



### Lab 3.2.3 Configure Basic Security using Security Device Manager (SDM)

#### Objective

In this lab, the students will complete the following tasks:

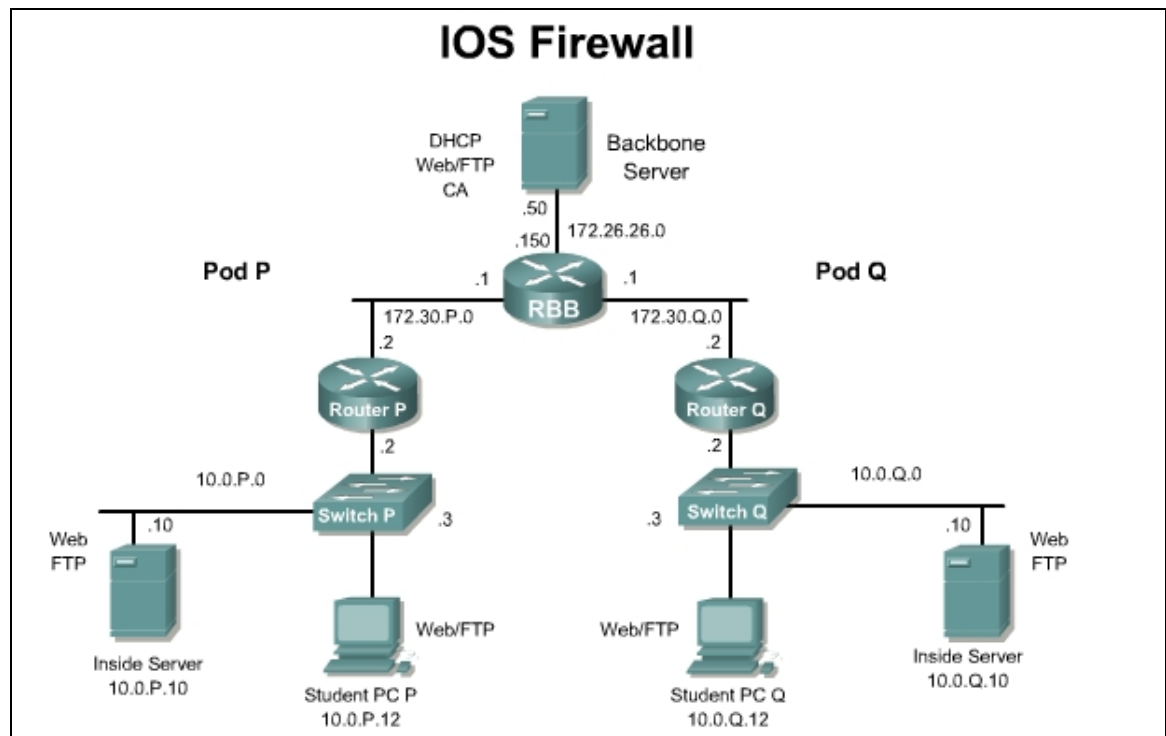
- Copy the SDM files to router Flash memory.
- Configure the router to support SDM.
- Configure a basic firewall.
- Reset a router interface.
- Configure PAT
- Create a banner.
- Configure secure management access

#### Scenario

Many SOHO and Small Business network administrators are not familiar or comfortable with the Cisco CLI. In this case, it is easier to use a GUI based tool to configure and monitor the router. Also, many experienced administrators are not familiar with security mechanisms and procedures which should be implemented on routers. SDM also uses an SSL encrypted session to secure the management traffic and prevent eavesdropping attacks.

## Topology

This figure illustrates the lab network environment.



## Preparation

Begin with the standard lab topology and verify the starting configuration on the pod router. Test the connectivity between the pod routers. Access the perimeter router console port using the terminal emulator on the Windows 2000 server. If desired, save the router configuration to a text file for later analysis. Refer back to the “*Student Lab Orientation*” if more help is needed.

## Tools and resources

In order to complete the lab, the following is required:

- Standard IOS Firewall lab topology
- Console cable
- HyperTerminal
- Java Virtual Machine. This is available for free from <http://www.java.sun.com/>.

## Additional materials

Further information regarding the objectives covered in this lab can be found at the following websites:

- <http://www.cisco.com/go/sdm>
- [http://www.cisco.com/en/US/products/sw/secursw/ps5318/prod\\_installation\\_guide09186a00803e4727.html](http://www.cisco.com/en/US/products/sw/secursw/ps5318/prod_installation_guide09186a00803e4727.html)
- [http://www.cisco.com/en/US/products/sw/secursw/ps5318/products\\_quick\\_start09186a00803f5bdf.html](http://www.cisco.com/en/US/products/sw/secursw/ps5318/products_quick_start09186a00803f5bdf.html)

## Command list

In this lab exercise, the following key commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
<code>ip http server</code>	Enable the Cisco Web browser user interface
<code>ip http secure-server</code>	Enable the Cisco Web secure browser user interface
<code>ip http authentication local</code>	Enable local authentication for Cisco Web browser user interface connections

### Step 1 Copy the SDM Files to Router Flash Memory if needed

Complete the following steps to copy the SDM files from the TFTP server to the Pod router flash memory (where **P** = pod number).

- Console into the pod router.
- Enter enable mode using a password of **cisco**.

```
RouterP> enable
Password: cisco
RouterP#
```

- Check the contents of flash memory.

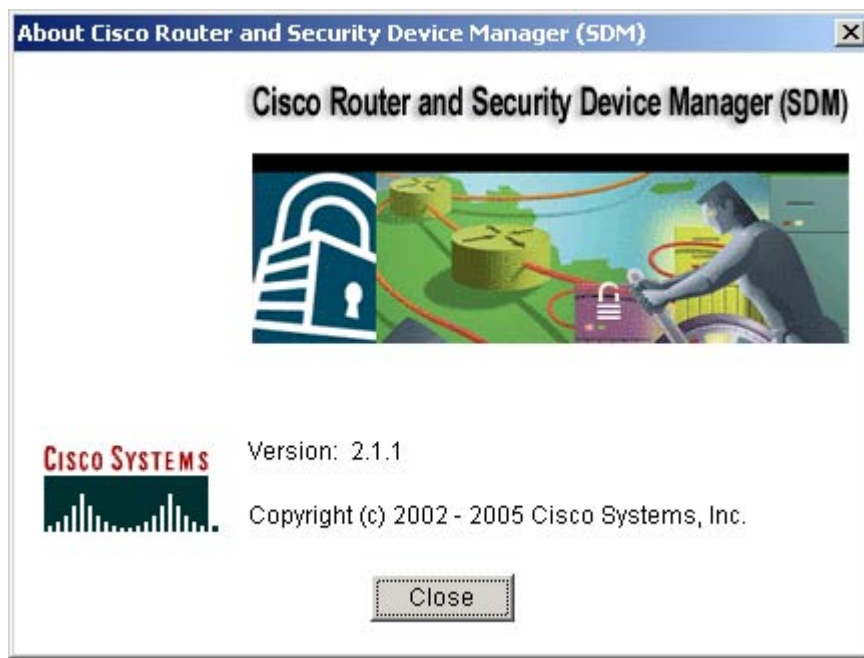
```
RouterP # show flash
System flash directory:
File      Length   Name/status
  1    16077820  c2600-advsecurityk9-mz.123-14.T1.bin
  2     1038    home.shtml
  3     1654    sdmconfig-26xx.cfg
  4    113152    home.tar
  5     820224    common.tar
  6    3085312    sdm.tar

[20099588 bytes used, 12930552 available, 33030140 total]
32768K bytes of processor board System flash (Read/Write)
```

**There are 2 options at this point:**

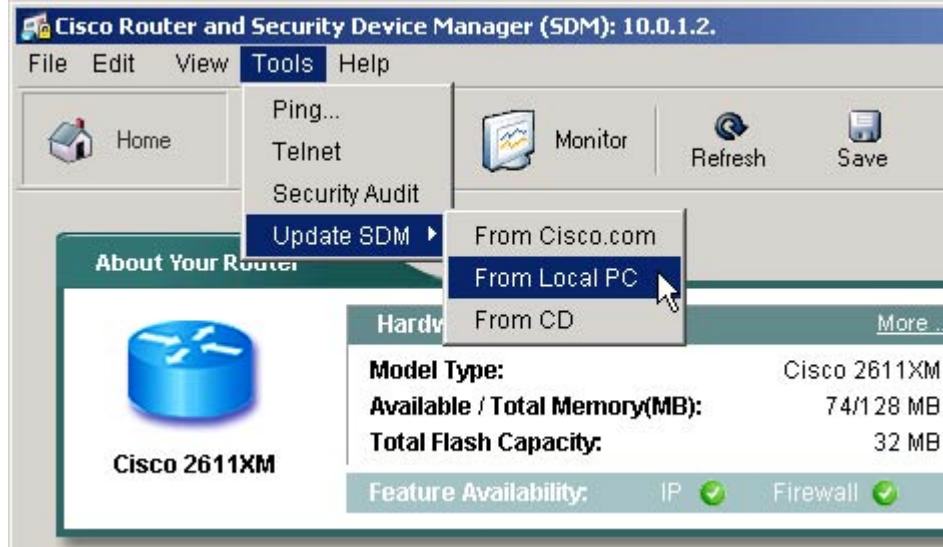
**Option 1:** If the files are not present, proceed to step d.

**Option 2:** If the files are present, proceed to Step 2 through Step 3. After step 3, go to **Help>About** to verify the version.



This course uses SDM version 2.1. Upgrade or downgrade as needed. The IOS image should also be a 12.3.(14) security image. The routers that are part of the standard course bundle ship with SDM installed by default.

- d. Check with the instructor before installing or upgrading SDM or follow the directions located at [http://www.cisco.com/en/US/products/sw/secursw/ps5318/prod\\_installation\\_guide09186a00803e4727.html](http://www.cisco.com/en/US/products/sw/secursw/ps5318/prod_installation_guide09186a00803e4727.html) to install, upgrade or downgrade SDM. A CCO login is required to obtain the needed SDM files. SDM can also be update from the SDM GUI interface.



Make sure all popup blockers have been disabled.

## Step 2 Configure the Router to Support SDM

Complete the following steps to configure the pod router to support SDM (where **P** = pod number).

- a. Enter global configuration mode using the `configure terminal` command.
 

```
RouterP# conf t
```
- b. Enable the Cisco Web browser user interface using the `ip http server` command.
 

```
RouterP(config)# ip http server
```

- c. Enable the Cisco Web secure browser user interface using the `ip http secure-server` command. RSA keys are generated and SSH is enabled when this command is entered.

```
RouterP(config)# ip http secure-server
```

- d. Enable local authentication for Cisco Web browser user interface connections using the `ip http authentication local` command.

```
RouterP(config)# ip http authentication local
```

- e. Create a local privilege level 15 user account for SDM Cisco Web browser user interface login authentication.

```
RouterP(config)# username sdm privilege 15 password 0 sdm
```

**Note:** Enter the command exactly as shown for this lab exercise only. Do not use a username/password combination of sdm/sdm on any production routers. Always use unique username/password combinations in production environments.

- f. Enter VTY line configuration mode using the `line vty` command.

```
RouterP(config)# line vty 0 4
RouterP(config-line)#
```

- g. Configure the VTY privilege level for level 15 using the privilege level command.

```
RouterP(config-line)# privilege level 15
```

- h. Configure VTY login for local authentication using the `login local` command.

```
RouterP(config-line)# login local
```

- i. Configure VTY to allow both Telnet and SSH connections using the `transport input` command.

```
RouterP(config-line)# transport input telnet ssh
RouterP(config-line)# end
```

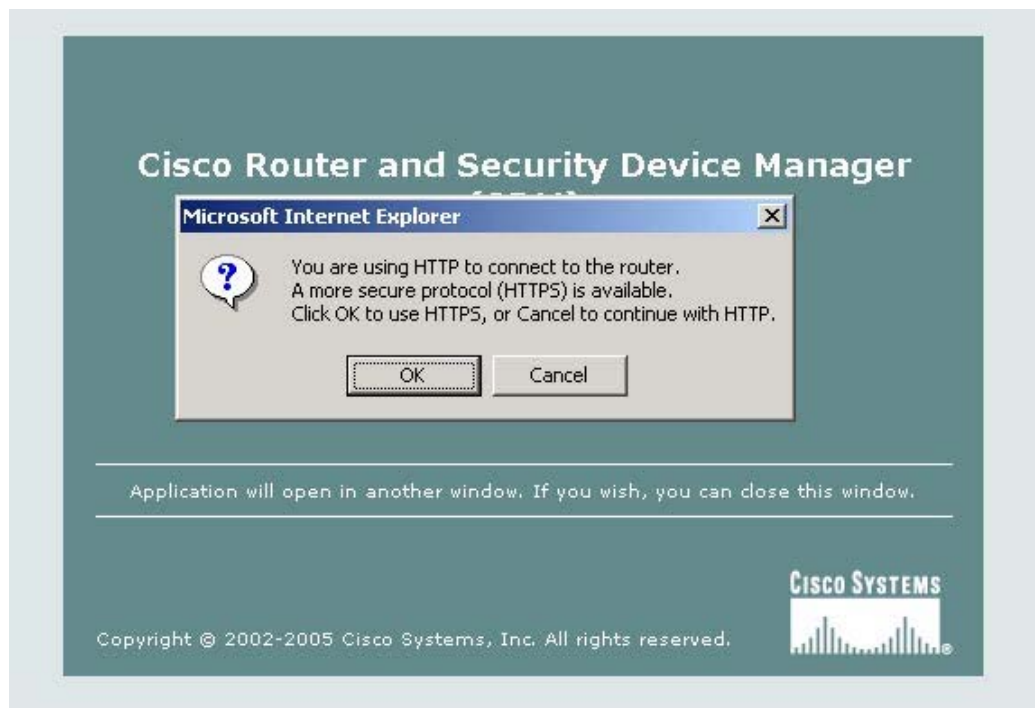
- j. Copy the router running configuration to the startup configuration.

```
RouterP# copy run start
RouterP#
```

### Step 3 Launch SDM

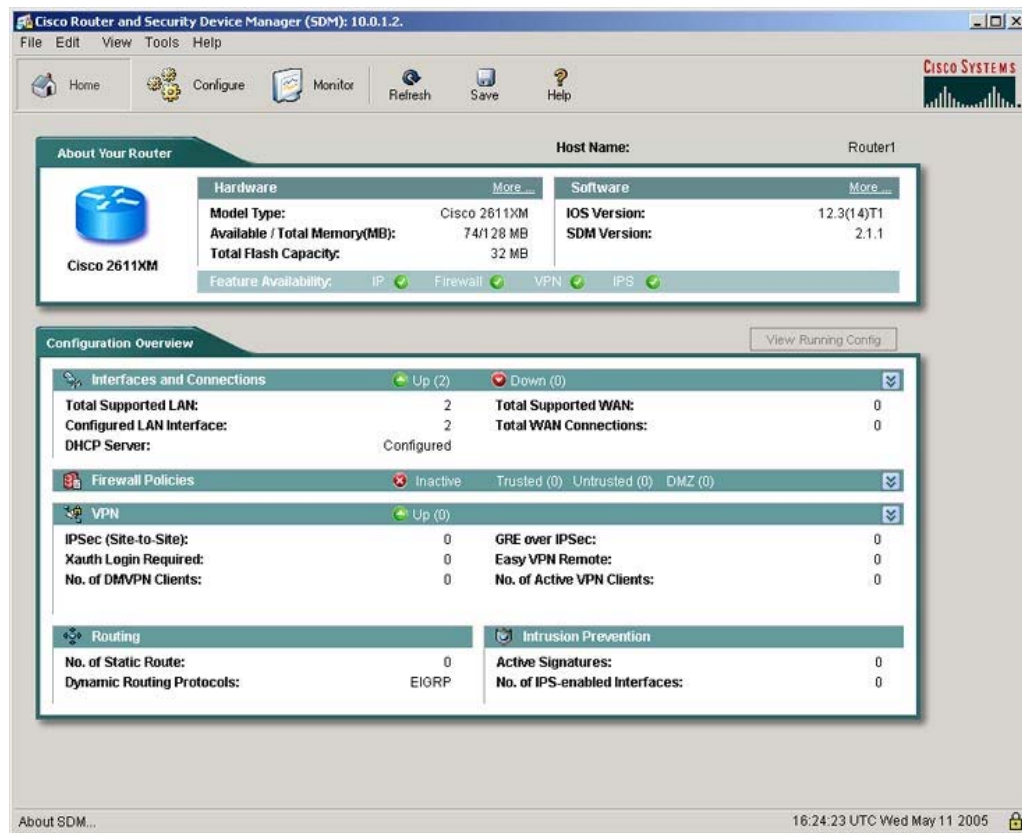
SDM is stored in the Flash memory of the router. It is launched by executing an HTML file, which then loads a signed SDM Java file. Complete the following steps to launch SDM.

- a. Open Internet Explorer on the student PC.
- b. Enter the following URL in the browser address field (where **P** = pod number).
- ```
http://10.0.P.2
```
- c. Enter the correct username "**sdm**" and password "**sdm**" in the Enter Network Password window.
- d. Notice that this is an insecure management session. Click on the **OK** button to enter into a HTTPS connection.



**Note:** Multiple security alert windows may appear when launching SDM. If a security alert window appears, review the message contained in the window, and click **Yes** to continue. A username and password prompt may also appear multiple times. Enter the correct username “**sdm**” and password “**sdm**” in the Enter Network Password window.

- e. Click **Yes** at the Security Warning window. The SDM window appears and the SDM loads the current configuration from the router.



- f. Notice the information provided in the **About Your Router** and **Configuration Overview** tabs.

1. What two categories are covered in the About Your Router section?

---

2. What version of IOS and SDM are installed?

---

3. What five categories are covered in the Configuration Overview section?

---

4. Is the Firewall Policies feature available? Active?

---

#### Step 4 Configure a Basic Firewall

Complete the following steps to configure a basic firewall on the Pod router.

- Click the **Configure** button along the top of the SDM interface to configure the router settings.
- Select **Firewall and ACL** from the category bar.



- Select **Basic Firewall**.

When should the Advanced firewall be used?

---

- Click **Launch the selected task**.
  - The Firewall Wizard screen appears. Click the **Next** button to begin the configuration.
  - For the outside (untrusted) interface, select the **FastEthernet0/1** Ethernet interface.
  - For the inside (trusted) interface, select the **FastEthernet0/0** interface.
  - Make sure the **Access rule log option** is checked.
  - A warning appears indicating that SDM cannot be launched from the FastEthernet0/1 interface after the Firewall Wizard is completed. Click the **OK** button to continue.
  - The Internet Firewall Configuration Summary screen appears. View the access rules that will be applied.
  - After viewing the configuration summary, click **Finish** to deliver the configuration to the router.
  - The Routing traffic configuration window appears. Make sure that **Allow EIGRP updates to come through the firewall** is checked, and then click **OK**.
1. Why are RIP and OSPF unavailable?

---



The Command Delivery status window appears. Verify the Configuration Delivery Status and click the **OK** button.

An Information widow appears. Click **OK** to proceed to the Firewall and ACL page.

Once complete, the new firewall appears in the Edit Firewall Policy / ACL tab in the Firewall and ACL page. Note the ACL rules that have been configured for both originating traffic and returning traffic.

**FastEthernet0/0 - inbound**

| Action | Source             | Destination | Service | Log | Option | Description |
|--------|--------------------|-------------|---------|-----|--------|-------------|
| Deny   | 172.30.1.0/0.0.0.2 | any         | IP      |     |        | ip          |
| Deny   | 255.255.255.255    | any         | IP      |     |        | ip          |
| Deny   | 127.0.0.0/0.255.2  | any         | IP      |     |        | ip          |
| Permit | any                | any         | IP      |     |        | ip          |

**FastEthernet0/1 - inbound**

| Action | Source             | Destination | Service | Log | Option | Description   |
|--------|--------------------|-------------|---------|-----|--------|---------------|
| Deny   | 10.0.1.0/0.0.0.255 | any         | IP      |     |        | ip            |
| Permit | any                | 172.30.1.2  | ICMP    |     |        | echo-reply    |
| Permit | any                | 172.30.1.2  | ICMP    |     |        | time-exceeded |
| Permit | any                | 172.30.1.2  | ICMP    |     |        | unreachable   |
| Permit | any                | any         | eigrp   |     |        |               |
| Deny   | 10.0.0.0/0.255.25  | any         | IP      |     |        | ip            |

- m. Resume a console connection with the router and verify that the configuration generated from the SDM tool is in the running configuration.

## Step 5 Reset a Router Interface

Complete the following steps to reset a router interface.

- a. Select **Interfaces and Connections** from the Tasks bar on the Configure page.
- b. Select the **Edit Interface/Connection** tab.
- c. Select the **172.30.P.2** interface (where **P** = pod number). The interface status should be up.
- d. Click **Disable**. Note how the status changes from up to down.
- e. Click **Enable**. The interface should come back up.



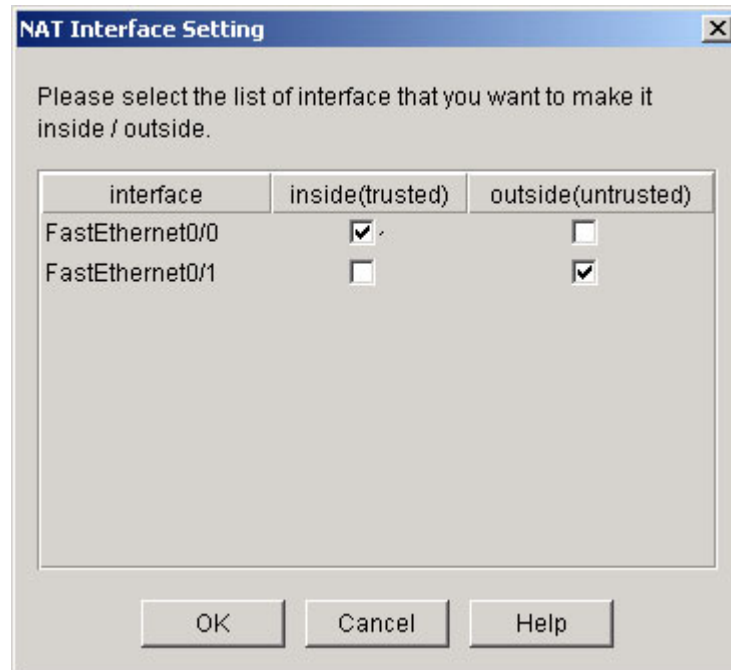
## Step 6 Configure PAT

Complete the following steps to configure NAT

- a. Select **NAT** from the Tasks bar on the Configure page.



- b. Click on the **Designate NAT Interfaces** button.



- c. Check the appropriate inside and outside interfaces
- d. Click the **OK** button. If the Command Delivery Status window appears, click the **OK** button on the window.
- e. Click on the **Add** button.
- f. Click on **Dynamic**. The direction should be **From inside to outside**.

**Add Address Translation Rule**

☐ Static
 ☒ **Dynamic**

Direction: From inside to outside

Translate from interface

Inside Interface(s): FastEthernet0/0

ACL Rule:  ...

Translate to interface

Outside Interface(s): FastEthernet0/1

Type: Interface

Interface: FastEthernet0/0

Address Pool:  ...

OK Cancel Help

- g. Click on the ACL rule button next to the **ACL Rule:** text field and click on **Create a new rule(ACL) and select...**
- h. Create and Extended ACL named ACL with a description of ACL for NAT.
- i. Click on the **Add** button and permit all IP traffic from the 10.0.P.0 network to any destination to be translated.

**Add an Extended Rule Entry**

Action: Select an action: **Permit**

Description:

Source Host/Network:

Type: **A Network**

IP Address: **10.0.1.0**

Wildcard Mask: **0.0.0.255**

(Mask bit 0 - Must match)  
(Mask bit 1 - Don't care)

Destination Host/Network:

Type: **Any IP Address**

Protocol and Service:

☒ TCP ☐ UDP ☐ ICMP ☒ IP

IP Protocol:

IP Protocol: **ip**

☐ Log matches against this entry

OK Cancel Help

- j. Click **OK** to return to the Add a Rule window.

**Add a Rule**

Name/Number: **ACL** Type: **Extended Rule**

Description: **ACL for NAT**

Rule Entry

**permit ip 10.0.1.0 0.0.0.255 any**

Add...  
Clone...  
Edit...  
Delete  
Move Up  
Move Down

Interface Association

None. Associate...

OK Cancel Help

- k. Click **OK** to return to the Add Address Translation Rule window.

**Add Address Translation Rule**

☐ Static ☒ Dynamic

Direction: From inside to outside

Translate from interface

Inside Interface(s): FastEthernet0/0

ACL Rule: ACL

Translate to interface

Outside Interface(s): FastEthernet0/1

Type: Interface

Interface: FastEthernet0/1

Address Pool:

OK Cancel Help

- l. Select **Interface** as the type of translation.
- m. Choose the outside interface of **FastEthernet0/1**
- n. Click the **OK** button. If the Command Delivery Status window appears, click the **OK** button on the window.

### Step 7 Create a Banner

Complete the following steps to create a banner to discourage unauthorized access.

- a. Select **Additional Tasks** from the Tasks bar on the Configure page.



- b. Select **Banner** under **Device Properties**.
- c. Click **Edit**.
- d. Enter a banner to discourage unauthorized access, and then click the **OK** button to apply the configuration. If the Command Delivery Status window appears, click the **OK** button on the window.

## Step 8 Management Access

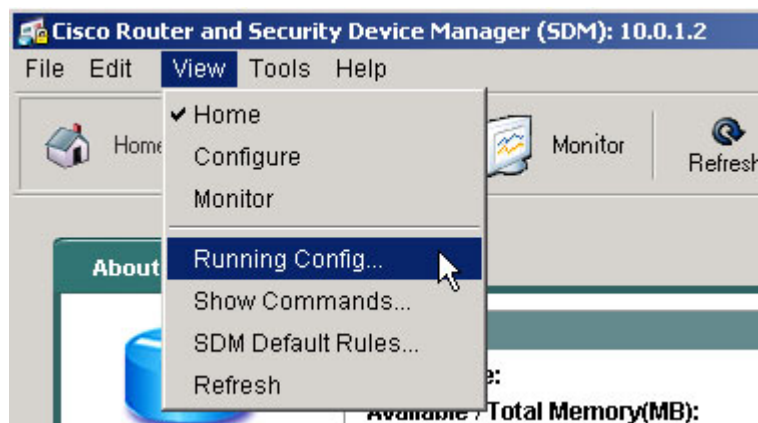
Complete the following steps to restrict management access to the router.

- a. Select **Additional Tasks** from the Tasks bar on the Configure page
  - b. Expand the **Router Access** menu and select **Management Access**.
  - c. Click the **Add** button.
  - d. Add the pod Host IP Address, 10.0.P.12.
  - e. Allow access from the FastEthernet0/0 interface
  - f. Check **Allow SDM**.
  - g. Check **Allow secure protocols only**.  
What protocols are removed?
- 
- h. Click **OK**.
  - i. A warning appears indicating that a Firewall is applied to the selected management interface. Click the **Yes** button to continue.
  - j. Click **Apply Changes**. If the Command Delivery Status window appears, click the **OK** button on the window.
  - k. Close the web browser and SDM. If prompted, click the Yes button to exit SDM. Open a new browser and enter **https://10.0.P.2** and reconnect to SDM. The browser refresh button may have to be used to reconnect as new keys are generated.

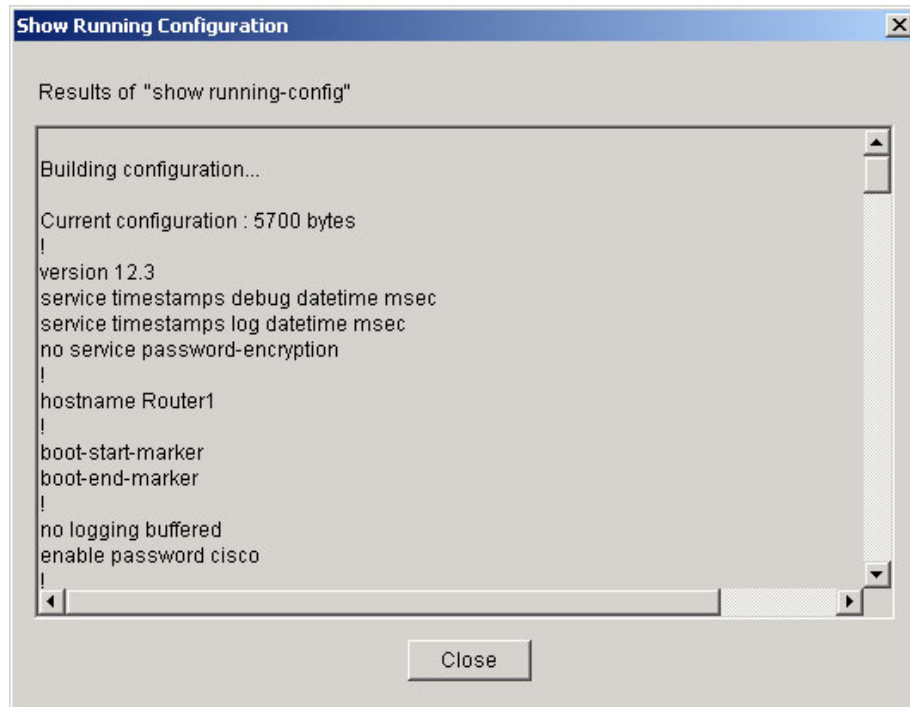
## Step 10 Verify the IOS Firewall configuration

Complete the following steps to verify the running configuration.

- a. In SDM, click on **View>Running Config...** from the top menu.



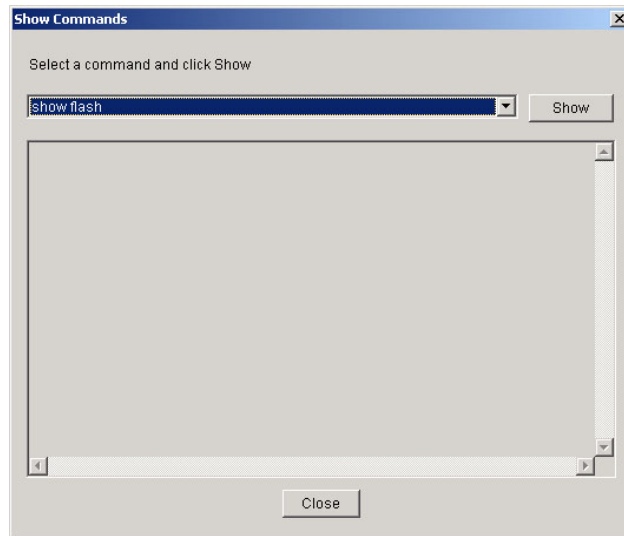
- b. The running configuration window will appear.



- c. Scroll through and verify the configuration. Click the **Close** button when finished.
- d. Next, click on **View>Show Commands...** from the top menu.



- e. The Show Commands window will appear.



What commands are available?

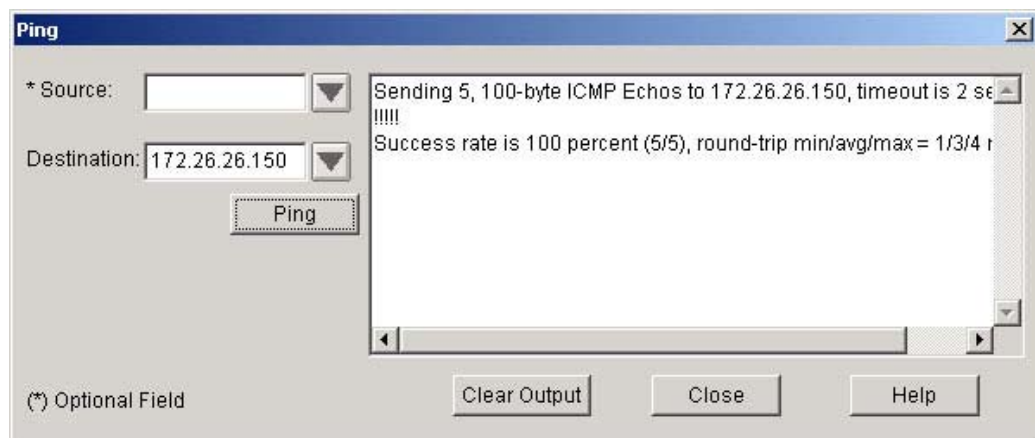
---

- f. Verify the Startup configuration using SDM. Click the **Close** button when finished.

### Step 11 Verify connectivity

Complete the following steps to verify connectivity.

- a. From the Student PC using SDM, ping RBB at 172.26.26.150. Click on **Tools>Ping** to access the ping window.



- b. Click on the **Clear Output** button.
- c. Ping the SW0 at 172.26.26.200. Click the **Close** button when finished.
- d. Open a web browser and connect to RBB.
- e. Next, try to access the pod router using https from an unauthorized address, such as the peer pod inside host.



- f. From the Student PC, try to access the pod router via telnet or http.

```
C:\ >telnet 10.0.P.2
```

```
C:\ >telnet 10.0.1.2
```

```
Connecting To 10.0.1.2...Could not open connection to the host, on  
port 23: Connect failed
```

Why is the connection refused?

- 
- g. From the student PC, telnet to RBB. Enter the password **cisco** when prompted. Use the **who** command in user mode to verify NAT operation and view the translated source address.

```
RBB>who
```

| Line       | User | Host(s) | Idle     | Location   |
|------------|------|---------|----------|------------|
| * 66 vty 0 |      | idle    | 00:00:00 | 172.30.1.2 |

| Interface<br>Address | User | Mode | Idle | Peer |
|----------------------|------|------|------|------|
|----------------------|------|------|------|------|

Notice that the 10.0.P.12 address is translated into a 172.30.P.2 address.