Basic Router Configuration using SDM

Document ID: 71305

Contents

Introduction
Prerequisites
Requirements
Components Used
Conventions
Configure
Network Diagram
Interface Configuration
NAT Configuration
Routing Configuration
Miscellaneous Configuration
CLI Configuration
Verify
Troubleshoot
Comatibility of SDM with 64-bit OS
Unable to Launch the SDM through Web Browser
Error: java.bling stack overflow
Related Information

Introduction

This document describes how to use the Cisco Security Device Manager (SDM) in order to set the basic configuration of the router. This includes the configuration of the IP address, default routing, static and dynamic routing , static and dynamic NATing, hostname, banner, secret password, user accounts, and so forth. Cisco SDM allows you to configure your router in all kinds of network environments that includes small office home office (SOHO), branch office (BO), regional office, and central site or Enterprise headquarters using an easy-to-use web-based management interface.

Prerequisites

Requirements

This document assumes that the Cisco router is fully operational and configured to allow the Cisco SDM to make configuration changes.

Note: Refer to Allowing HTTPS Access for SDM in order to allow the router to be configured by the SDM.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 3640 Router with Cisco IOS® Software Release 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.

Note: If you use a Cisco Integrated Service Router (ISR), refer to Basic Router Configuration Using Cisco Configuration Professional for similar configuration details with more powerful features. For information on which routers are suppoted by Cisco CP, refer to the Supported Routers section of the *Release Notes for Cisco Configuration Professional 2.5*.

Conventions

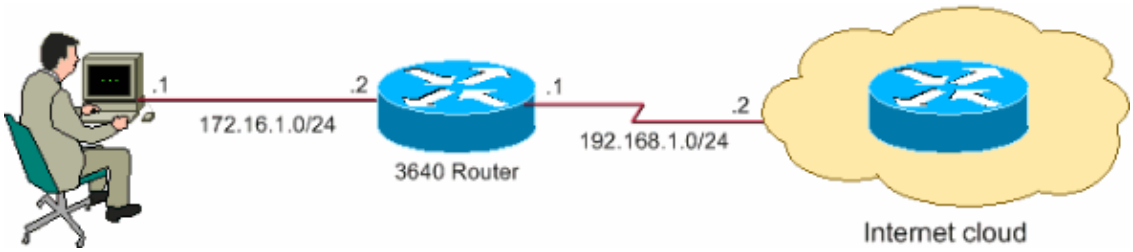
Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Configure

In this section, you are presented with the information to configure the basic settings for router in a network.

Network Diagram

This document uses this network setup:



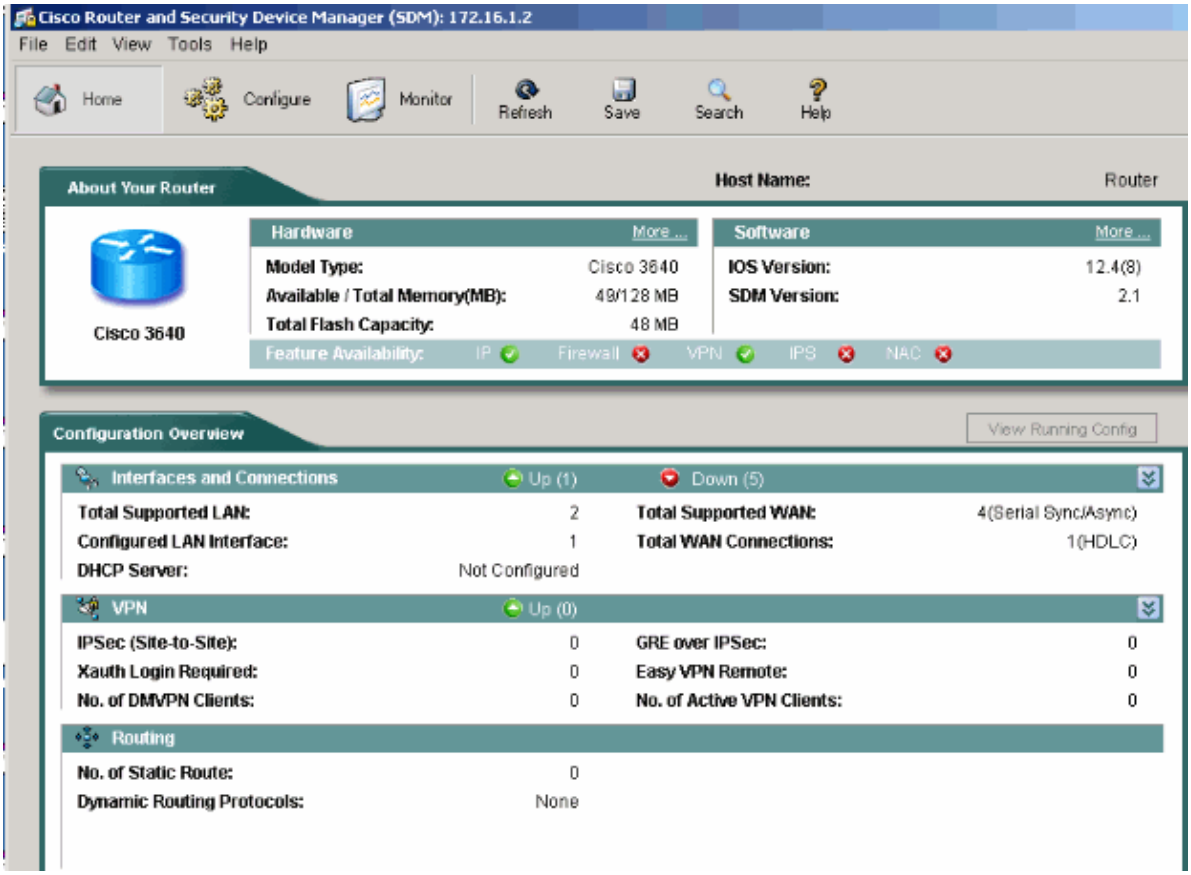
Note: The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 addresses which have been used in a lab environment.

Interface Configuration

Complete these steps in order to configure the interfaces of a Cisco router.

1. Click **Home** in order to go to the SDM Home page.

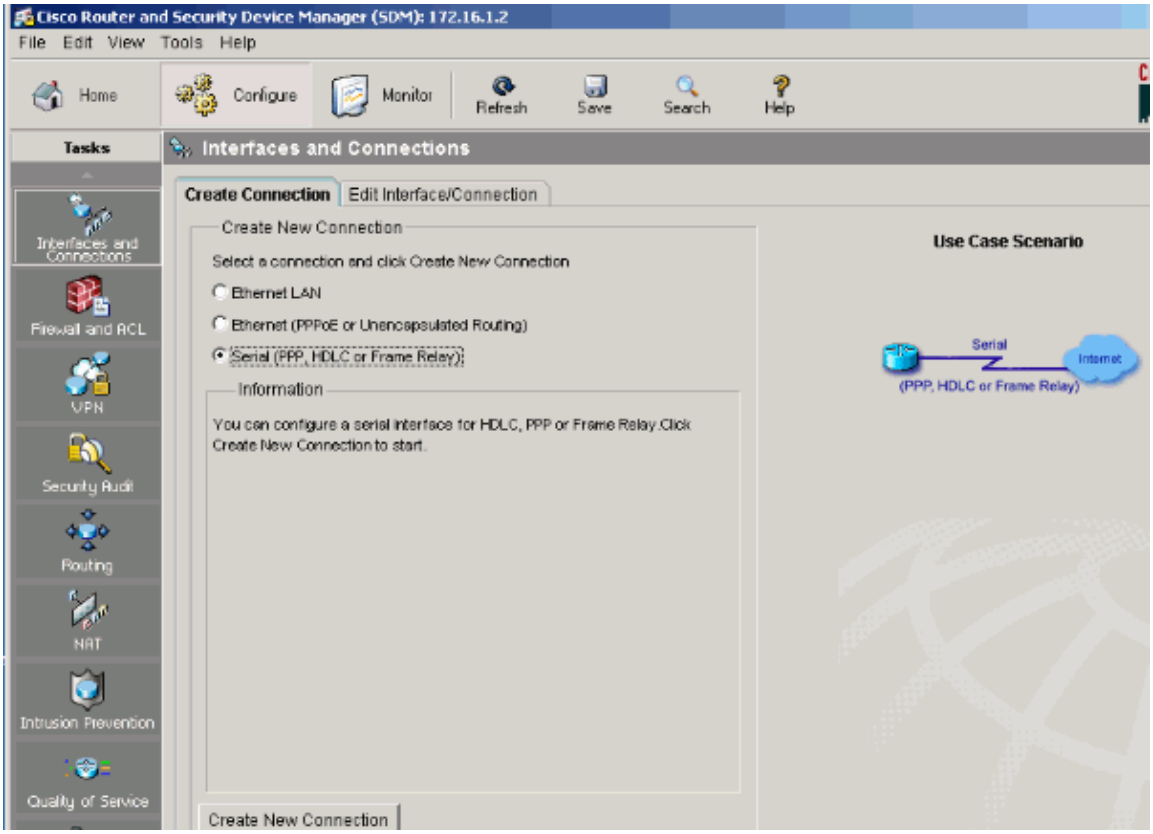
   The SDM Home page provides information such as hardware and software of the router, feature availability, and a configuration summary. The green circles show the features supported in this router and the red circles show the features not supported.



2. Choose **Configure > Interfaces and Connections > Create Connection** in order to configure the WAN connection for the interface.

   As an example, for serial interface 2/0, choose the **Serial** option and click **Create New Connection**.

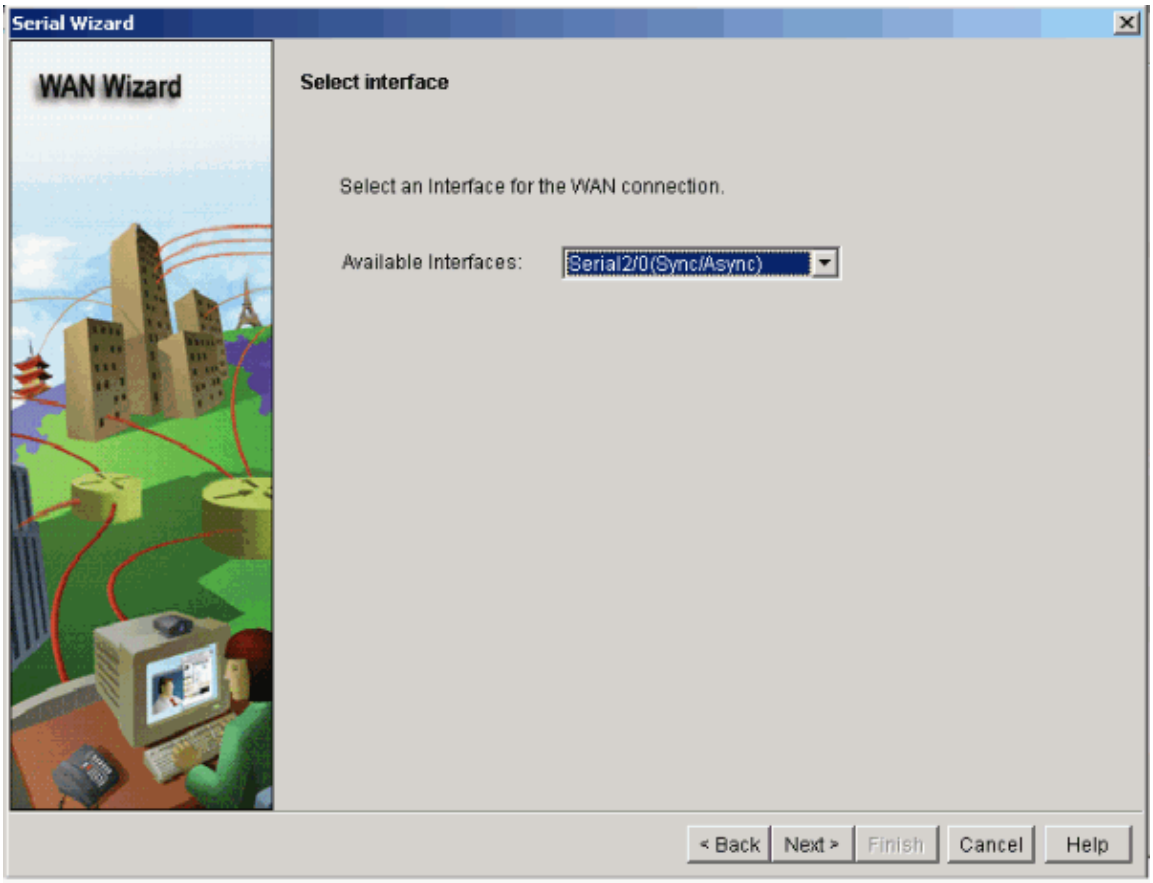
   Note: For other types of interfaces like **Ethernet**, choose the respective interface type and proceed by clicking the **Create New Connection** button.



3. Click **Next** in order to proceed once this interface appears.



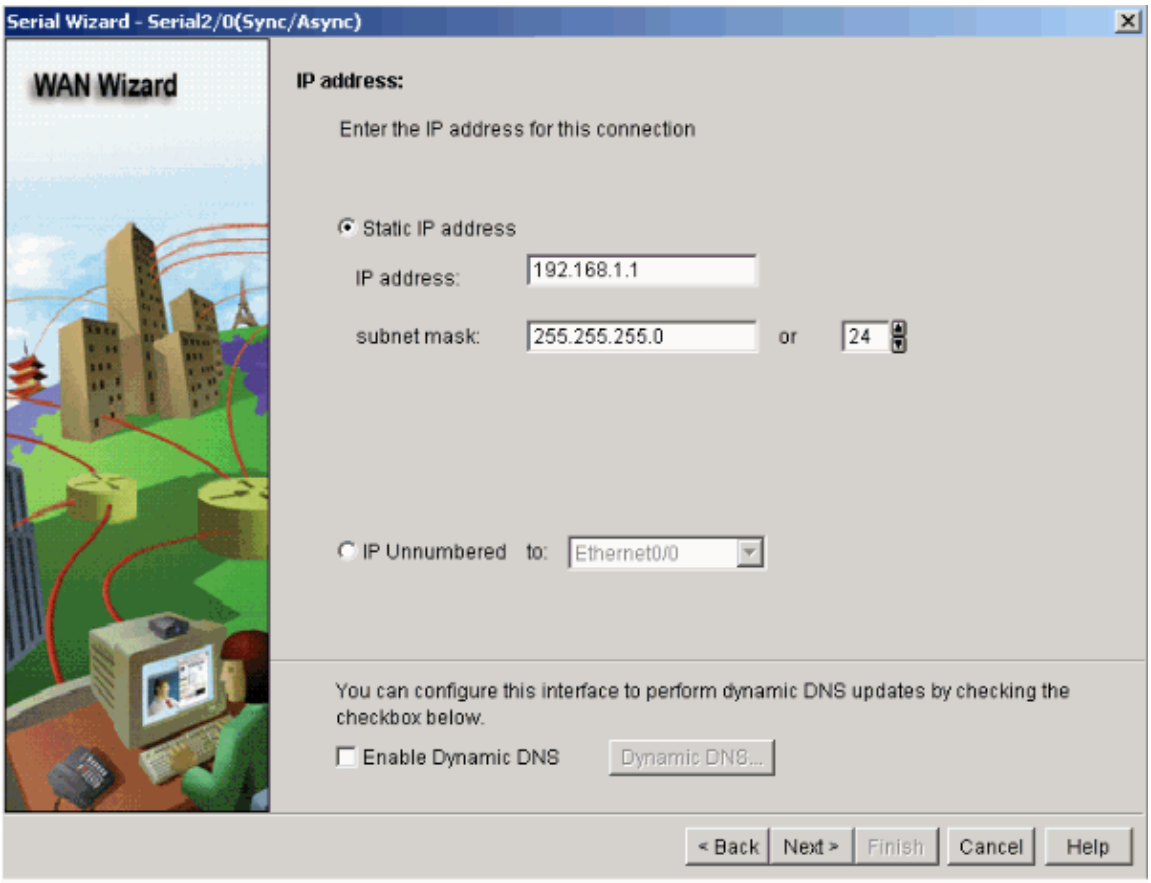
4. Select **Serial interface 2/0** (desired) from the Available Interfaces option and click **Next**.



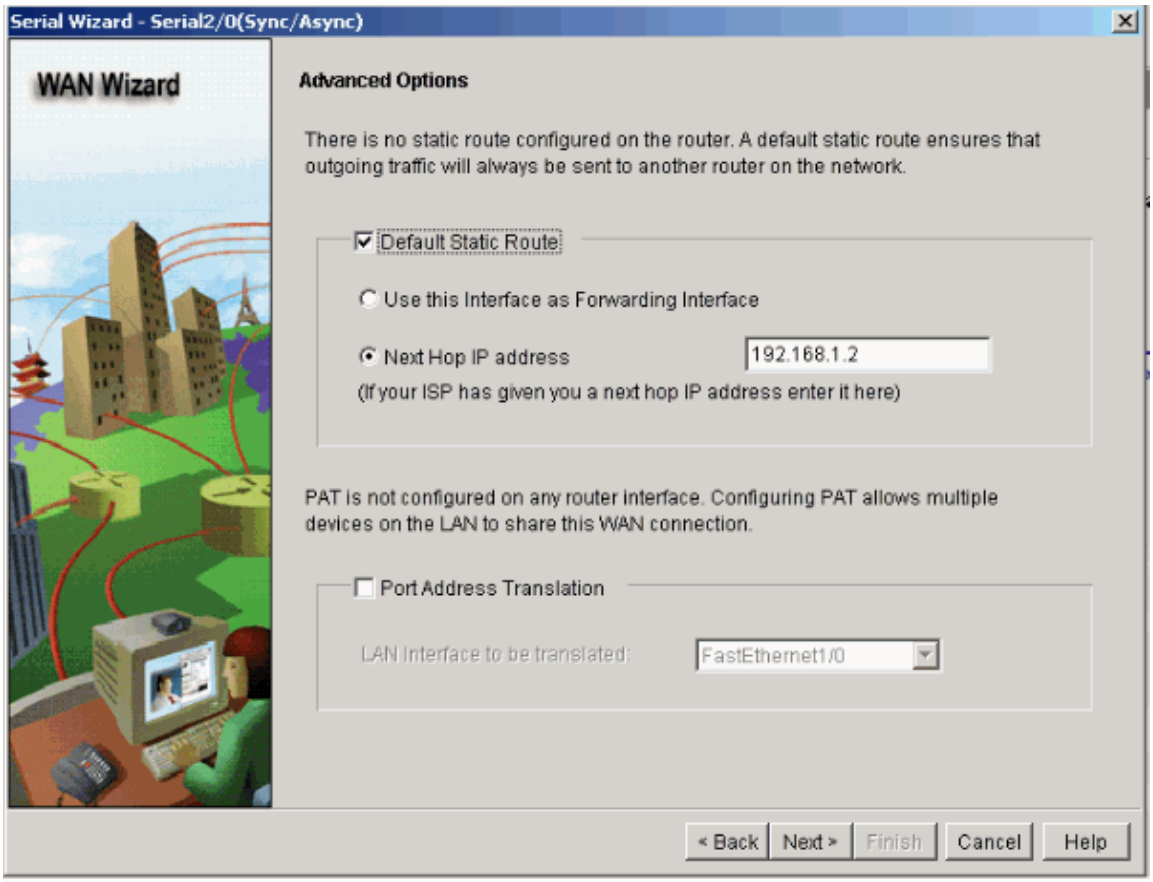
5. Choose the encapsulation type for the serial interface and click **Next**.



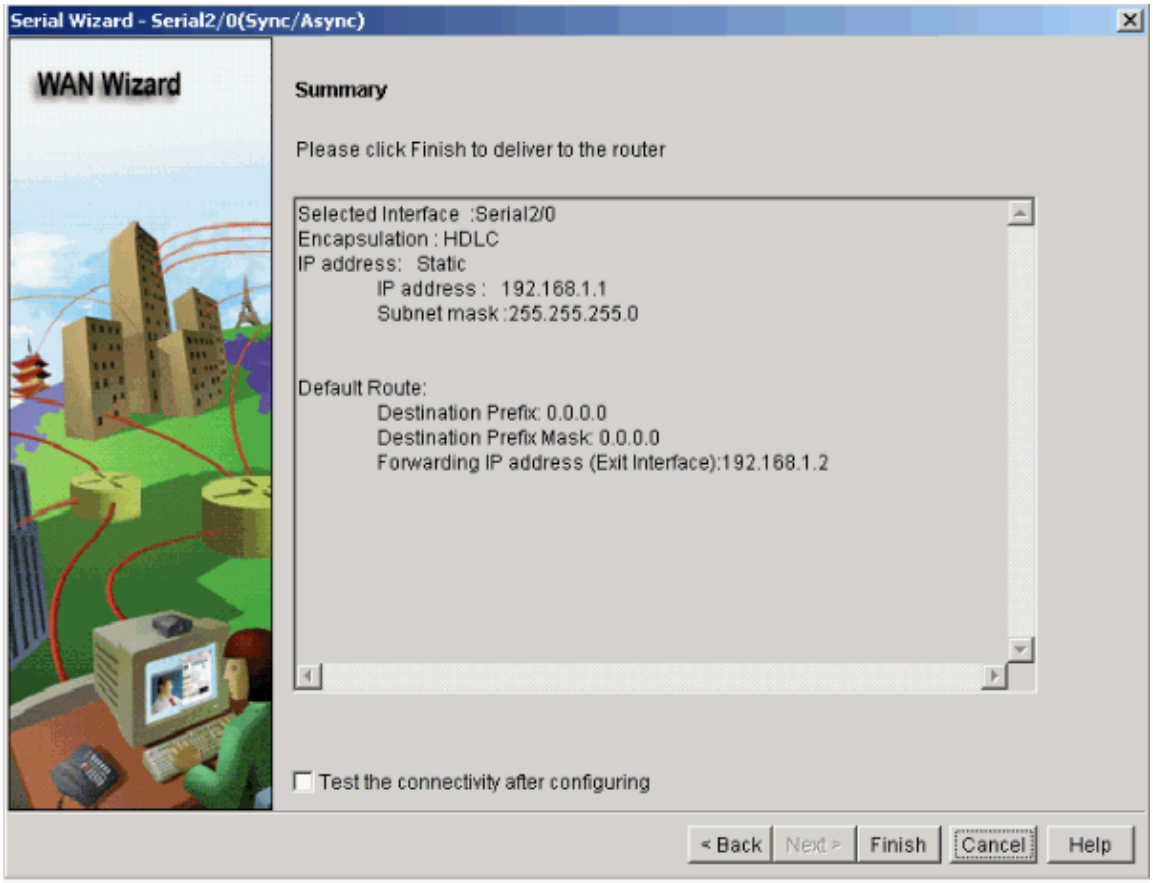
6. Specify the static IP address with the corresponding subnet mask for the interface and click **Next**.



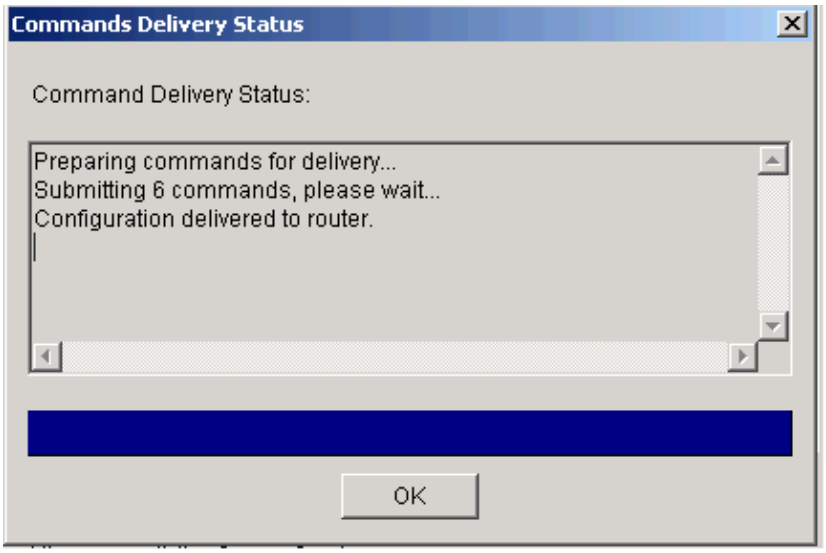
7. Configure the default routing with optional parameters such as the next hop IP address (192.168.1.2 as per network diagram) supplied by the ISP and click **Next**.



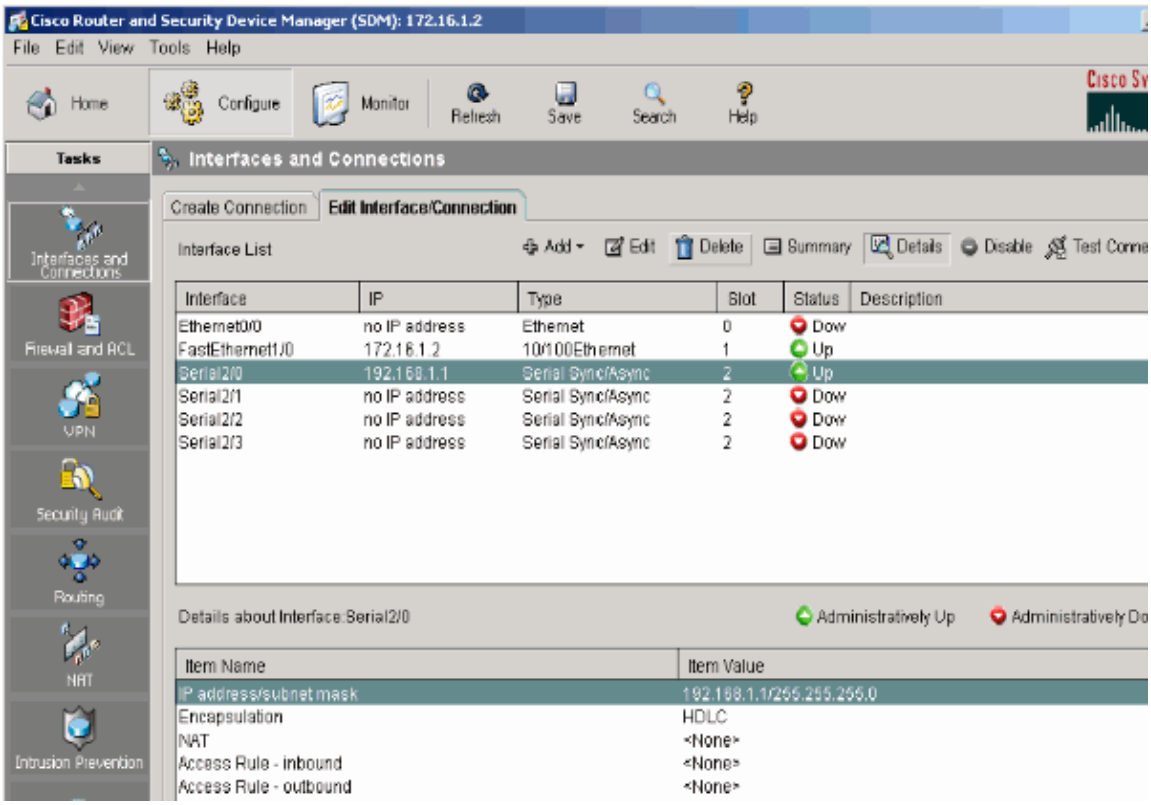
This window appears and shows the configuration summary configured by the user. Click **Finish**.



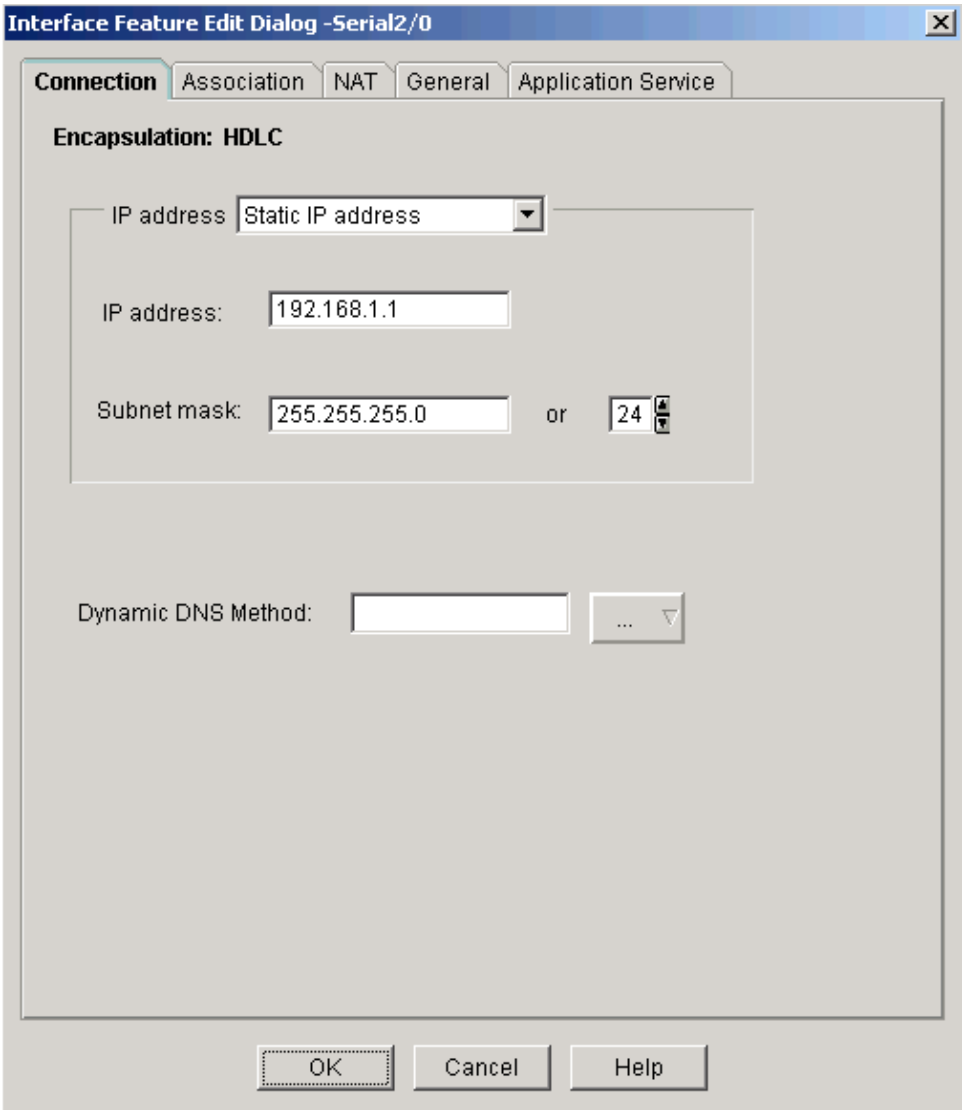
This window appears and shows the command delivery status to the router. Otherwise, it displays errors if the command delivery fails due to incompatible commands or unsupported features.



8. Choose **Configure > Interfaces and Connections > Edit Interfaces/Connections** in order to add/edit/delete the various interfaces.



Highlight the interface with which you want to make changes and click **Edit** if you want to edit or change the interface configuration. Here you can change the existing static IP address.

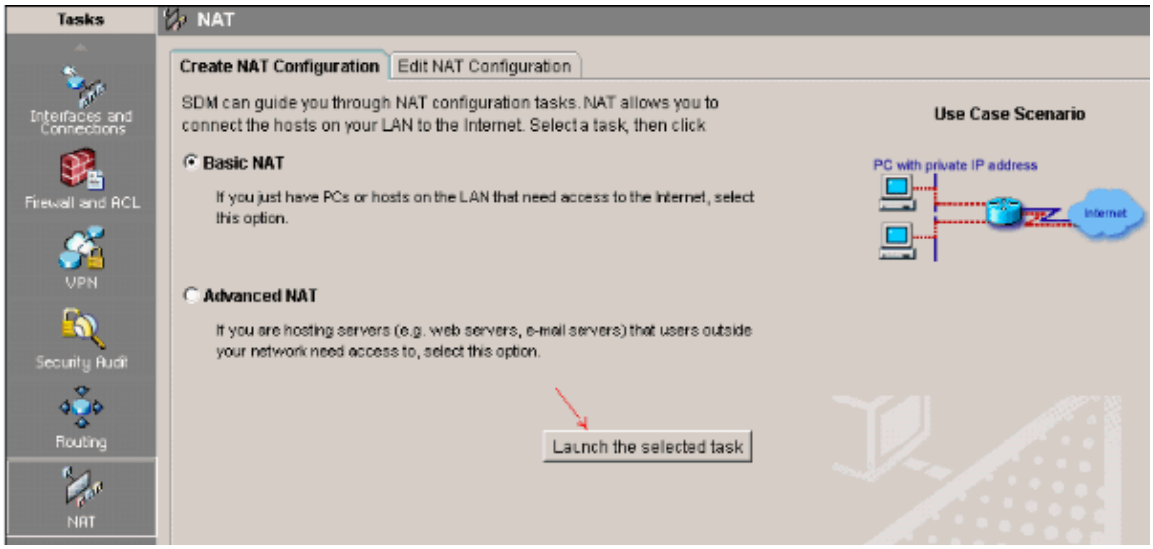


NAT Configuration

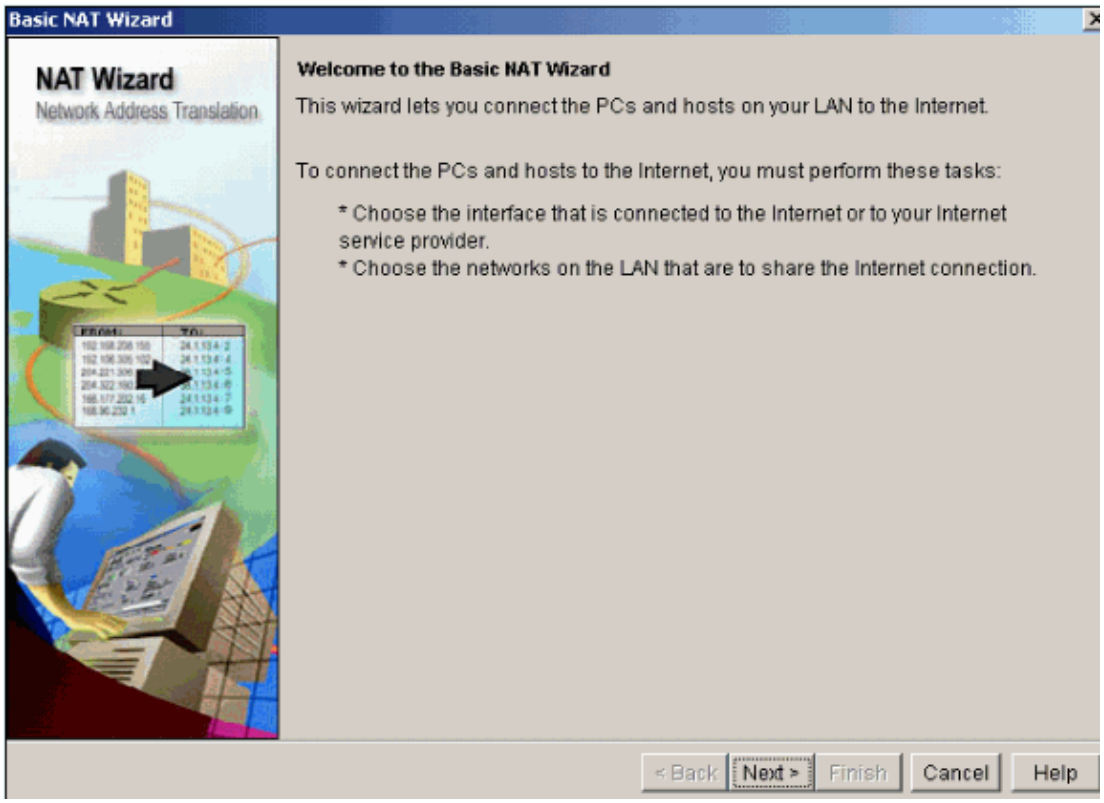
Dynamic NAT Configuration

Complete these steps in order to configure the dynamic NAT in a Cisco router.

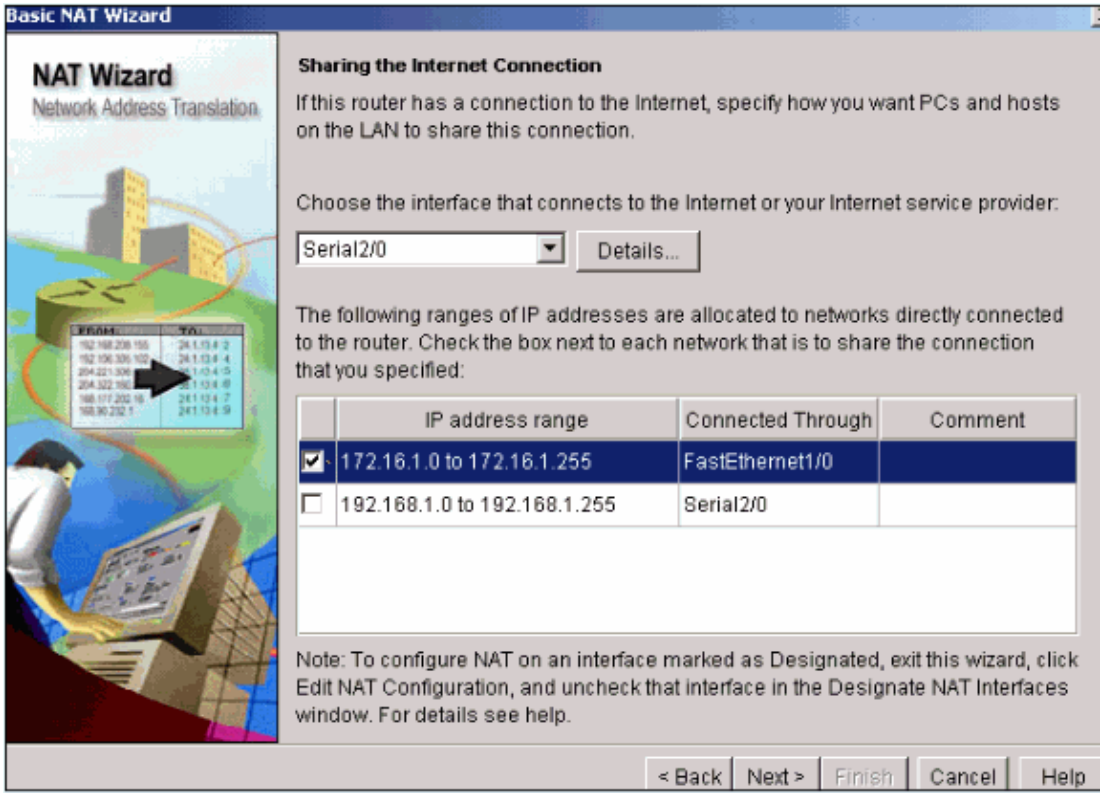
1. Choose **Configure > NAT > Basic NAT** and click **Launch the selected task** in order to configure basic NATing.



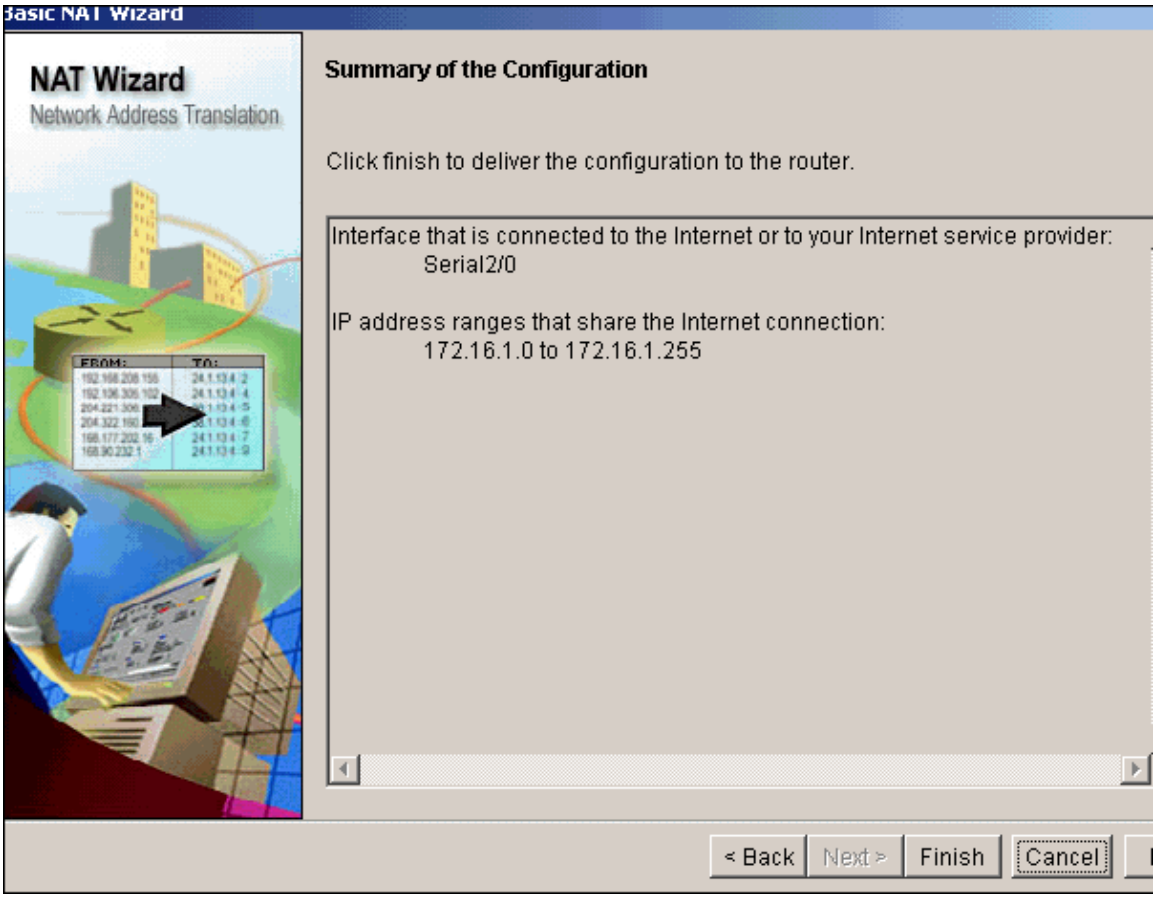
2. Click **Next**.



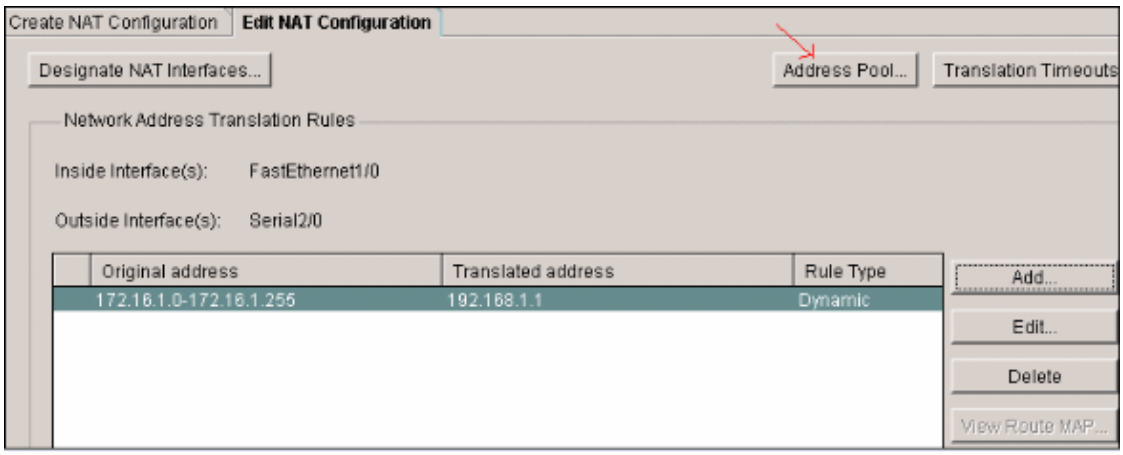
3. Choose the interface that connects to the Internet or your ISP and choose the IP address range to which Internet access is to be shared.



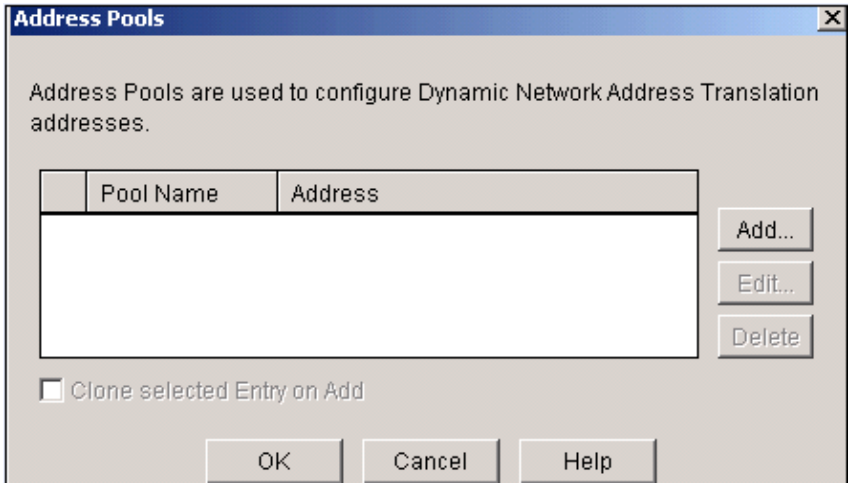
4. This window appears and shows the configuration summary configured by the user. Click **Finish**.



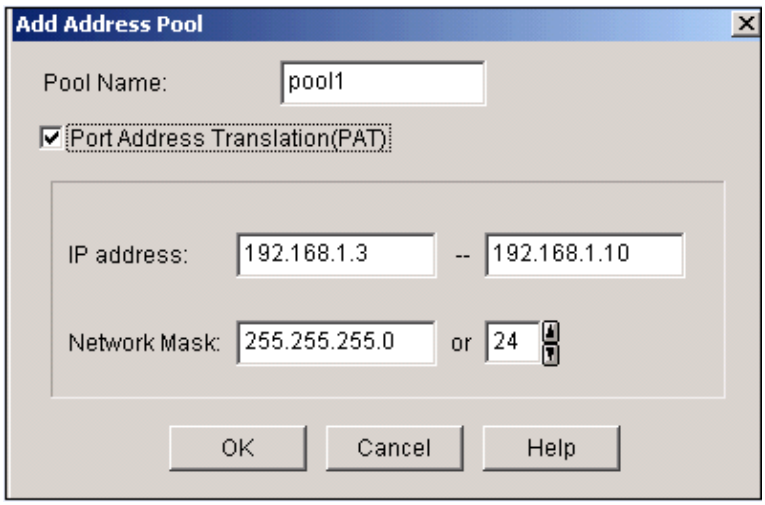
5. The Edit NAT Configuration window shows the configured dynamic NAT configuration with the translated IP address overloaded (PATing). If you want to configure the dynamic NATing with address pool, click **Address Pool**.



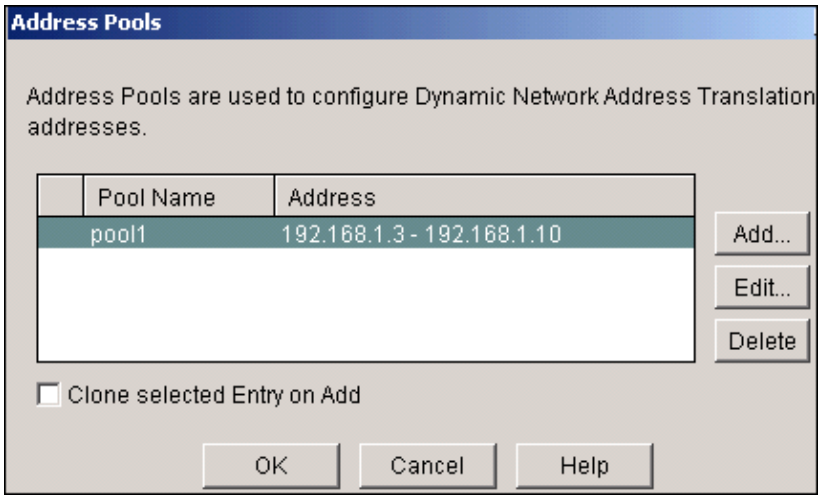
6. Click **Add**.



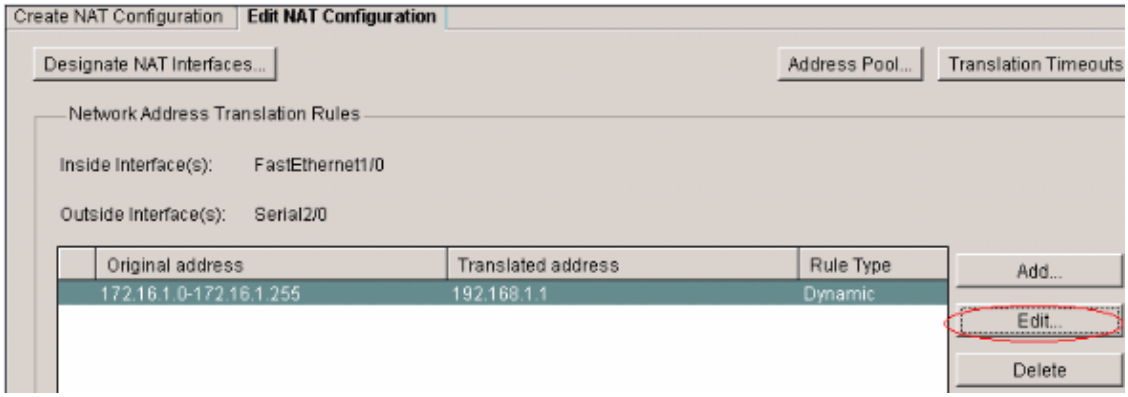
Here informations such as the pool name and IP address range with netmask are provided. There can be times when most of the addresses in the pool have been assigned, and the IP address pool is nearly depleted. When this occurs, PAT can be used with a single IP address in order to satisfy additional requests for IP addresses. Check **Port Address Translation (PAT)** if you want the router to use PAT when the address pool is close to depletion.



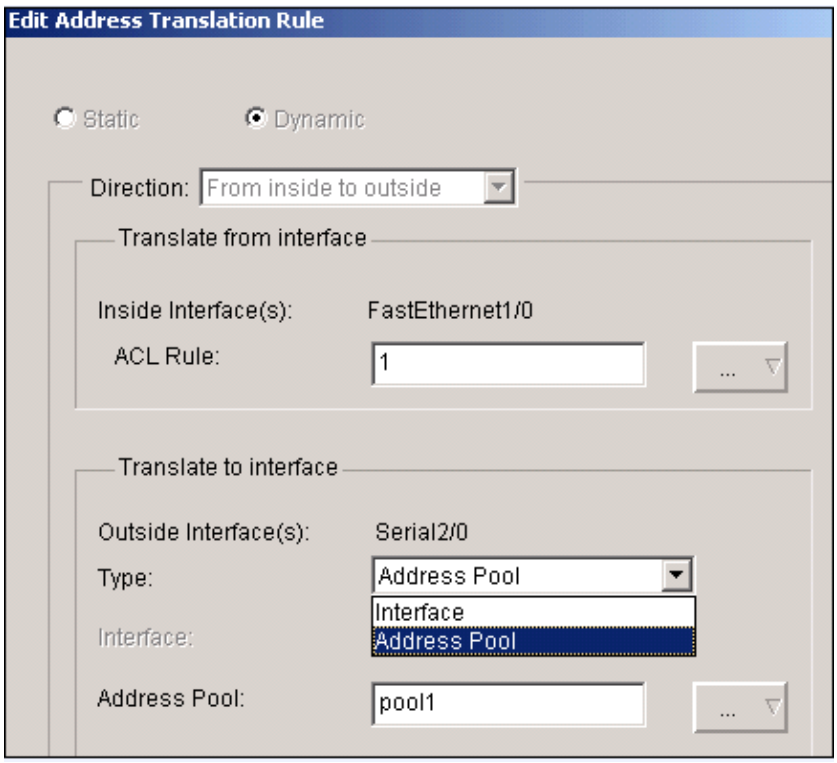
7. Click **Add**.



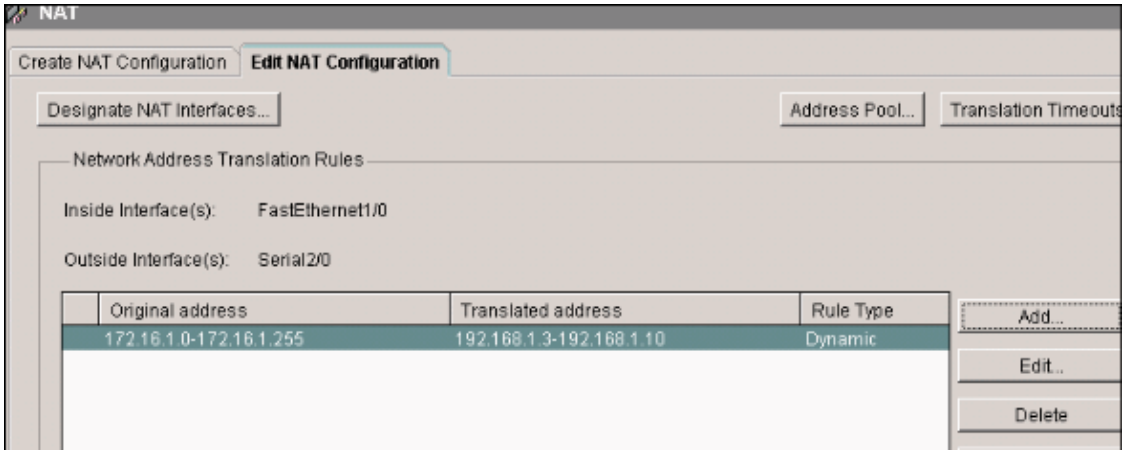
8. Click **Edit**.



9. Choose **Address Pool** in the Type field, provide the name to the Address Pool as **pool1** and click **OK**.

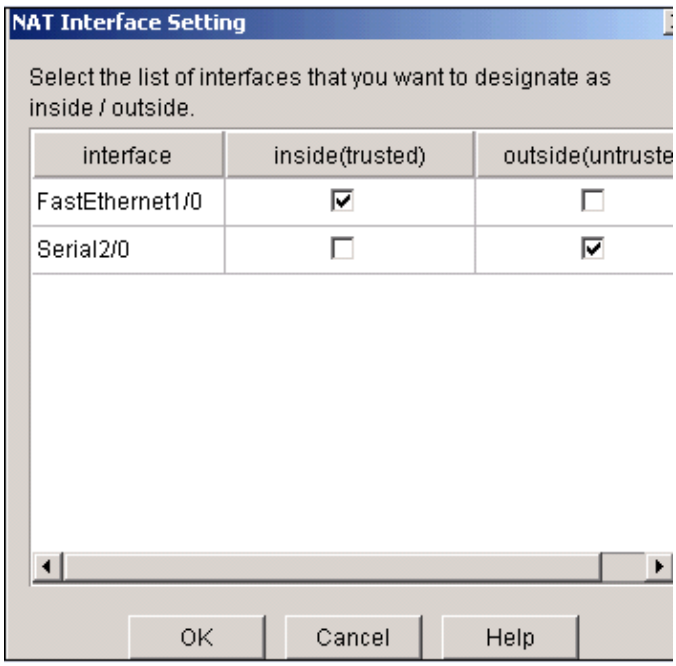


10. This window shows the configuration for dynamic NATing with the address pool. Click **Designate NAT Interfaces**.



Use this window in order to designate the inside and outside interfaces that you want to use in NAT translations. NAT uses the inside and outside designations when it interprets translation rules, because translations are performed from inside to outside, or from outside to inside.

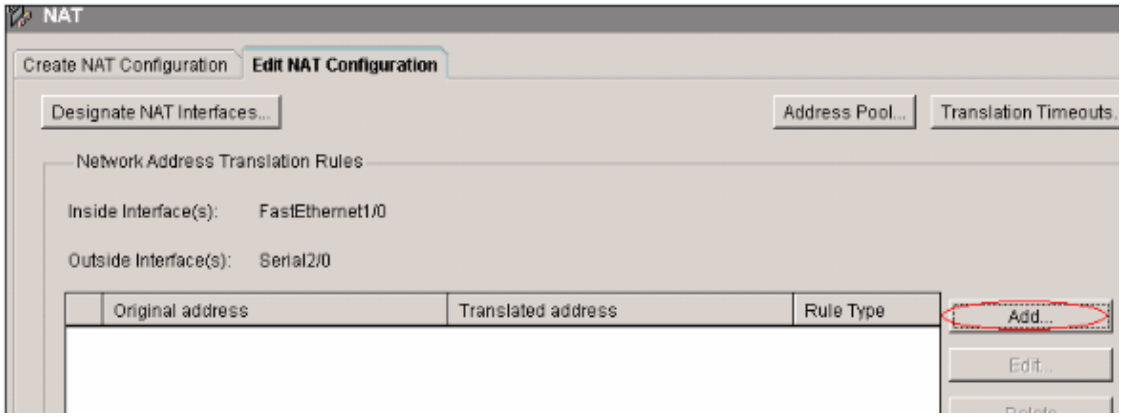
Once designated, these interfaces are used in all NAT translation rules. The designated interfaces appear above the Translation Rules list in the main NAT window.



Static NAT Configuration

Complete these steps in order to configure static NAT in a Cisco router.

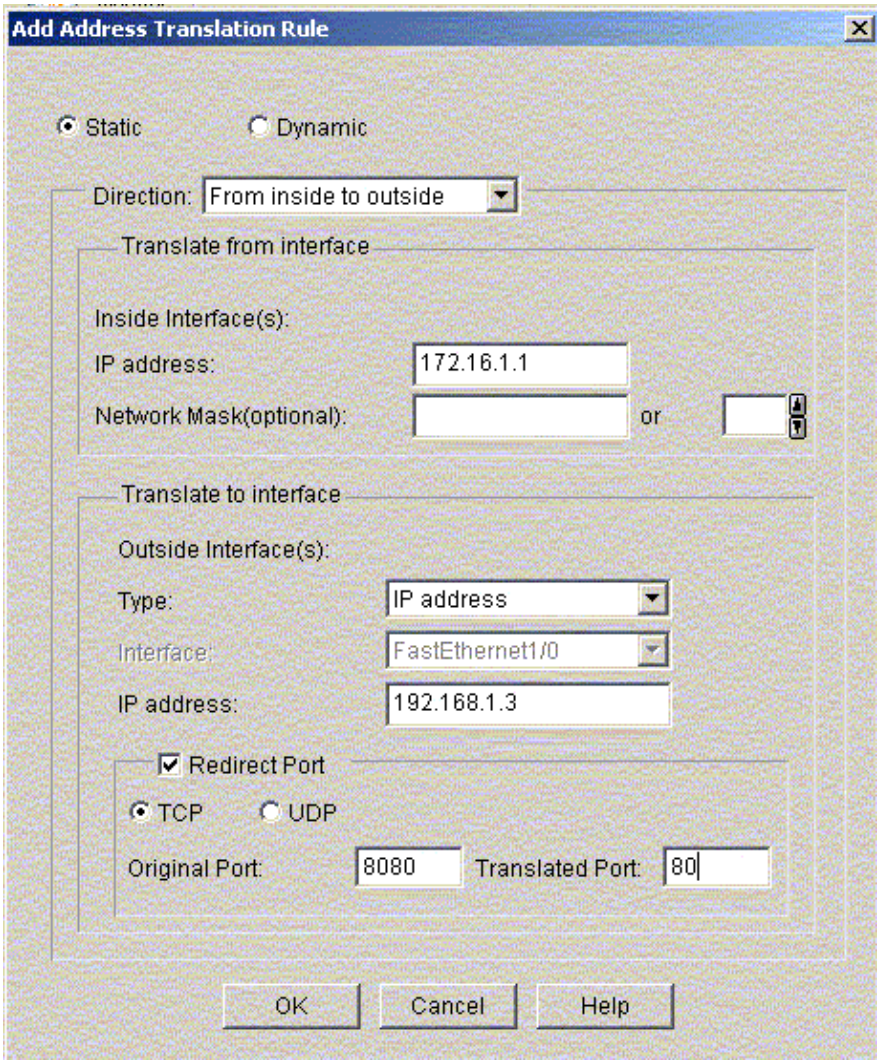
1. Choose **Configure > NAT > Edit NAT Configuration** and click **Add** in order to configure static NATing.



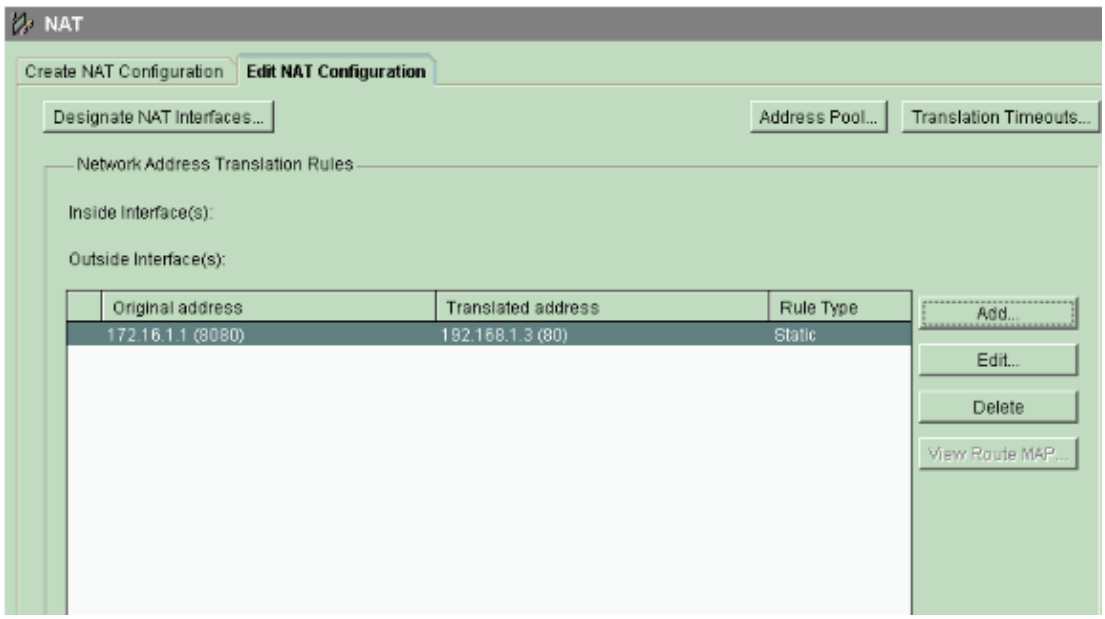
2. Choose the **Direction** either from inside to outside or from outside to inside, specify the inside IP address to be translated under **Translate from Interface**. For the **Translate to Interface** area select the Type.

    - Choose **IP Address** if you want the Translate from Address to be translated to an IP address defined in the IP Address field.
    - Choose **Interface** if you want the **Translate from Address** to use the address of an interface on the router. The **Translate from Address** is translated to the IP address assigned to the interface that you specify in the Interface field.

   Check **Redirect Port** if you want to include port information for the inside device in the translation. This enables you to use the same public IP address for multiple devices, as long as the port specified for each device is different. You must create an entry for each port mapping for this Translated to address. Click **TCP** if this is a TCP port number and click **UDP** if it is a UDP port number. In the Original Port field, enter the port number on the inside device. In the Translated Port field, enter the port number that the router is to use for this translation. Refer to the Allowing the Internet to Access Internal Devices section of Configuring Network Address Translation: Getting Started.



This window shows the static NATing configuration with port redirection enabled.

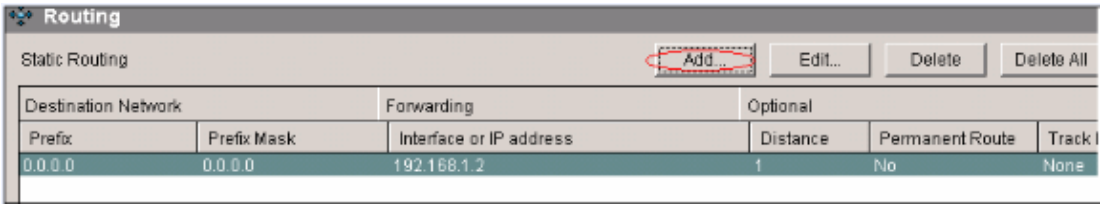


Routing Configuration

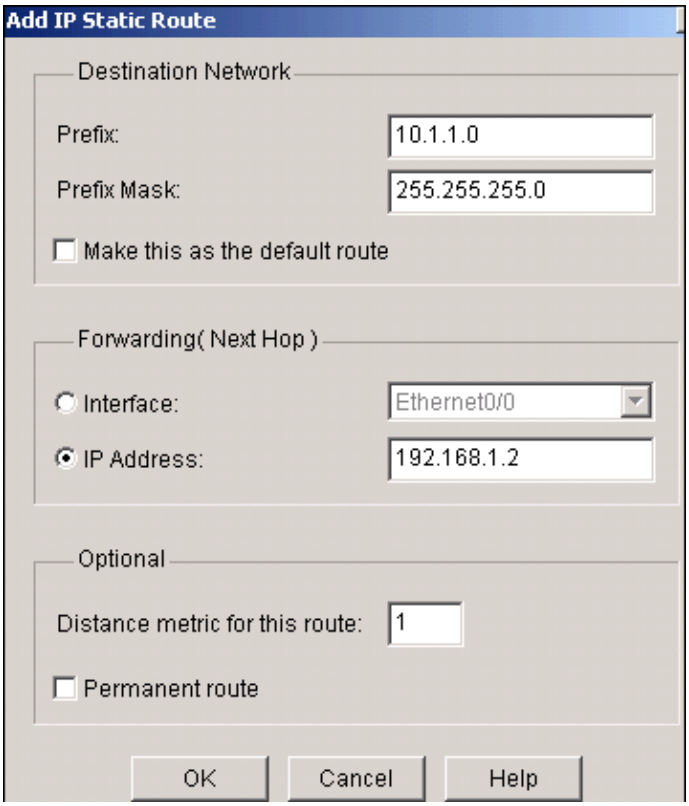
Static Routing Configuration

Complete these steps in order to configure static routing in a Cisco router.

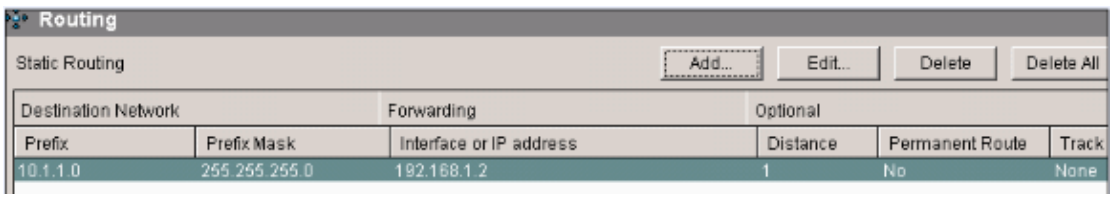
1. Choose **Configure > Routing > Static Routing** and click **Add** in order to configure static routing.



2. Enter the Destination Network address with mask and select either outgoing interface or next hop IP address.



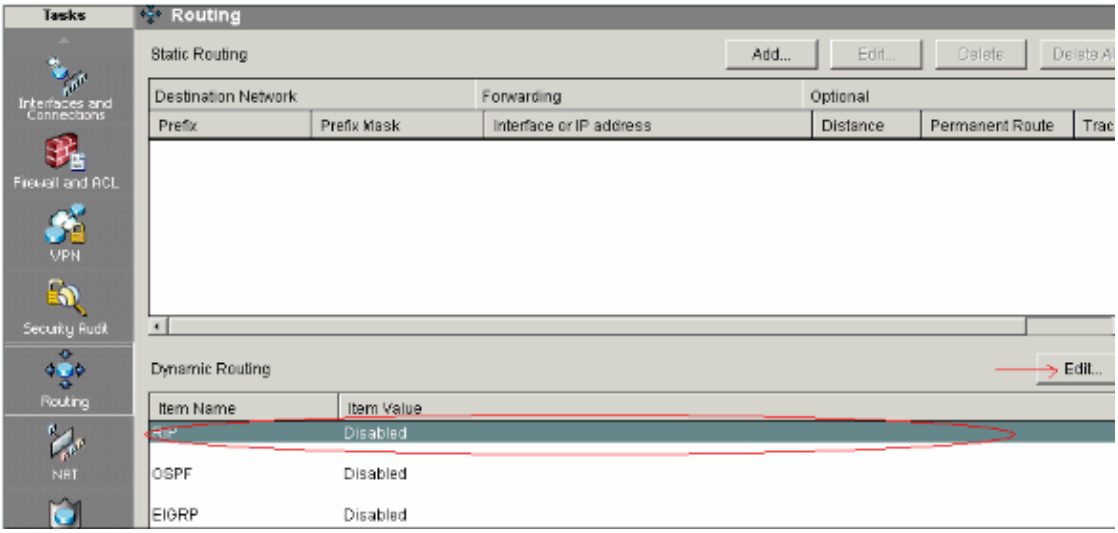
This window shows the static route configured for the 10.1.1.0 network with 192.168.1.2 as the next hop IP address.



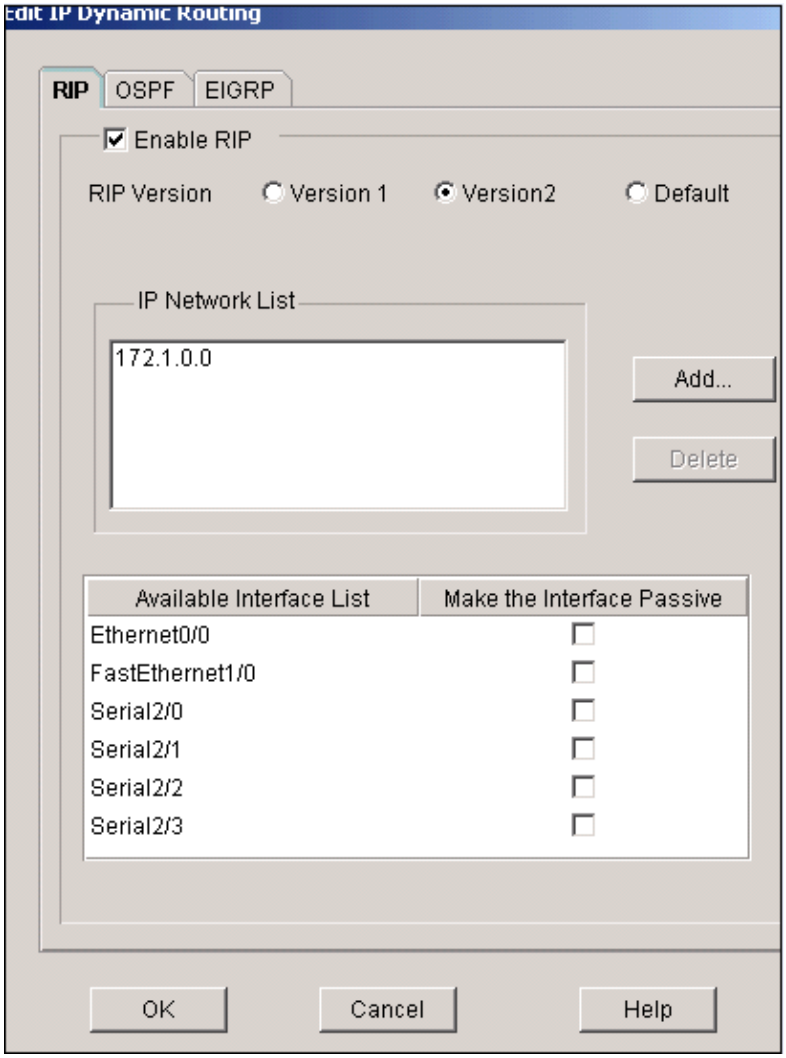
Dynamic Routing Configuration

Complete these steps in order to configure the dynamic routing in a Cisco router.

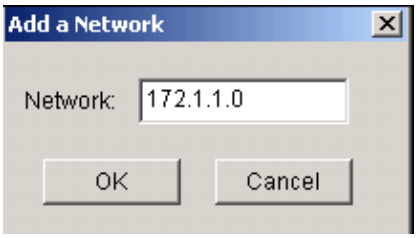
1. Choose **Configure > Routing > Dynamic Routing**.
2. Select the **RIP** and click **Edit**.



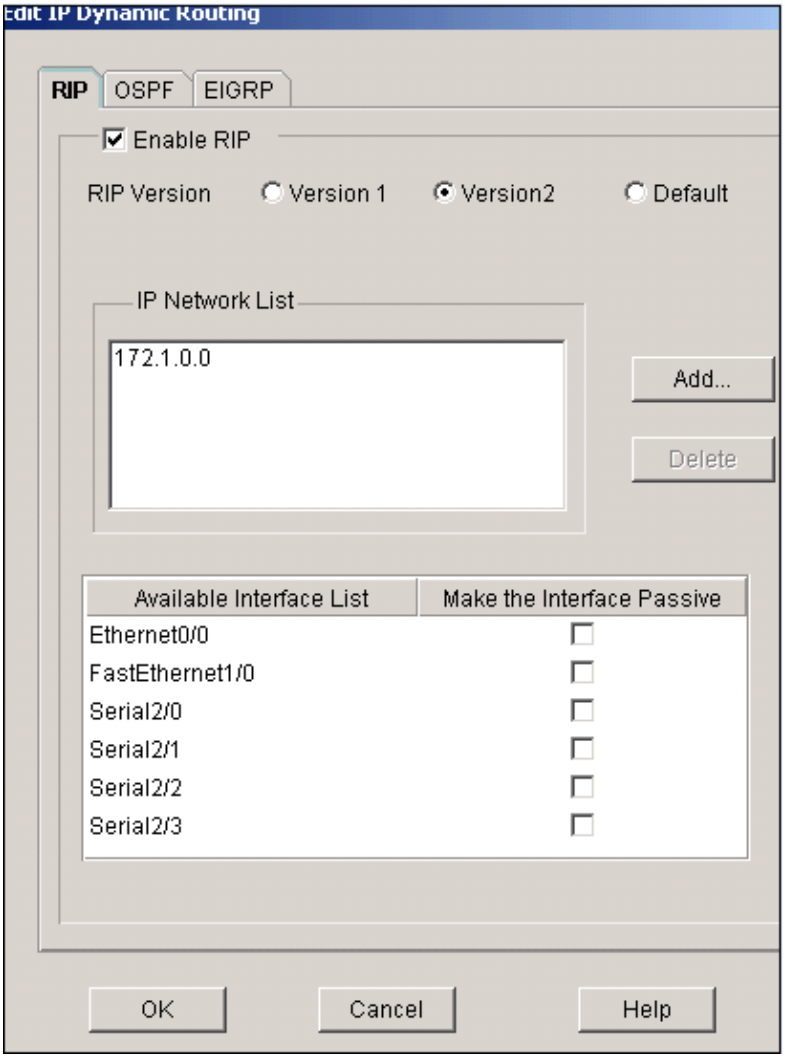
3. Check **Enable RIP**, select the RIP version, and click **Add**.



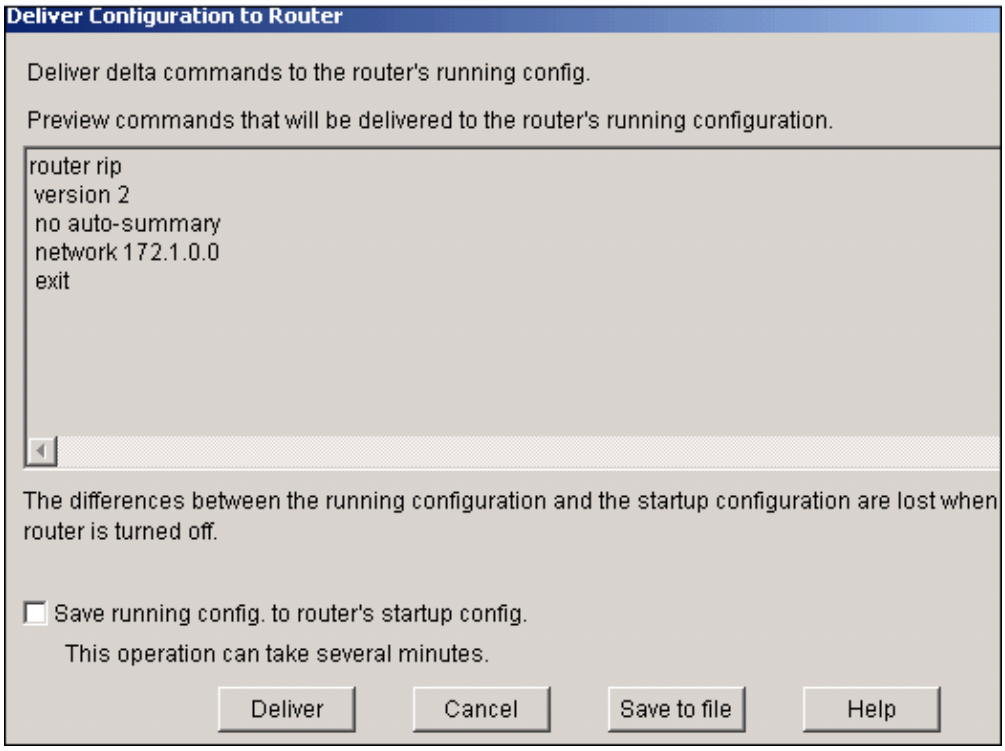
4. Specify the Network address to be advertised.



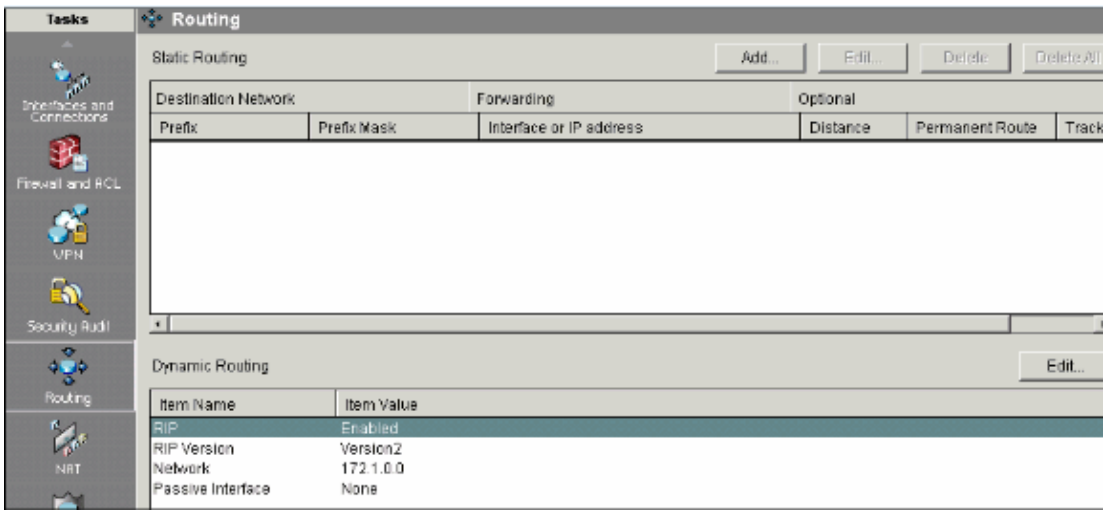
5. Click **OK**.



6. Click **Deliver** in order to transfer the commands to the router.



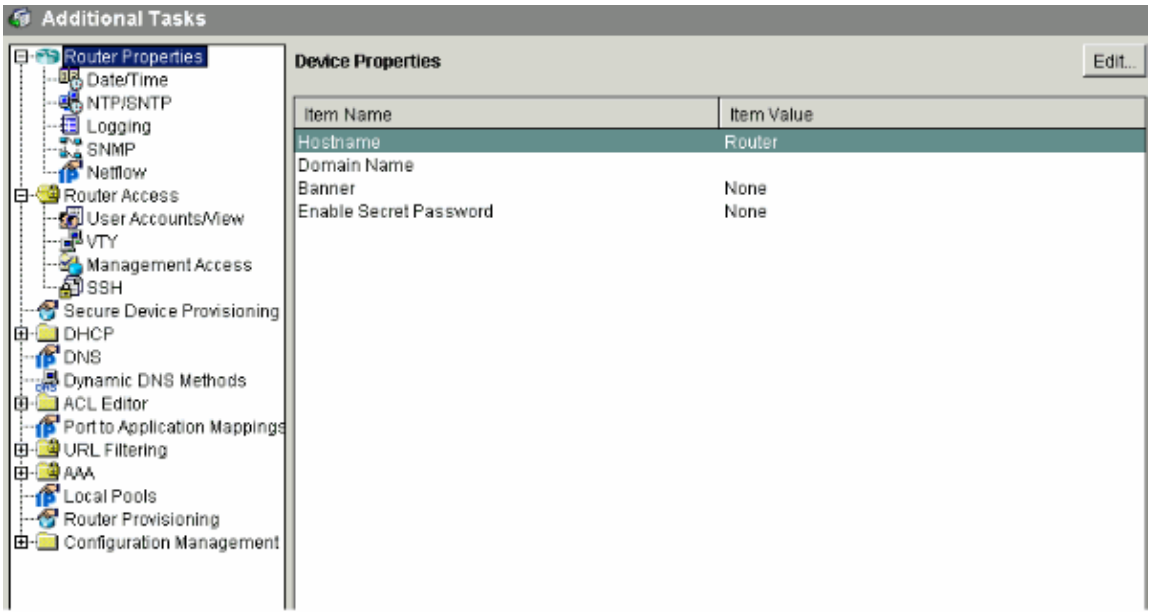
This window shows the dynamic RIP routing configuration.



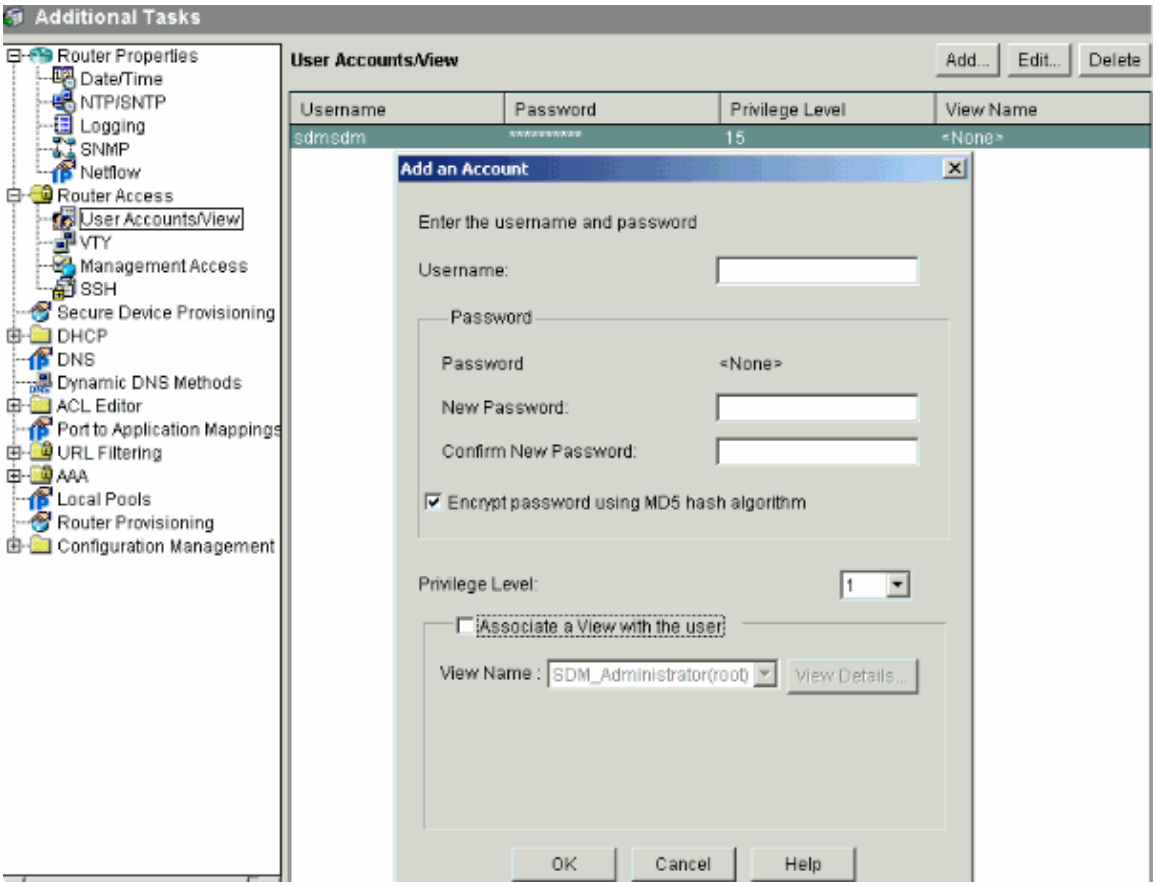
Miscellaneous Configuration

Complete these steps in order to configure the other basic settings in a Cisco router.

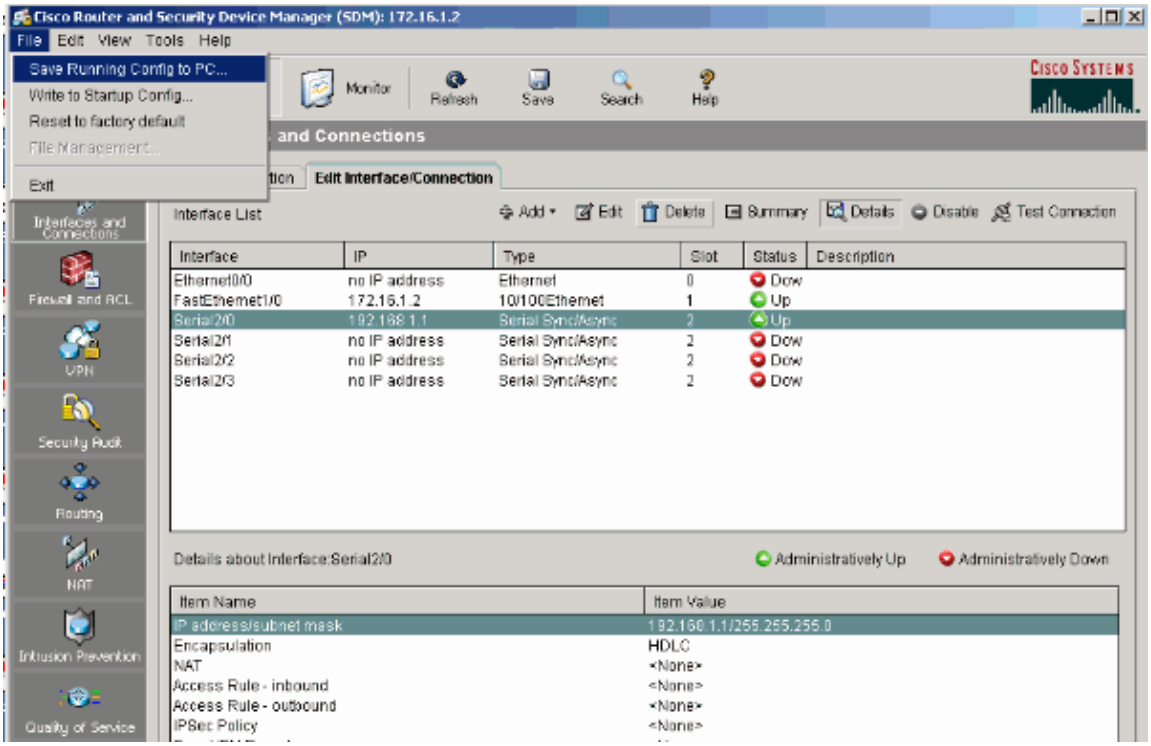
1. Choose **Configure > Additional Tasks > Router Properties** and click **Edit** if you want to change the Hostname, Domain Name, Banner and Enable Secret Password properties for a router.



2. Choose **Configure > Additional Tasks > Router Access > User Accounts/View** in order to add/edit/delete the User Accounts to the router.

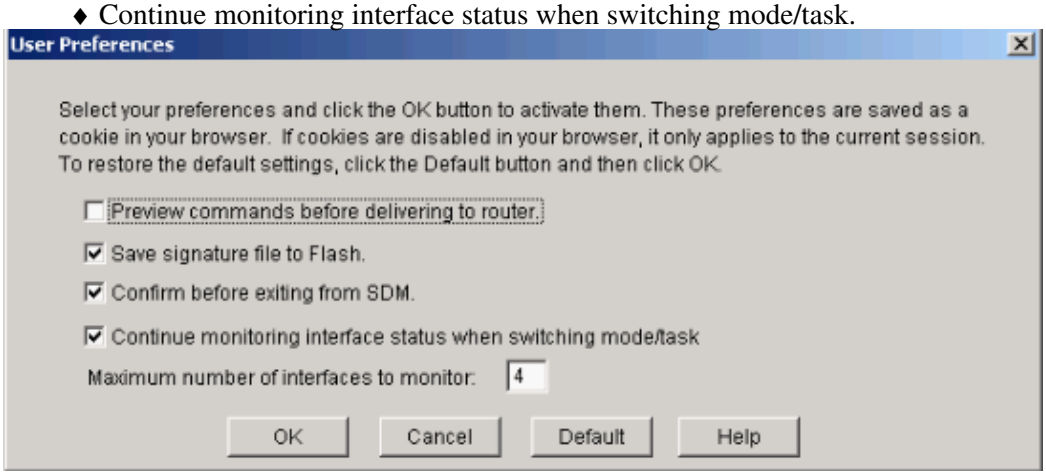


3. Choose **File > Save Running Config to PC...** in order to save the configuration to the NVRAM of the router as well as the PC and to reset the current configuration to default (factory) settings.



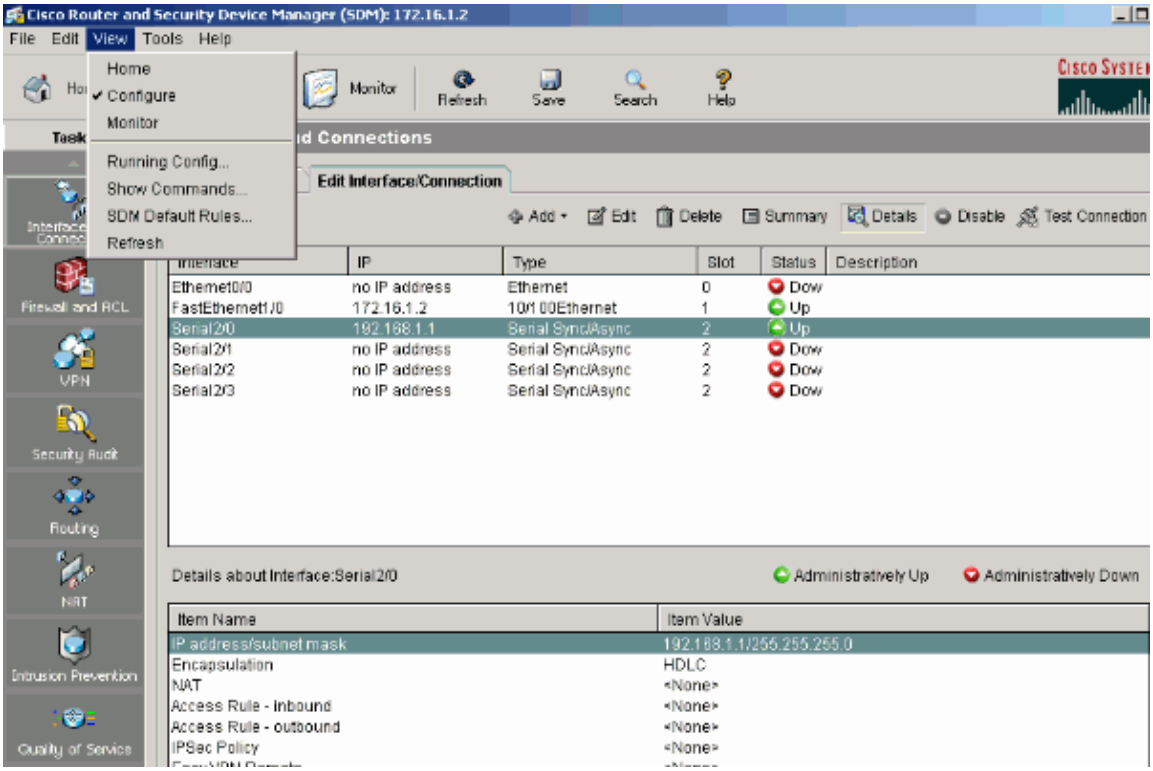
4. Go to the task bar and choose **Edit > Preferences** in order to enable these User Preferences options:

- ♦ Preview commands before delivering to router.
- ♦ Save signature file to Flash.
- ♦ Confirm before exiting from SDM.
- ♦ Continue monitoring interface status when switching mode/task.



5. Choose **View** from the task bar if you want to:

- ♦ View the Home, Configure, or Monitor pages.
- ♦ View the running configuration of the router.
- ♦ View various **show** commands.
- ♦ View SDM default rules.
- ♦ Choose **Refresh** in order to synchronize the router configuration if there are any configured through the CLI with SDM.



CLI Configuration

Router Configuration

```
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.

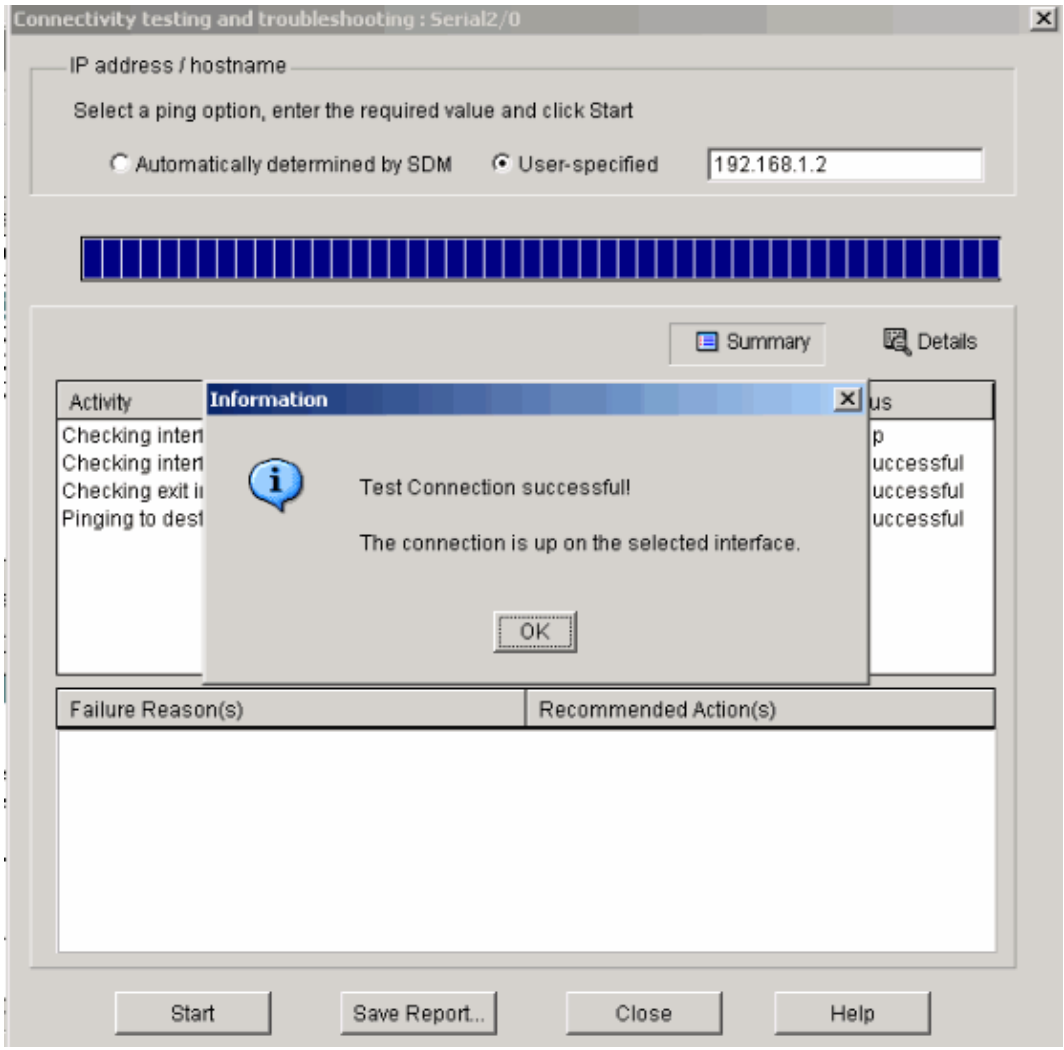
ip route 10.1.1.0 255.255.255.0 192.168.1.2
!
!
control-plane
!
!
!
!
!
!
!
!
!
!
line con 0
line aux 0

!--- Telnet enabled with password as sdmsdm.

line vty 0 4
 password sdmsdm
 login
!
!
end
```

Verify

Choose **Configure > Interface & Connections > Edit Interface Connections > Test Connection** in order to test the end-to-end connectivity. You can specify the remote end IP address if you click the **User-specified** radio button.



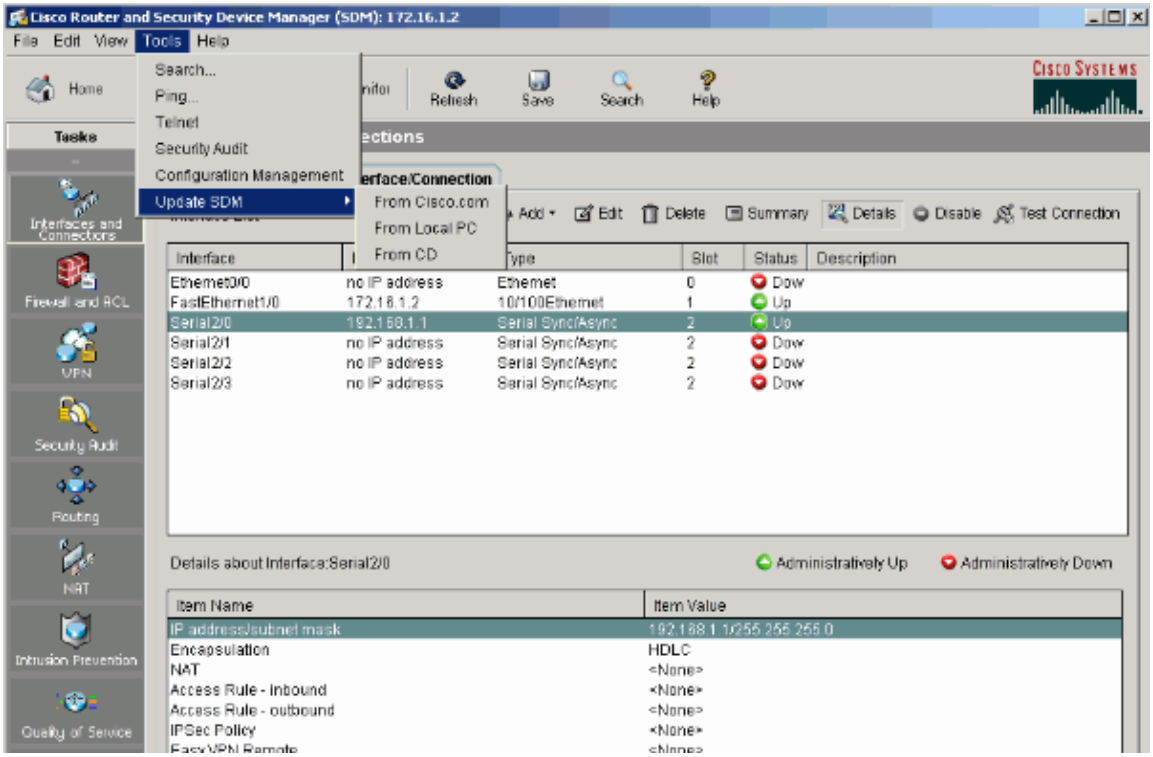
Troubleshoot

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

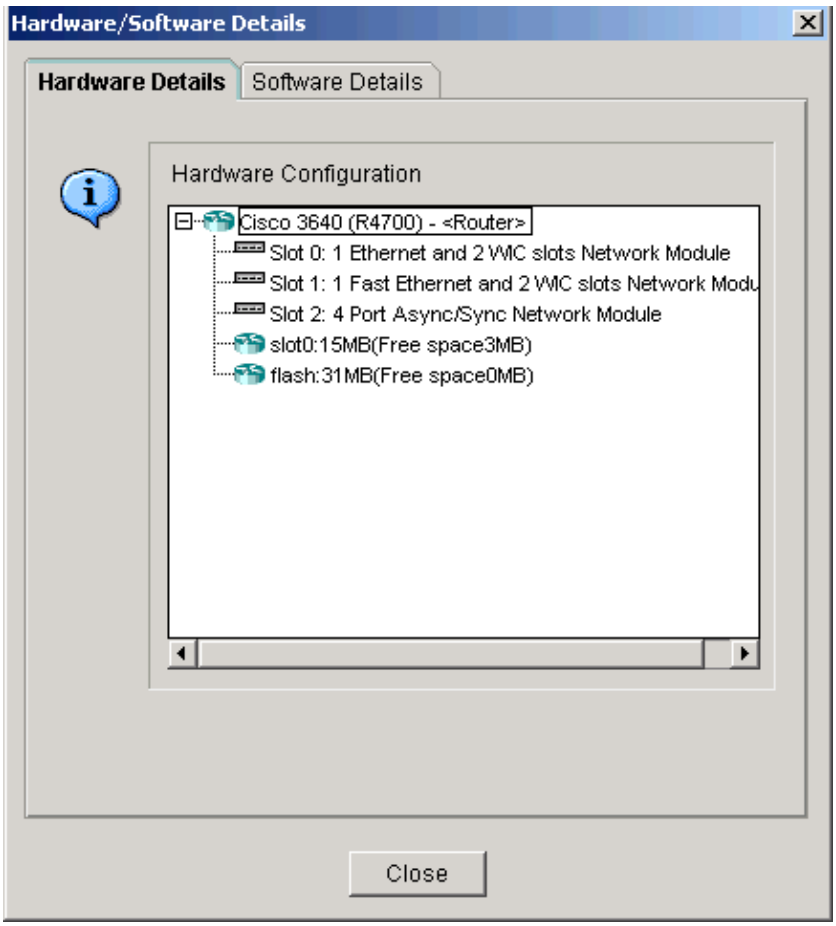
Note: Refer to Important Information on Debug Commands before you issue debug commands.

You can use these options in order to troubleshoot:

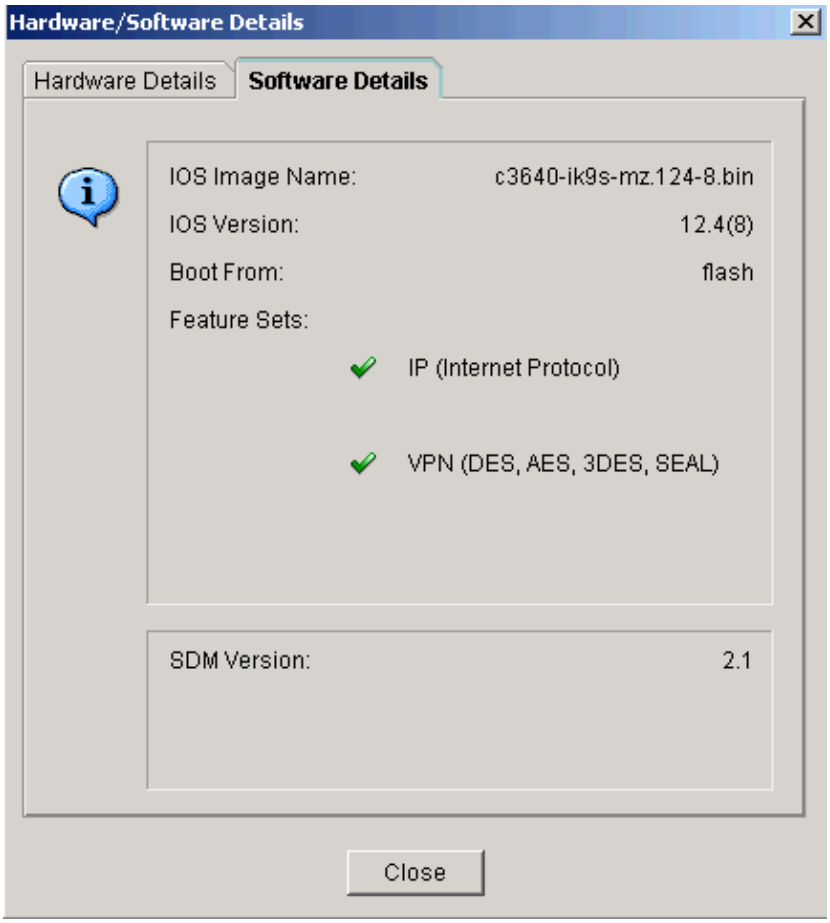
- Choose **Tools > Update SDM** from the task bar in order to ping, Telnet, and upgrade the SDM to the latest version. You can do this from Cisco.com, from the local PC, or from the CD.



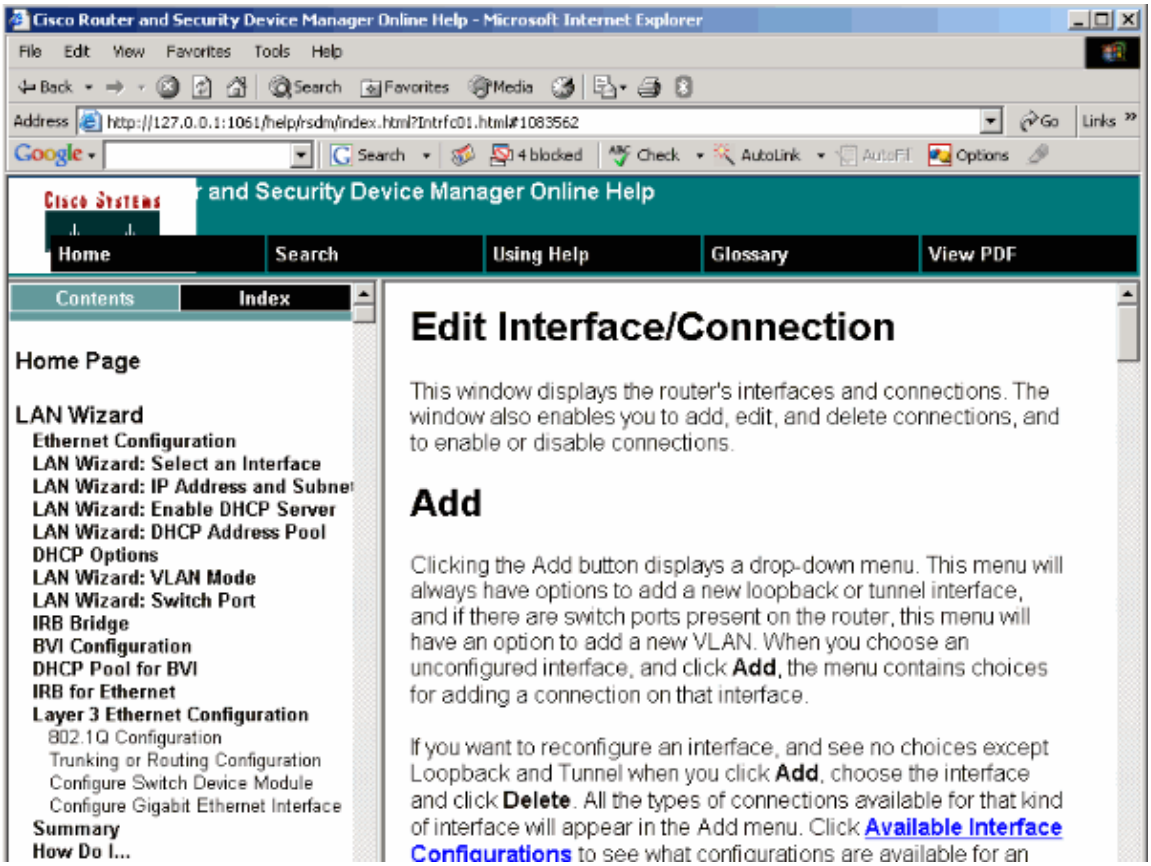
- Choose **Help > About this Router** in order to view information on the hardware configuration of the router.



This window shows information about the IOS image stored in the router.



- The **Help** option provides information about the various available options in the SDM for the configuration of routers.



Comatibility of SDM with 64-bit OS

SDM is not supported on machines with 64-bit OS. You should install SDM on the router and access it through the web browser.

Refer to Task 4: Install the SDM Files for more information on the installation of SDM files on the router.

Unable to Launch the SDM through Web Browser

Problem

When you use SDM through the web browser, an SDM start up error message appears.

Solution 1

The issue could be with the version of the Java. The Java update may not be compatible with the SDM version. If the version of Java is Java 6 update 12, then **uninstall that version and install Java 6 update 3**. This fixes the problem. Refer to the Web Browser Versions and Java Runtime Environment Versions section of SDM 2.5 Release Note for more information about the compatibility. SDM version 2.5 runs under updates 2 and 3 of Java version 6.

Solution 2

Enable **Allow active content to run in files on My Computer** in Internet Explorer options in order to resolve the issue.

1. Open Internet Explorer and choose**Tools > Internet Options > Advanced**.
2. Under the security section, make sure that the checkboxes next to the options **Allow active content to run in files on my computer** and **Allow active content to install software even if the signature is invalid** are checked.
3. Now click **OK** and restart the browser in order for the changes to take effect.

Error: java.bling stack overflow

Problem

I am unable to connect to the SDM, and I receive this error message:

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

Solution

This problem usually occurs when Java code version 1.5.0_06 is used. For information on how to resolve this issue, refer to The user is unable to connect to Security Device Manager (SDM) and receives the java.bling stack over flow error message.

Related Information

- **Cisco Security Device Manager Installation Guide**
- **Cisco Product Support Page - Routers**
- **Cisco Configuration Professional Support Page**
- **NAT Support Page**
- **Technical Support & Documentation - Cisco Systems**

Contacts & Feedback | Help | Site Map
© 2014 - 2015 Cisco Systems, Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems, Inc.

Updated: Jul 27, 2011 Document ID: 71305