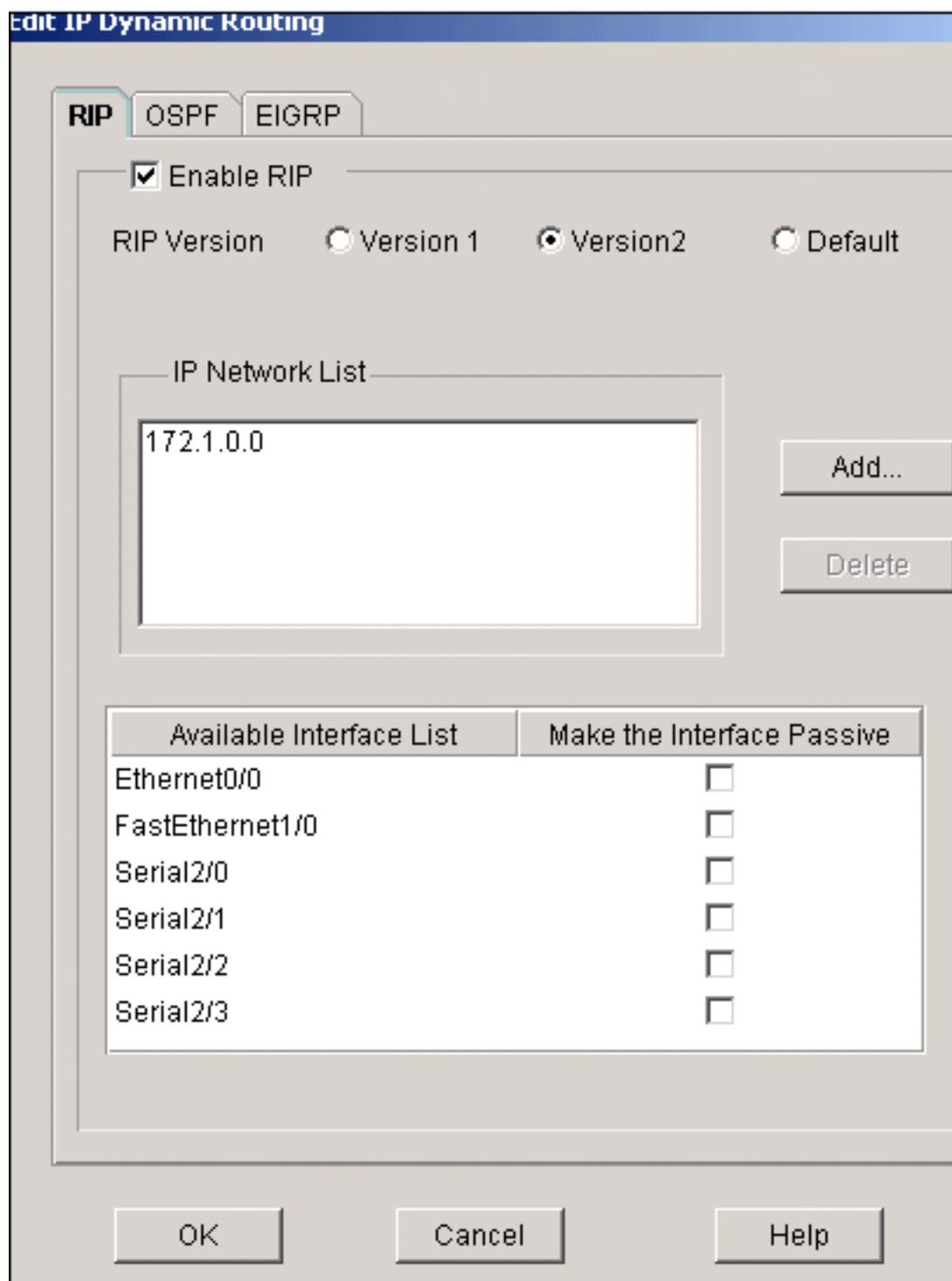
3. [Enable RIP] にチェックマークを付け RIP のバージョンを選択し、[Add] をクリックします



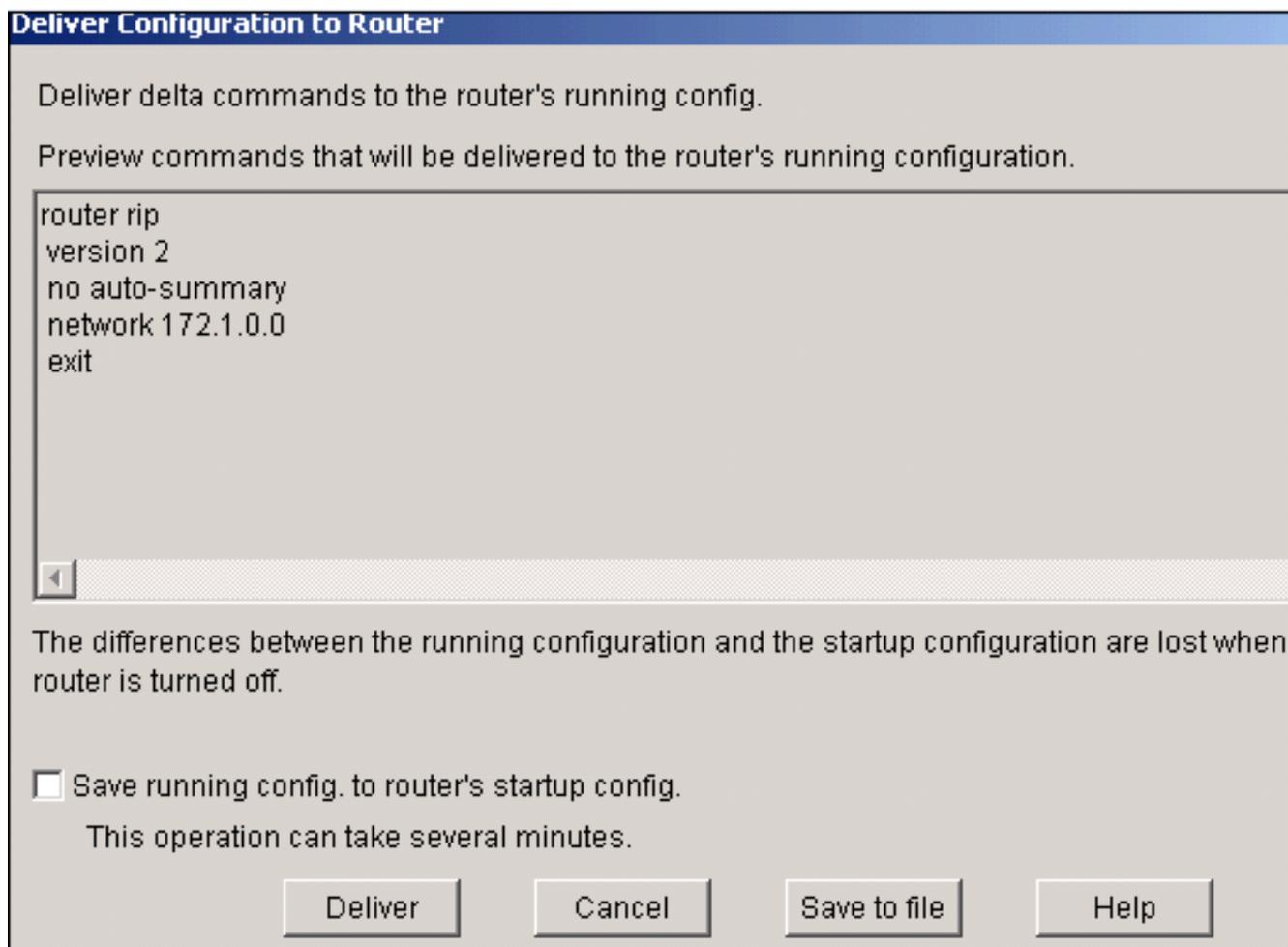
4. アドバタイズするネットワークアドレスを指定します。



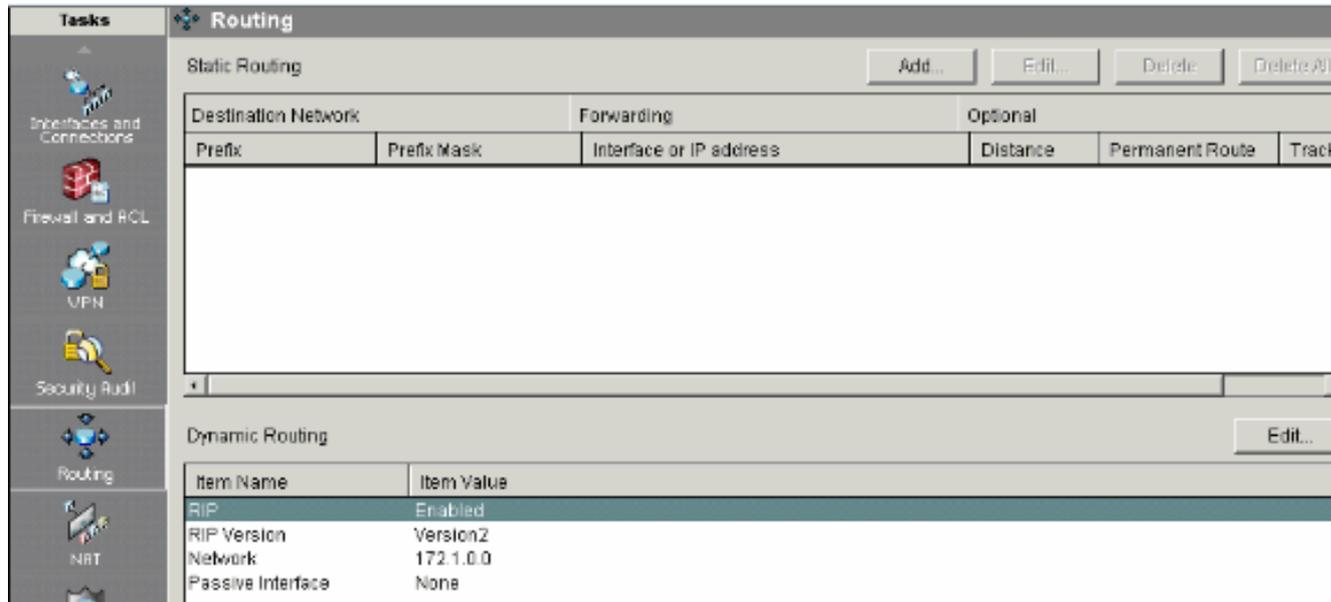
5. [OK] をクリックします。



6. [Deliver] をクリックして、コマンドをルータに転送します。



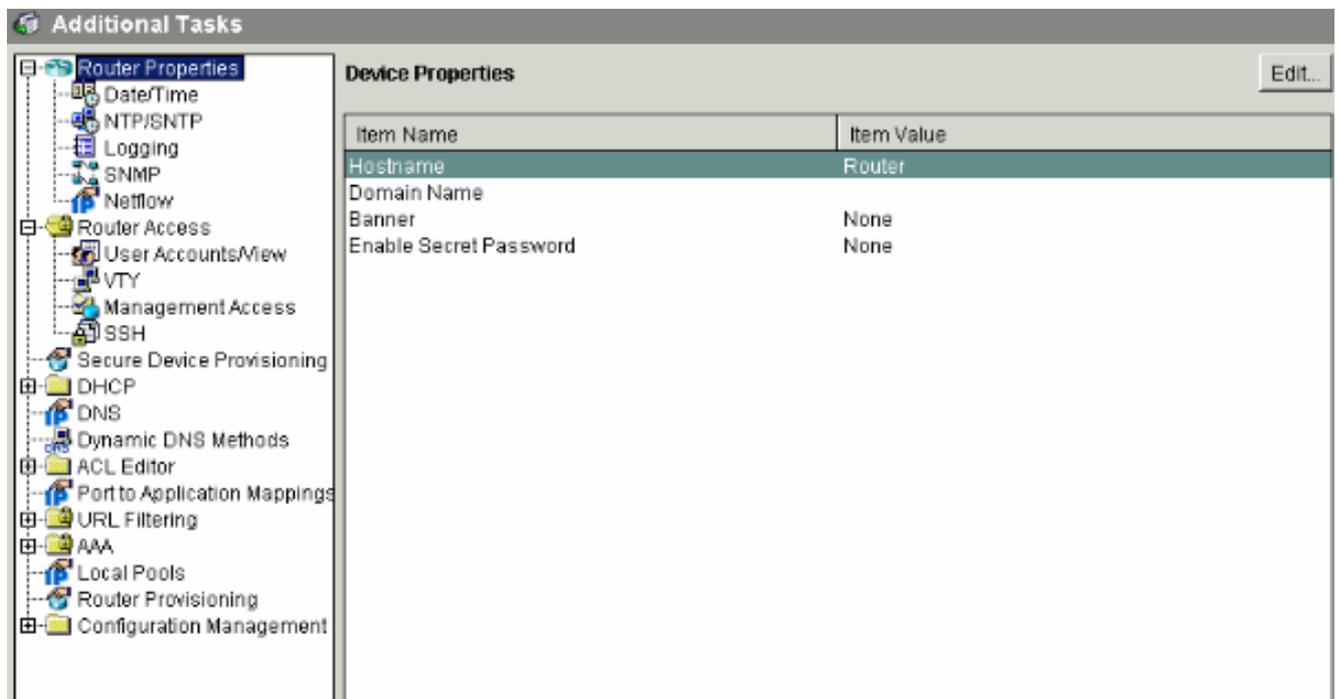
次のウィンドウに、ダイナミック RIP ルーティングの設定が表示されます。



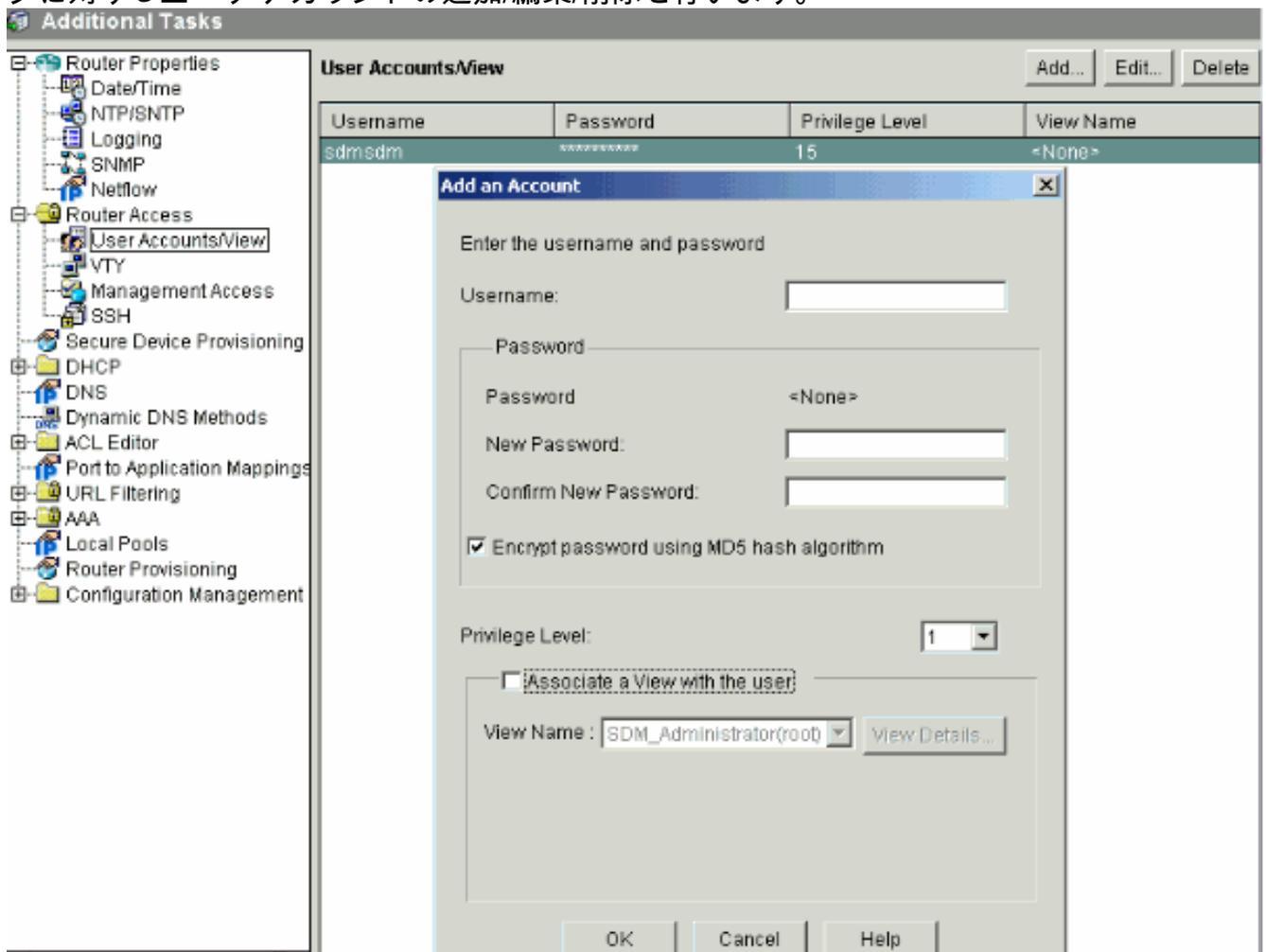
その他の設定

Cisco ルータでその他の基本的な設定を行うには、次の手順を実行します。

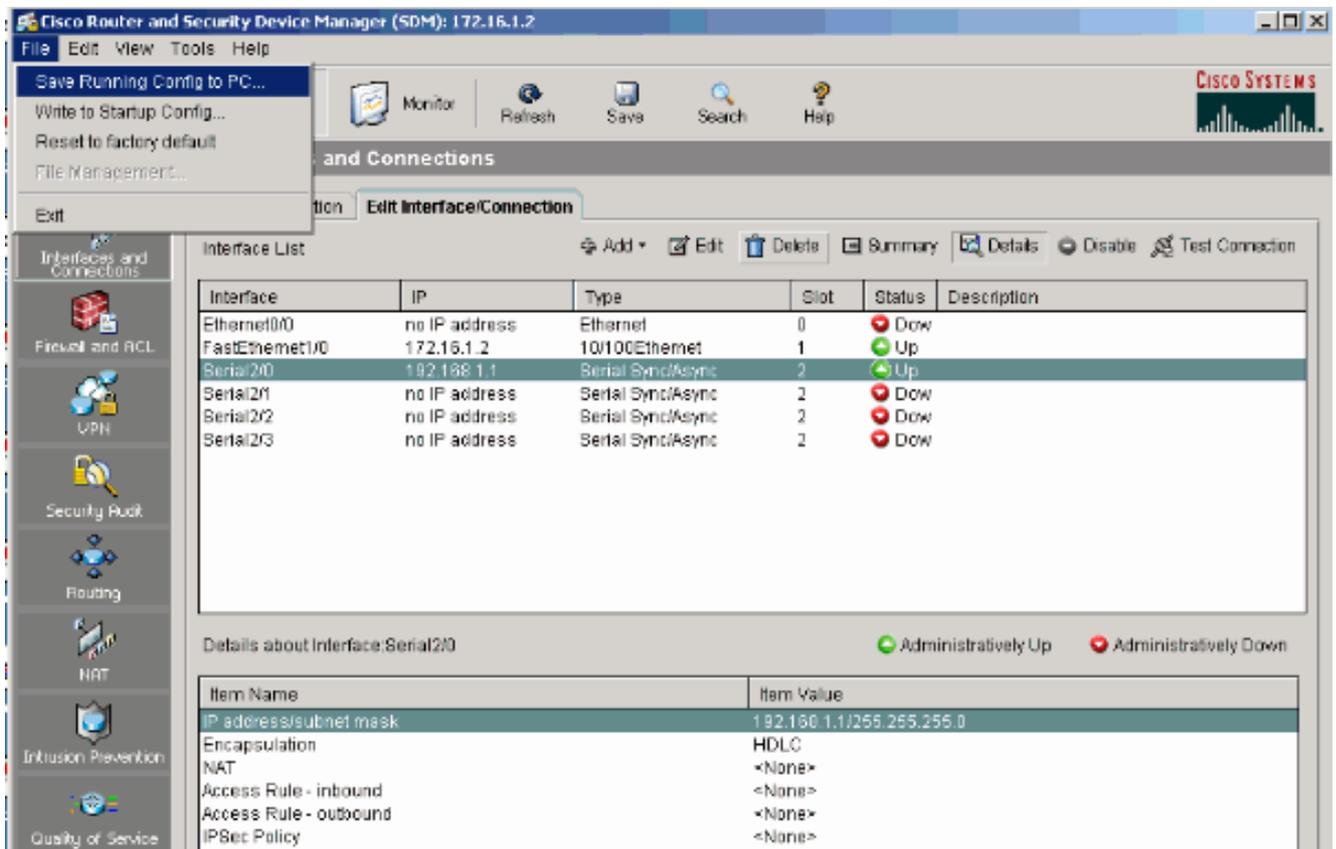
1. ルータのホスト名、ドメイン名、バナー、およびイネーブル シークレット パスワードのプロパティを変更する場合は、[Configure] > [Additional Tasks] > [Router Properties] を選択して、[Edit] をクリックします。



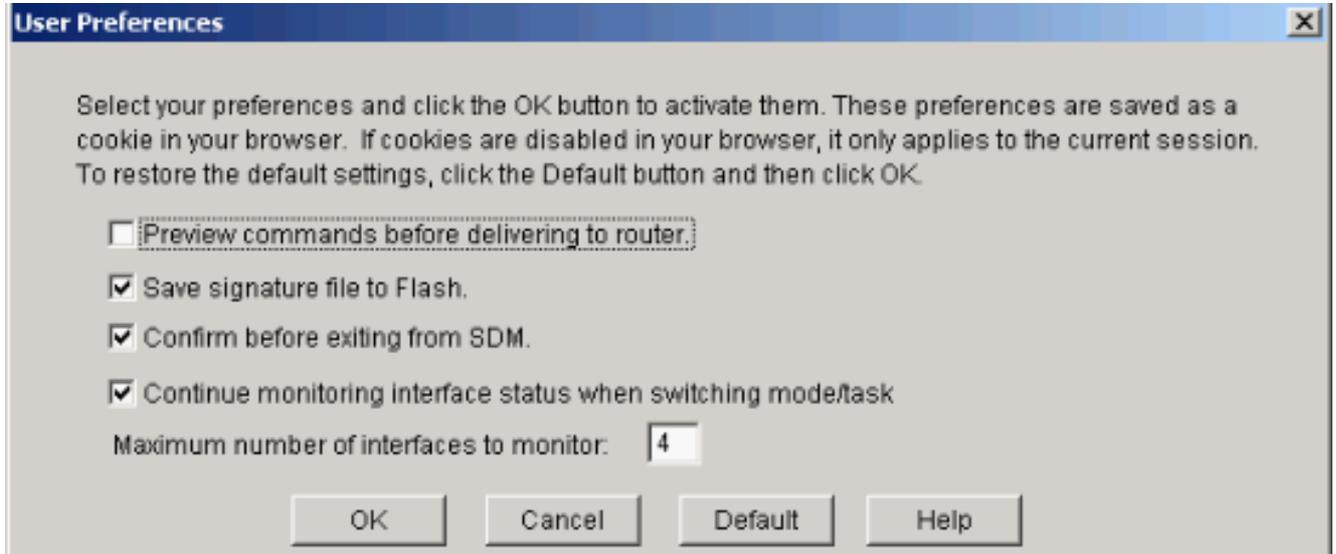
2. [Configure] > [Additional Tasks] > [Router Access] > [User Accounts/View] を選択して、ルータに対するユーザアカウントの追加/編集/削除を行います。



3. [File] > [Save Running Config to PC...] を選択して、設定内容をルータの NVRAM および PC に保存し、現在の設定をデフォルト (工場出荷時) 設定にリセットします。



4. タスク バーに移動し、[Edit] > [Preferences] を選択して、次のユーザ設定オプションを有効にします。ルータへの転送前にコマンドをプレビューする。シグニチャ ファイルをフラッシュに保存する。SDM を終了する前に確認する。モード/タスクの切り替え時に、インターフェイスのステータスのモニタリングを継続する。



5. 次の操作を行う場合は、タスク バーから [View] を選択します。Home、Configure、または Monitor ページを表示する。ルータの実行コンフィギュレーションを表示する。さまざまな show コマンドを表示する。SDM のデフォルトの規則を表示する。CLI で設定されたルータ設定がある場合に、[Refresh] を選択して、ルータの設定を SDM に同期させる。

The screenshot shows the Cisco Router and Security Device Manager (SDM) interface. The main window displays a table of network connections. The 'Serial2/0' interface is highlighted, and its details are shown in a separate pane below.

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

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>
...	...

CLI での設定

ルータの設定

```

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 !----

```



```

!
!
!
!
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

```

確認

[Configure] > [Interface] & [Connections] > [Edit Interface Connections] > [Test Connection] の順に選択して、エンドツーエンド接続をテストします。リモート エンドの IP アドレスを指定するには、[User-specified] オプション ボタンをクリックします。

Connectivity testing and troubleshooting : Serial2/0

IP address / hostname

Select a ping option, enter the required value and click Start

Automatically determined by SDM User-specified

Summary Details

Activity	Information	us
Checking inter	 <p>Test Connection successful!</p> <p>The connection is up on the selected interface.</p> <p>OK</p>	
Checking inter		p
Checking exit i		uccessful
Pinging to dest		uccessful

Failure Reason(s)	Recommended Action(s)

Start Save Report... Close Help

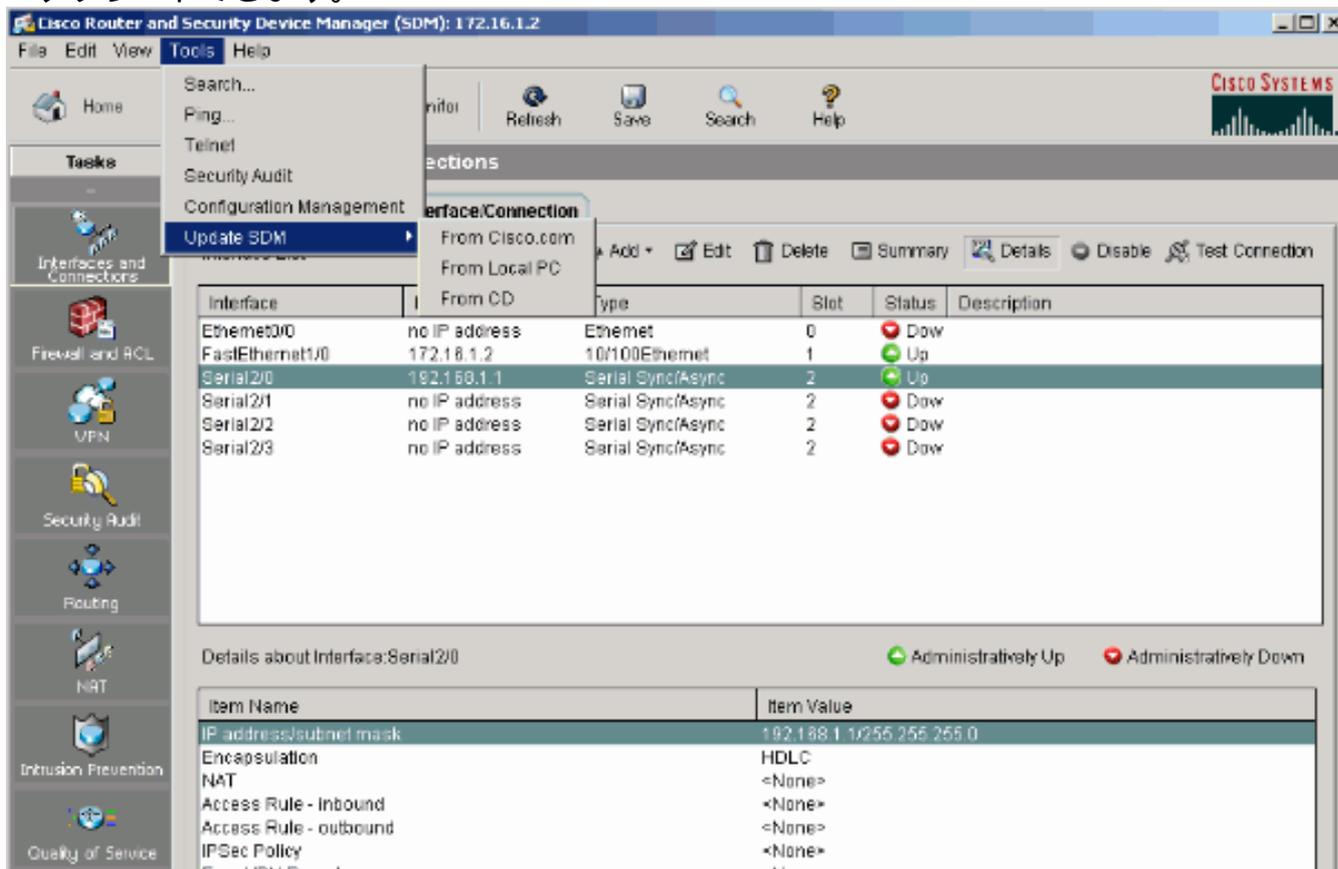
トラブルシューティング

[アウトプット インタープリタ ツール \(登録ユーザ専用\) \(OIT\)](#) は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

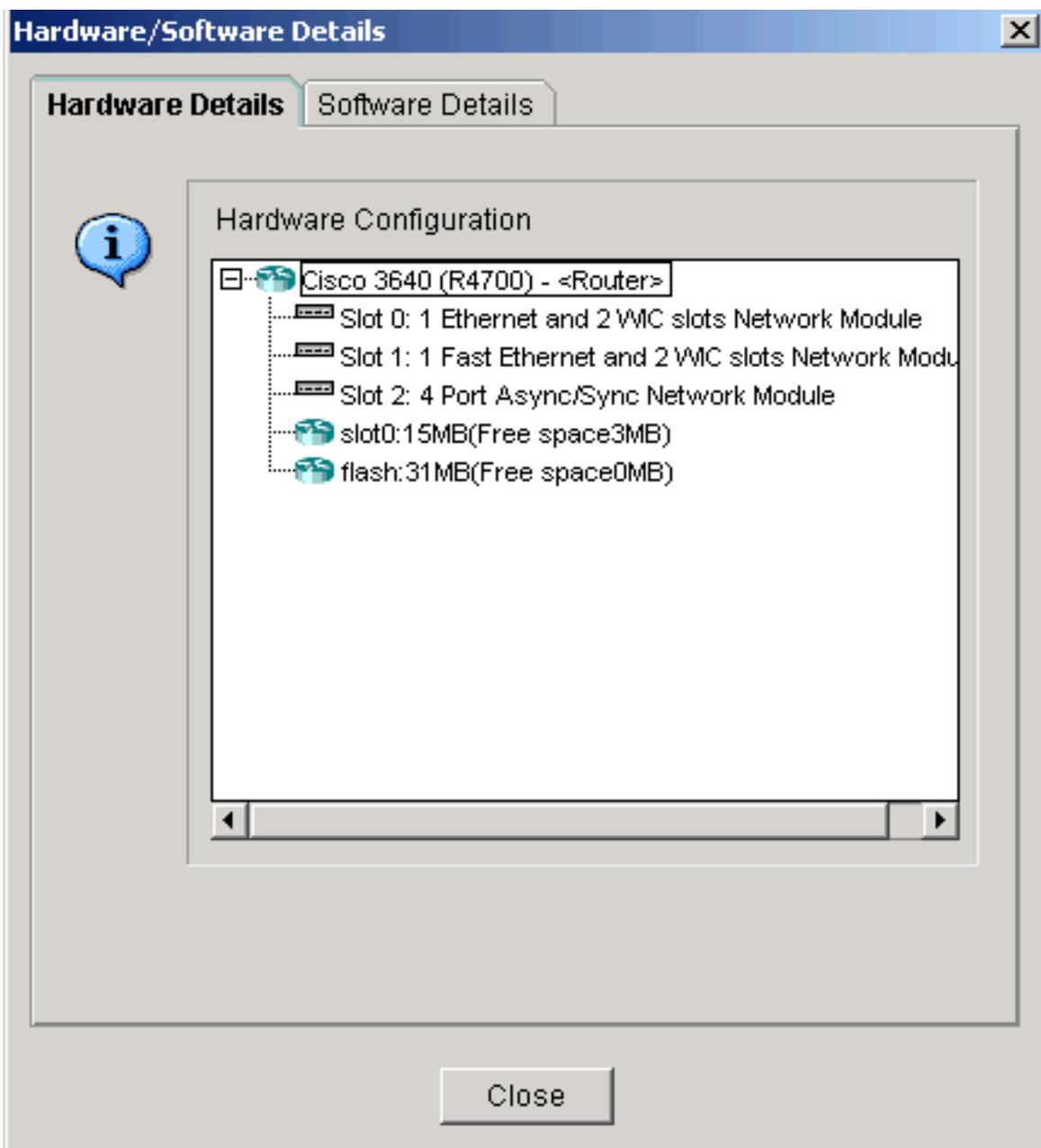
注：debugコマンドを発行する前に、『[デバッグコマンドの重要な情報](#)』を参照してください。

次の方法をトラブルシューティングに使用できます。

- タスク バーから [Tools] > [Update SDM] を選択して、SDM に対する ping、Telnet、および最新バージョンへのアップグレードを行います。Cisco.com、ローカル PC、または CD からアップグレードできます。



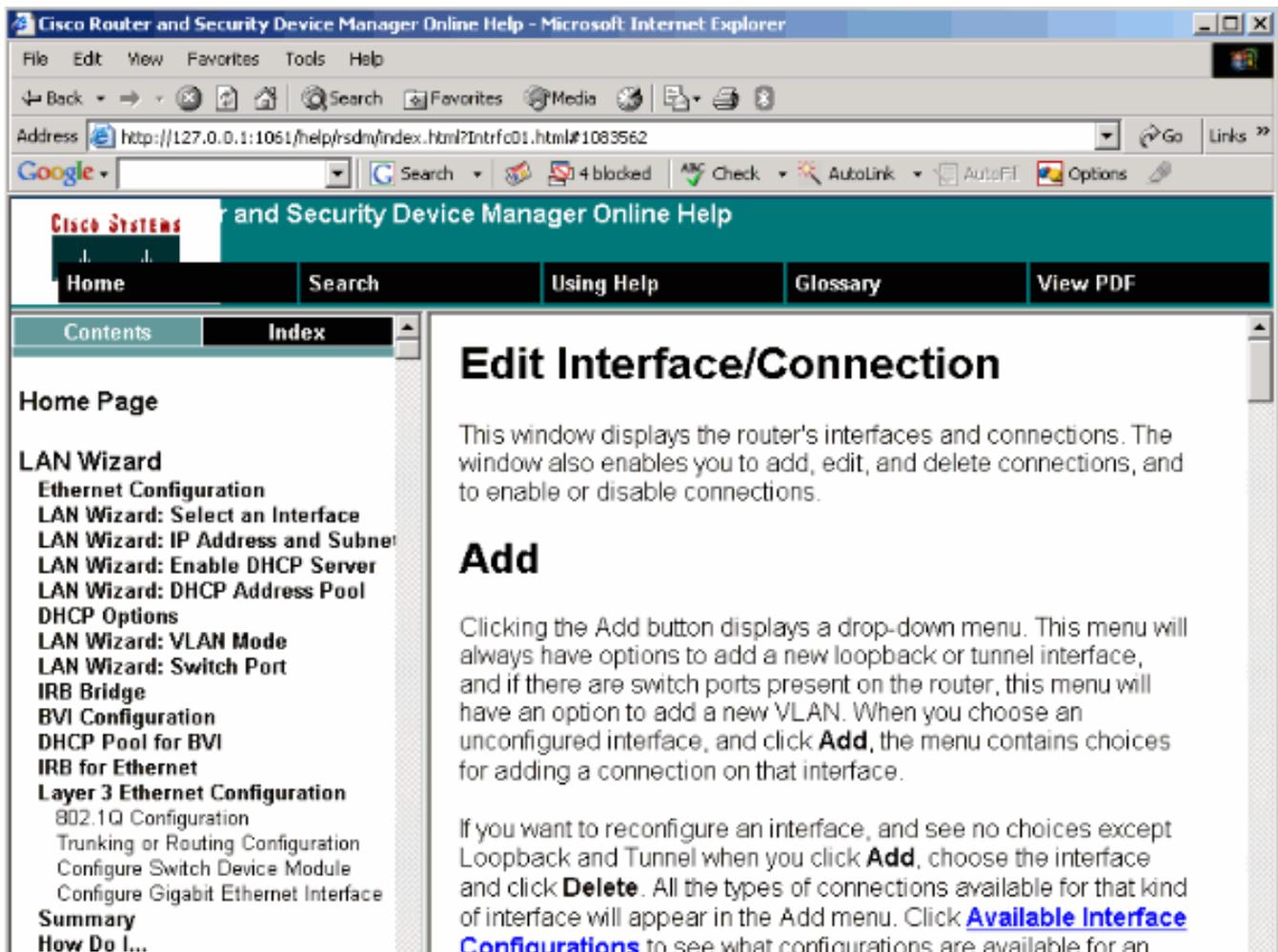
- [Help] > [About this Router] を選択して、ルータのハードウェア設定に関する情報を表示しま



す。 次のウ
インドウに、ルータに保存されている IOS イメージに関する情報が表示されます。



- [Help] オプションでは、ルータの設定に使用できる SDM のさまざまなオプションに関する情報が表示されます。



SDM の 64 ビット OS との互換性

SDM は 64 ビット OS マシンではサポートされていません。ルータに SDM をインストールし、Web ブラウザからアクセスする必要があります。

ルータへの SDM ファイルのインストールに関する詳細については、「[タスク 4 : SDM ファイルのインストール](#)」を参照してください。

Web ブラウザから SDM を起動できない

問題

Web ブラウザを使用して SDM を使用すると、SDM の起動エラー メッセージが表示されます。

解決策 1

問題は Java のバージョンである可能性があります。Java の更新プログラムは SDM のバージョンと互換性がない場合があります。Java のバージョンが Java 6 update 12 の場合は、そのバージョンをアンインストールして、Java 6 update 3 をインストールします。これで問題が解決します。互換性に関する詳細については、「[SDM 2.5 Release Note](#)」の「[Web Browser Versions and Java Runtime Environment Versions](#)」の項を参照してください。SDM バージョン 2.5 は Java バージョン 6 の update 2 および 3 で動作します。

解決策 2

問題を解決するために、Internet Explorer オプションの [Allow active content to run in files on My Computer] を有効にします。

1. Internet Explorer を開き、[Tools] > [Internet Options] > [Advanced] を選択します。
2. セキュリティのセクションで、[Allow active content to run in files on my computer] オプションと [Allow active content to install software even if the signature is invalid] オプションのチェックボックスをオンにします。
3. 変更を有効にするには、[OK] をクリックして、ブラウザを再起動します。

[エラー:java.bling のスタック オーバーフロー](#)

問題

SDM に接続できず、次のエラー メッセージが表示されます。

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

解決方法

この問題は通常、Java コード バージョン 1.5.0_06 が使用されているときに発生します。この問題を解決する方法については、「[The user is unable to connect to Security Device Manager \(SDM\) and receives the java.bling stack over flow error message.](#)」を参照してください。

[関連情報](#)

- [Cisco Security Device Manager インストール ガイド](#)
- [Cisco 製品に関するサポートページ：ルータ](#)
- [Cisco Configuration Professional のサポート ページ](#)
- [NAT に関するサポート ページ](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)