CCNA Security Lab Manual

Cisco Networking Academy

Cisco Press
800 East 96th Street
Indianapolis, Indiana 46240 USA

CCNA Security Lab Manual

Cisco Networking Academy

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Printed in the United States of America

First Printing August 2009

Library of Congress Cataloging-in-Publication Data available upon request.

ISBN-13: 978-1-58713-249-0
ISBN-10: 1-58713-249-4

Warning and Disclaimer

This book is designed to provide information about networking. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

This book is part of the Cisco Networking Academy® series from Cisco Press. The products in this series support and complement the Cisco Networking Academy curriculum. If you are using this book outside the Networking Academy, then you are not preparing with a Cisco trained and authorized Networking Academy provider.

For more information on the Cisco Networking Academy or to locate a Networking Academy, please visit www.cisco.com/edu.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher	**Paul Boger**
Associate Publisher	**Dave Dusthimer**
Cisco Representative	**Erik Ullanderson**
Cisco Press Program Manager	**Anand Sundaram**
Executive Editor	**Mary Beth Ray**
Managing Editor	**Patrick Kanouse**
Editorial Assistant	**Vanessa Evans**
Cover Designer	**Louisa Adair**
Proofreader	**Apostrophe Editing Services**

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Contents

About This Lab Manual

The only authorized Lab Manual for the Cisco Networking Academy CCNA Security course

The Cisco® Networking Academy® course on CCNA® Security provides a next step for students who want to expand their CCNA-level skill set to prepare for a career in network security. The CCNA Security course also prepares students for the Implementing Cisco IOS® Network Security (IINS) certification exam (640-553), which leads to the CCNA Security certification.

The CCNA Security Lab Manual provides you with all 11 labs from the course designed as hands-on practice to master the knowledge and skills needed to prepare for entry-level security specialist careers.

All the hands-on labs in the course can be completed on actual physical equipment or in conjunction with the NDG NETLAB+® solution. For current information on labs compatible with NETLAB+® go to http://www.netdevgroup.com/ae/labs.htm.

Through procedural, skills integration challenges, troubleshooting, and model building labs, this CCNA Security course aims to develop your in-depth understanding of network security principles as well as the tools and configurations used.

Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Chapter 1: Lab A: Researching Network Attacks and Security Audit Tools

Objectives

Part 1: Researching Network Attacks

- Research network attacks that have occurred.
- Select a network attack and develop a report for presentation to the class.

Part 2: Researching Security Audit Tools

- Research network security audit tools.
- Select a tool and develop a report for presentation to the class.

Background/Scenario

Network attacks have resulted in the loss of sensitive data and significant network downtime. When a network or the resources in it are inaccessible, worker productivity can suffer, and business income may be lost.

Attackers have developed many tools over the years to attack and compromise the networks of organizations. These attacks take many forms, but in most cases, they seek to obtain sensitive information, destroy resources, or deny legitimate users access to resources.

To understand how to defend a network against attacks, an administrator must first identify network vulnerabilities. Specialized security audit software developed by equipment and software manufacturers can be used to help identify potential weaknesses. In addition, the same tools used by attackers can be used to test the ability of a network to mitigate an attack. After the vulnerabilities are known, steps can be taken to help mitigate the network attacks.

This lab provides a structured research project that is divided into two parts: Researching Network Attacks and Researching Security Audit Tools. You can elect to perform Part 1, Part 2, or both. Let your instructor know what you plan to do so to ensure that a variety of network attacks and vulnerability tools are reported on by the members of the class.

In Part 1, you research various network attacks that have actually occurred. You select one of these and describe how the attack was perpetrated and how extensive the network outage or damage was. You also investigate how the attack could have been mitigated or what mitigation techniques might have been implemented to prevent future attacks. You prepare a report based on a predefined form included in the lab.

In Part 2, you research network security audit tools and investigate one that can be used to identify host or network device vulnerabilities. You create a one-page summary of the tool based on a predefined form included in the lab. You prepare a short (5–10 minute) presentation to present to the class.

You may work in teams of two with one person reporting on the network attack and the other reporting on the security audit tools. Each team member delivers a short overview (5–10 minutes) of their findings. You can use live demonstrations or PowerPoint to summarize your findings.

Required Resources

- Computer with Internet access for research.
- Presentation computer with PowerPoint or other presentation software installed.
- Video projector and screen for demonstrations and presentations.

Part 1. Researching Network Attacks

In Part 1 of this lab, you research various network attacks that have actually occurred and select one on which to report. Fill in the form below based on your findings.

Step 1: Research various network attacks.

List some of the attacks you identified in your search.

_____
_____
_____

Step 2: Fill in the following form for the network attack selected.

• **Name of attack:**	•
• **Type of attack:**	•
• **Dates of attacks:**	•
• **Computers/Organizations affected:**	•
• **How it works and what it did:**	

• **Mitigation options**:
• •
• **References and info links:**
• • •
• **Presentation support graphics (include PowerPoint filename or web links):**
• •

Part 2. Researching Security Audit Tools

In Part 2 of this lab, you research network security audit tools and attacker tools and investigate one that can be used to identify host or network device vulnerabilities. Fill in the report below based on your findings.

Step 1: Research various security audit and network attack tools.

List some of the tools that you identified in your search.

_____
_____
_____

Step 2: Fill in the following form for the security audit or network attack tool selected.

• **Name of tool:**	•
• **Developer:**	•
• **Type of tool (character-based or GUI):**	•
• **Used on (network device or computer host):**	•
• **Cost:**	•
• **Description of key features and capabilities of product or tool:**	
•	

•
•
•
•
•
•
•
•
•
• **References and info links:**
•
•
• **Presentation support graphics:**
•
•

Step 3: Reflection

a. What is the prevalence of network attacks and what is their impact on an organization's operation? What are some key steps organizations can take to help protect their networks and resources?

_____
_____
_____
_____
_____

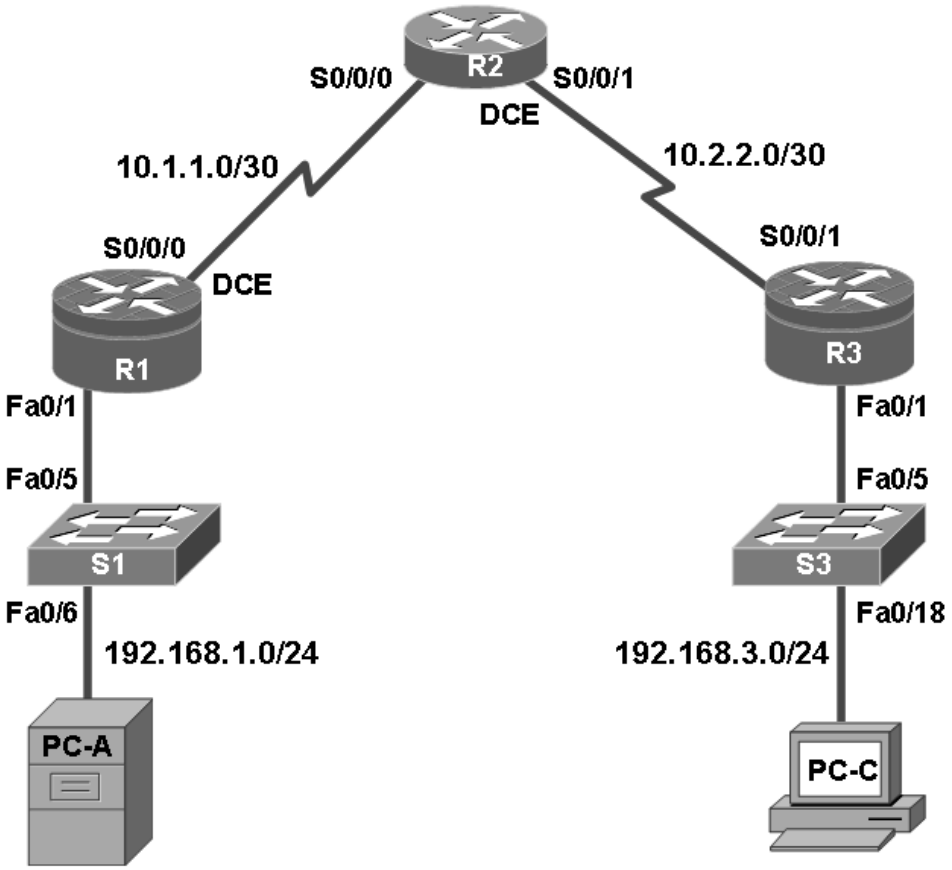
b. Have you actually worked for an organization or know of one where the network was compromised? If so, what was the impact to the organization and what did they do about it?

c. What steps can you take to protect your own PC or laptop computer?

_____
_____
_____

Chapter 2: Lab A: Securing the Router for Administrative Access

Topology



IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	FA0/1	192.168.1.1	255.255.255.0	N/A	S1 FA0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	FA0/1	192.168.3.1	255.255.255.0	N/A	S3 FA0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 FA0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 FA0/18

Objectives

Part 1: Basic Network Device Configuration

- Cable the network as shown in the topology.
- Configure basic IP addressing for routers and PCs.
- Configure static routing, including default routes.
- Verify connectivity between hosts and routers.

Part 2: Control Administrative Access for Routers

- Configure and encrypt all passwords.
- Configure a login warning banner.
- Configure enhanced username password security.
- Configure enhanced virtual login security.
- Configure an SSH server on a router.
- Configure an SSH client and verify connectivity.

Part 3: Configure Administrative Roles

- Create multiple role views and grant varying privileges.
- Verify and contrast views.

Part 4: Configure Cisco IOS Resilience and Management Reporting

- Secure the Cisco IOS image and configuration files.
- Configure a router as a synchronized time source for other devices using NTP.
- Configure Syslog support on a router.
- Install a Syslog server on a PC and enable it.
- Configure trap reporting on a router using SNMP.
- Make changes to the router and monitor syslog results on the PC.

Part 5: Configure Automated Security Features

- Lock down a router using AutoSecure and verify the configuration.
- Use the SDM Security Audit tool to identify vulnerabilities and lock down services.
- Contrast the AutoSecure configuration with SDM.

Background/Scenario

The router is a key component that controls the movement of data into and out of the network and between devices within the network. It is particularly important to protect the network routers because the failure of one of these devices due to malicious activity could make sections of the network or the entire network inaccessible. Controlling access to routers and enabling reporting on routers are critical to network security and should be part of a comprehensive security policy.

In this lab, you build a multi-router network and configure the routers and hosts. You use various CLI and SDM tools to secure local and remote access to the routers, analyze potential vulnerabilities, and take steps to mitigate them. You also enable management reporting to monitor router configuration changes.

The router commands and output in this lab are from Cisco 1841s using Cisco IOS software, release 12.4(20)T (advanced IP image). Other routers and Cisco IOS versions can be used. See the Router Interface Summary table at the end of the lab to determine which interface identifiers to use based on the equipment in

the lab. Depending on the model of the router, the commands available and output produced may vary from what is shown in this lab.

Note: Make sure that the routers and the switches have been erased and have no startup configurations.

Required Resources

- 3 routers with SDM 2.5 installed (Cisco 1841 with Cisco IOS software, release 12.4(20)T1 or comparable)
- 2 switches (Cisco 2960 or comparable)
- PC-A: Windows XP, Vista, or Windows Server with PuTTy SSH Client (no ACS required for this lab)
- PC-C: Windows XP or Vista with PuTTy SSH Client and Kiwi or Tftpd32 Syslog server
- Serial and Ethernet cables as shown in the topology
- Rollover cables to configure the routers via the console port

Part 1. Basic Router Configuration

In Part 1 of this lab, you set up the network topology and configure basic settings such as interface IP addresses and static routing.

Step 1: Cable the network.

Attach the devices shown in the topology diagram and cable as necessary.

Step 2: Configure basic settings for each router.

a. Configure host names as shown in the topology.

b. Configure interface IP addresses as shown in the IP Addressing Table.

c. Configure a clock rate for routers with a DCE serial cable attached to their serial interface. Router R1 is shown here as an example.

```
R1(config)#interface S0/0/0
R1(config-if)#clock rate 64000
```

d. To prevent the router from attempting to translate incorrectly entered commands as though they were host names, disable DNS lookup. Router R1 is shown here as an example.

```
R1(config)#no ip domain-lookup
```

Step 3: Configure static routing on the routers.

a. Configure a static default route from R1 to R2 and from R3 to R2.

b. Configure a static route from R2 to the R1 LAN and from R2 to the R3 LAN.

Step 4: Configure PC host IP settings.

Configure a static IP address, subnet mask, and default gateway for PC-A and PC-C as shown in the IP Addressing Table.

Step 5: Verify connectivity between PC-A and R3.

a. Ping from R1 to R3.

Were the ping results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

b. Ping from PC-A on the R1 LAN to PC-C on the R3 LAN.

Were the ping results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Note: If you can ping from PC-A to PC-C you have demonstrated that static routing is configured and functioning correctly. If you cannot ping but the device interfaces are up and IP addresses are correct, use the **`show run`** and **`show ip route`** commands to help identify routing protocol related problems.

Step 6: Save the basic running configuration for each router.

Use the **Transfer > Capture text** option in HyperTerminal or some other method to capture the running configs for each router. Save the three files so that they can be used to restore configs later in the lab.

Part 2. Control Administrative Access for Routers

In Part 2 of this lab, you will:

- Configure and encrypt passwords.
- Configure a login warning banner.
- Configure enhanced username password security.
- Configure enhanced virtual login security.
- Configure an SSH server on router R1 using the CLI.
- Research terminal emulation client software and configure the SSH client.

Note: Perform all tasks, on both R1 and R3. The procedures and output for R1 are shown here.

Task 1. Configure and Encrypt Passwords on Routers R1 and R3

Step 1: Configure a minimum password length for all router passwords.

Use the **`security passwords`** command to set a minimum password length of 10 characters.

```
R1(config)#security passwords min-length 10
```

Step 2: Configure the enable secret password.

Configure the enable secret encrypted password on both routers.

```
R1(config)#enable secret cisco12345
```

How does configuring an enable secret password help protect a router from being compromised by an attack?

_____
_____
_____

Step 3: Configure basic console, auxiliary port, and virtual access lines.

Note: Passwords in this task are set to a minimum of 10 characters but are relatively simple for the benefit of performing the lab. More complex passwords are recommended in a production network.

a. Configure a console password and enable login for routers. For additional security, the **exec-timeout** command causes the line to log out after 5 minutes of inactivity. The **logging synchronous** command prevents console messages from interrupting command entry.

Note: To avoid repetitive logins during this lab, the **exec-timeout** command can be set to 0 0, which prevents it from expiring. However, this is not considered a good security practice.

```
R1(config)#line console 0
R1(config-line)#password ciscocon
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
R1(config-line)#logging synchronous
```

When you configured the password for the console line, what message was displayed?

_____

b. Configure a new password of **ciscoconpass** for the console.

c. Configure a password for the AUX port for router R1.

```
R1(config)#line aux 0
R1(config-line)#password ciscoauxpass
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
```

d. Telnet from R2 to R1.

```
R2>telnet 10.1.1.1
```

Were you able to login? Why or why not? _____

What messages were displayed?

_____
_____
_____

e. Configure the password on the vty lines for router R1.

```
R1(config)#line vty 0 4
R1(config-line)#password ciscovtypass
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
```

f. Telnet from R2 to R1 again. Were you able to login this time? _____

g. Enter privileged EXEC mode and issue the show run command. Can you read the enable secret password? Why or why not? _____

Can you read the console, aux, and vty passwords? Why or why not? _____

h. Repeat the configuration portion of steps 3a through 3g on router R3.

Step 4: Encrypt clear text passwords.

a. Use the **service password-encryption** command to encrypt the console, aux, and vty passwords.

```
R1(config)# service password-encryption
```

b. Issue the **show run** command. Can you read the console, aux, and vty passwords? Why or why not? _____

c. At what level (number) is the enable secret password encrypted? _____

d. At what level (number) are the other passwords encrypted? _____

e. Which level of encryption is harder to crack and why? _____

Task 2. Configure a Login Warning Banner on Routers R1 and R3

Step 1: Configure a warning message to display prior to login.

a. Configure a warning to unauthorized users with a message-of-the-day (MOTD) banner using the **banner motd** command. When a user connects to one of the routers, the MOTD banner appears before the login prompt. In this example, the dollar sign ($) is used to start and end the message.

```
R1(config)#banner motd $Unauthorized access strictly prohibited and
prosecuted to the full extent of the law$
R1(config)#exit
```

b. Issue the **show run** command. What does the $ convert to in the output? _____

c. Exit privileged EXEC mode using the **disable** or **exit** command and press **Enter** to get started. Does the MOTD banner look like what you created with the **banner motd** command? _____

Note: If the MOTD banner is not as you wanted it, recreate it using the **banner motd** command.

Task 3. Configure Enhanced Username Password Security on Routers R1 and R3.

Step 1: Investigate the options for the username command.

In global configuration mode, enter the following command:

```
R1(config)#username user01 password ?
```

What options are available?

_____
_____
_____

Step 2: Create a new user account using the username command.

a. Create the user01 account, specifying the password with no encryption.

```
R1(config)#username user01 password 0 user01pass
```

b. Use the **show run** command to display the running configuration and check the password that is enabled.

You still cannot read the password for the new user account. Even though unencrypted (0) was specified because the **service password-encryption** command is in effect.

Step 3: Create a new user account with a secret password.

a. Create a new user account with MD5 hashing to encrypt the password.

```
R1(config)#username user02 secret user02pass
```

b. Exit global configuration mode and save your configuration.

c. Display the running configuration. Which hashing method is used for the password?

Step 4: Test the new account by logging in to the console.

a. Set the console line to use the locally defined login accounts.

```
R1(config)#line console 0
R1(config-line)#login local
R1(config-line)#end
R1#exit
```

b. Exit to the initial router screen which displays: **R1 con0 is now available, Press RETURN to get started.**

c. Log in using the user01 account and password previously defined.

What is the difference between logging in at the console now and previously?

_____

d. After logging in, issue the **show run** command. Were you able to issue the command? Why or why not?

_____

e. Enter privileged EXEC mode using the **enable** command. Were you prompted for a password? Why or why not? _____

Step 5: Test the new account by logging in from a Telnet session.

a. From PC-A, establish a Telnet session with R1.

```
PC-A>telnet 192.168.1.1
```

Were you prompted for a user account? Why or why not? _____

b. Set the vty lines to use the locally defined login accounts.

```
R1(config)#line vty 0 4
R1(config-line)#login local
```

c. From PC-A, telnet to R1 again.

```
PC-A>telnet 192.168.1.1
```

Were you prompted for a user account? Why or why not? _____

d. Log in as user01 with a password of user01pass.

e. While telnetted to R1, access privileged EXEC mode with the **enable** command.

What password did you use? _____

f. For added security, set the AUX port to use the locally defined login accounts.

```
R1(config)#line aux 0
R1(config-line)#login local
```

g. End the Telnet session with the **exit** command.

Task 4. Configure Enhanced Virtual Login Security on Routers R1 and R3

Step 1: Configure the router to watch for login attacks.

Use the **login block-for** command to help prevent brute-force login attempts from a virtual connection, such as Telnet, SSH, or HTTP. This can help slow down dictionary attacks and help protect the router from a possible DoS attack.

a. From the user EXEC or privileged EXEC prompt, issue the **show login** command to see the current router login attack settings.

```
R1#show login
   No login delay has been applied.
   No Quiet-Mode access list has been configured.
   Router NOT enabled to watch for login Attacks
```

b. Use the **login block-for** command to configure a 60 second login shutdown (quiet mode timer) if two failed login attempts are made within 30 seconds.

```
R1(config)#login block-for 60 attempts 2 within 30
```

c. Exit global configuration mode and issue the **show login** command.

```
R1#show login
```

Is the router enabled to watch for login attacks? _____

What is the default login delay? _____

Step 2: Configure the router to log login activity.

a. Configure the router to generate system logging messages for both successful and failed login attempts. The following commands log every successful login and log failed login attempts after every second failed login.

```
R1(config)#login on-success log
R1(config)#login on-failure log every 2
R1(config)#exit
```

b. Issue the **show login** command. What additional information is displayed?

_____

Step 3: Test the enhanced login security login configuration.

a. From PC-A, establish a Telnet session with R1.

```
PC-A> telnet 10.1.1.1
```

b. Attempt to log in with the wrong user ID or password two times. What message was displayed on PC-A after the second failed attempt? _____

What message was displayed on the router R1 console after the second failed login attempt?

c. From PC-A, attempt to establish another Telnet session to R1 within 60 seconds. What message was displayed on PC-A after the attempted Telnet connection?

_____

What message was displayed on router R1 after the attempted Telnet connection?

d. Issue the **show login** command within 60 seconds. What additional information is displayed?

_____

Task 5. Configure the SSH Server on Router R1 and R3 Using the CLI

In this task, you use the CLI to configure the router to be managed securely using SSH instead of Telnet. Secure Shell (SSH) is a network protocol that establishes a secure terminal emulation connection to a router or other networking device. SSH encrypts all information that passes over the network link and provides authentication of the remote computer. SSH is rapidly replacing Telnet as the remote login tool of choice for network professionals.

Note: For a router to support SSH, it must be configured with local authentication, (AAA services, or username) or password authentication. In this task, you configure an SSH username and local authentication.

Step 1: Configure a domain name.

Enter global configuration mode and set the domain name.

```
R1#conf t
R1(config)#ip domain-name ccnasecurity.com
```

Step 2: Configure a privileged user for login from the SSH client.

a. Use the **username** command to create the user ID with the highest possible privilege level and a secret password.

```
R1(config)#username admin privilege 15 secret cisco12345
```

b. Exit to the initial router login screen, and log in with this username. What was the router prompt after you entered the password? _____

Step 3: Configure the incoming vty lines.

Specify a privilege level of 15 so that a user with the highest privilege level (15) will default to privileged EXEC mode when accessing the vty lines. Other users will default to user EXEC mode. Use the local user accounts for mandatory login and validation, and accept only SSH connections.

```
R1(config)#line vty 0 4
R1(config-line)#privilege level 15
```

```
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#exit
```

Note: The **login local** command should already be configured in a previous step. It is included here to provide all commands if you were doing this for the first time.

Note: If you add the keyword **telnet** to the **transport input** command, users can log in using Telnet as well as SSH, however, the router will be less secure. If only SSH is specified, the connecting host must have an SSH client installed.

Step 4: Erase existing key pairs on the router.

```
R1(config)#crypto key zeroize rsa
```

Note: If no keys exist, you might receive this message: `% No Signature RSA Keys found in configuration.`

Step 5: Generate the RSA encryption key pair for the router.

The router uses the RSA key pair for authentication and encryption of transmitted SSH data.

Configure the RSA keys with 1024 for the number of modulus bits. The default is 512, and the range is from 360 to 2048.

```
R1(config)#crypto key generate rsa general-keys modulus 1024
R1(config)#exit

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R1(config)#
*Dec 16 21:24:16.175: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Note: The details of encryption methods are covered in Chapter 7.

Step 6: Verify the SSH configuration.

a. Use the **show ip ssh** command to see the current settings.

```
R1#show ip ssh
```

b. Fill in the following information based on the output of the **show ip ssh** command.

SSH version enabled: _____
Authentication timeout: _____
Authentication retries: _____

Step 7: Configure SSH timeouts and authentication parameters.

The default SSH timeouts and authentication parameters can be altered to be more restrictive using the following commands.

```
R1(config)#ip ssh time-out 90
R1(config)#ip ssh authentication-retries 2
```

Step 8: Save the running-config to the startup-config.

```
R1#copy running-config startup-config
```

Task 6. Research Terminal Emulation Client Software and Configure the SSH Client

Step 1: Research terminal emulation client software.

Conduct a web search for freeware terminal emulation client software, such as TeraTerm or PuTTy. What are some capabilities of each?

_____
_____
_____

Step 2: Install an SSH client on PC-A and PC-C.

a. If the SSH client is not already installed, download either TeraTerm or PuTTY.

b. Save the application to the desktop.

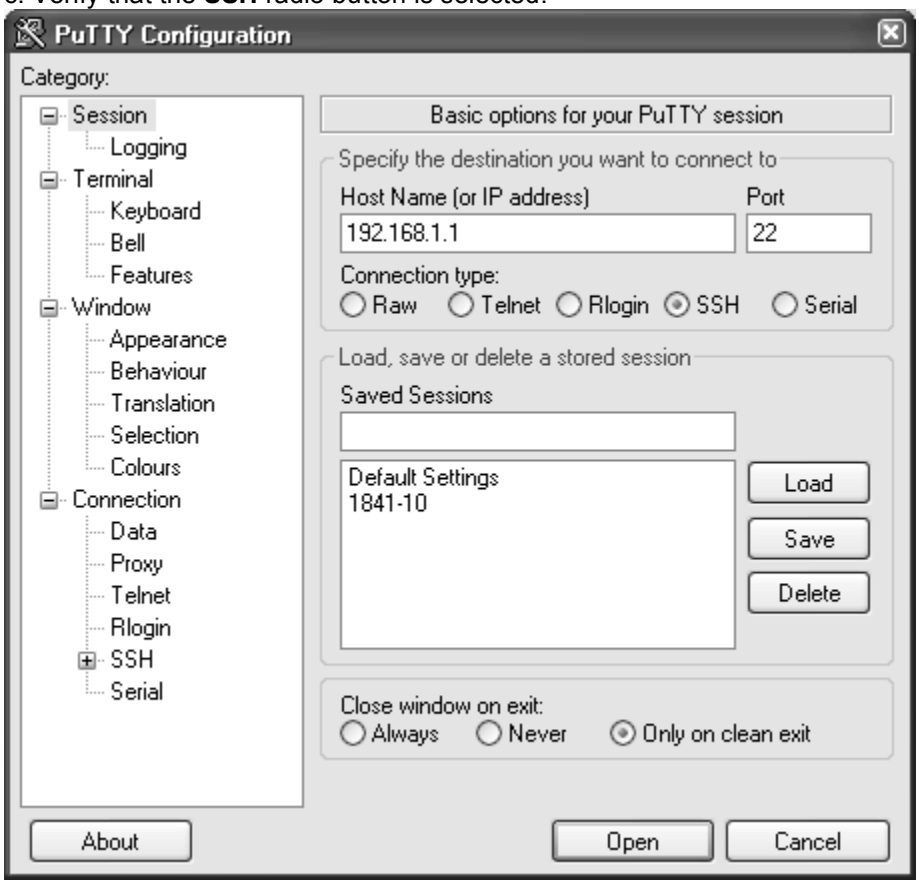
Note: The procedure described here is for PuTTY and pertains to PC-A.

Step 3: Verify SSH connectivity to R1 from PC-A.

a. Launch PuTTY by double-clicking the putty.exe icon.

b. Input the R1 Fa0/1 IP address 192.168.1.1 in the **Host Name or IP address** field.

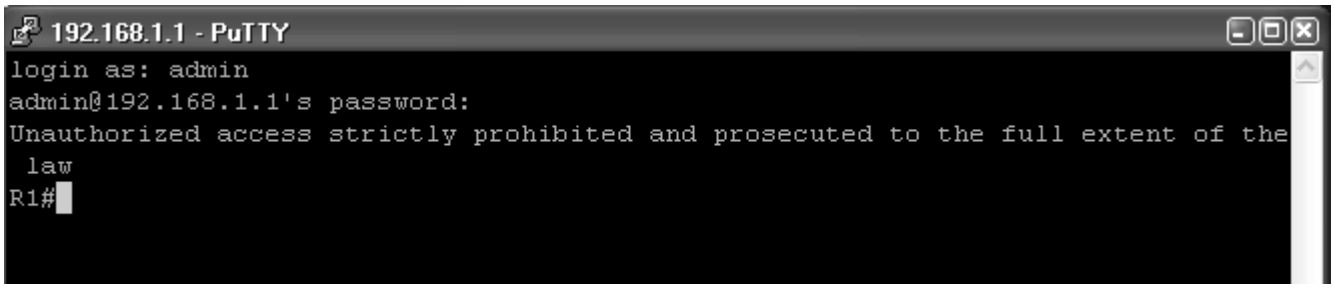
c. Verify that the **SSH** radio button is selected.



d. Click **Open**.

e. In the PuTTY Security Alert window, click **Yes**.

f. Enter the admin username and password cisco12345 in the PuTTY window.



g. At the R1 privileged EXEC prompt, enter the **show users** command.

```
R1#show users
```

What users are connected to router R1 at this time?

_____

h. Close the PuTTY SSH session window.

i. Try to open a Telnet session to your router from PC-A. Were you able to open the Telnet session? Why or why not?

_____

j. Open a PuTTY SSH session to the router from PC-A. Enter the user01 username and password user01pass in the PuTTY window to try connecting for user who does not have privilege level of 15. Were you able to login? _____ What was the prompt? _____

k. Use the **enable** command to enter privilege EXEC mode and enter the enable secret password **cisco12345**.

l. Disable the generation of system logging messages for successful login attempts.

```
R1(config)#no login on-success log
```

Step 4: Save the configuration.

Save the running configuration to the startup configuration from the privileged EXEC prompt.

```
R1#copy running-config startup-config
```

Part 3. Configure Administrative Roles

In Part 3 of this lab, you will:

- Create multiple administrative roles or views on routers R1 and R3.
- Grant each view varying privileges.
- Verify and contrast the views.

The role-based CLI access feature allows the network administrator to define views, which are a set of operational commands and configuration capabilities that provide selective or partial access to Cisco IOS EXEC and configuration (config) mode commands. Views restrict user access to the Cisco IOS CLI and configuration information. A view can define which commands are accepted and what configuration information is visible.

Note: Perform all tasks on both R1 and R3. The procedures and output for R1 are shown here.

Task 1. Enable Root View on R1 and R3

If an administrator wants to configure another view to the system, the system must be in root view. When a system is in root view, the user has the same access privileges as a user who has level-15 privileges, but the root view user can also configure a new view and add or remove commands from the view. When you are in a CLI view, you have access only to the commands that have been added to that view by the root view user.

Step 1: Enable AAA on router R1.

To define views, AAA must be enabled.

```
R1#config t
R1(config)#aaa new-model
R1(config)#exit
```

Note: AAA is covered in Chapter 3.

Step 2: Enable the root view.

Use the command **enable view** to enable the root view. Use the enable secret password **cisco12345**. If the router does not have an enable secret password, create one now.

```
R1# enable view
Password: cisco12345
*Dec 16 22:41:17.483: %PARSER-6-VIEW_SWITCH: successfully set to view
'root'.
```

Task 2. Create New Views for the Admin1, Admin2, and Tech Roles on R1 and R3

Step 1: Create the admin1 view, establish a password, and assign privileges.

a. The admin1 user is the top-level user below root that is allowed to access this router. It has the most authority. The admin1 user can use all show, config, and debug commands. Use the following command to create the admin1 view while in the root view.

```
R1(config)#parser view admin1
R1(config-view)#
*Dec 16 22:45:27.587: %PARSER-6-VIEW_CREATED: view 'admin1'
successfully created.
<ENTER>
```

Note: To delete a view, use the command **no parser view** *viewname.*

b. Associate the admin1 view with an encrypted password.

```
R1(config-view)#secret admin1pass
R1(config-view)#
```

c. Review the commands that can be configured in the admin1 view. Use the **commands ?** command. The following is a partial listing of the available commands.

```
R1(config-view)#commands ?
  RITE-profile           Router IP traffic export profile command mode
  RMI Node Config        Resource Policy Node Config mode
  RMI Resource Group     Resource Group Config mode
  RMI Resource Manager   Resource Manager Config mode
  RMI Resource Policy    Resource Policy Config mode
  SASL-profile           SASL profile configuration mode
  aaa-attr-list          AAA attribute list config mode
  aaa-user               AAA user definition
  accept-dialin          VPDN group accept dialin configuration mode
  accept-dialout         VPDN group accept dialout configuration mode
  address-family         Address Family configuration mode
<output omitted>
```

d. Add all config, **show**, and **debug** commands to the admin1 view and then exit from view configuration mode.

```
R1(config-view)#commands exec include all show
R1(config-view)#commands exec include all config terminal
R1(config-view)#commands exec include all debug
R1(config-view)#end
```

e. Verify the admin1 view.

```
R1#enable view admin1
Password:admin1pass
```

```
*Dec 16 22:56:46.971: %PARSER-6-VIEW_SWITCH: successfully set to view
'admin1'

R1#show parser view
R1#Current view is 'admin1'
```

f. Examine the commands available in the admin1 view.

```
R1#?
Exec commands:
  configure  Enter configuration mode
  debug      Debugging functions (see also 'undebug')
  enable     Turn on privileged commands
  exit       Exit from the EXEC
  show       Show running system information
```

g. Examine the **show** commands available in the admin1 view.

```
R1#show ?
  aaa           Show AAA values
  accounting    Accounting data for active sessions
  adjacency     Adjacent nodes
  alignment     Show alignment information
  appfw         Application Firewall information
  archive       Archive of the running configuration information
  arp           ARP table
<output omitted>
```

Step 2: Create the admin2 view, establish a password, and assign privileges.

The Admin2 user is a junior administrator in training who is allowed to view all configurations but is not allowed to configure the routers or use debug commands.

a. Use the **enable view** command to enable the root view, and enter the enable secret password cisco12345.

```
R1#enable view
Password:cisco12345
```

b. Use the following command to create the admin2 view.

```
R1(config)#parser view admin2
R1(config-view)#
*Dec 16 23:02:27.587: %PARSER-6-VIEW_CREATED: view 'admin2'
successfully created. <ENTER>
```

c. Associate the admin2 view with a password.

```
R1(config-view)#secret admin2pass
R1(config-view)#
```

d. Add all show commands to the view and then exit from view configuration mode.

```
R1(config-view)#commands exec include all show
R1(config-view)#end
```

e. Verify the admin2 view.

```
R1(config-view)#end
R1#enable view admin2
Password: admin2pass
*Dec 16 23:05:46.971: %PARSER-6-VIEW_SWITCH: successfully set to view
'admin2'
```

```
R1#show parser view
R1# Current view is 'admin2'
```

f. Examine the commands available in the admin2 view.

```
R1#?
Exec commands:
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  show        Show running system information
```

What is missing from the list of admin2 commands that is present in the admin1 commands? _____

Step 3: Create the tech view, establish a password, and assign privileges.

a. The Tech user typically installs end-user devices and cabling. Tech users are only allowed to use selected show commands.

b. Use the **enable view** command to enable the root view, and enter the enable secret password cisco12345.

```
R1#enable view
Password:cisco12345
```

c. Use the following command to create the tech view.

```
R1(config)#parser view tech
R1(config-view)#
```

*Dec 16 23:10:27.587: %PARSER-6-VIEW_CREATED: view 'tech' successfully created.
<ENTER>

d. Associate the tech view with a password.

```
R1(config-view)#secret techpasswd
R1(config-view)#
```

e. Add the following show commands to the view and then exit from view configuration mode.

```
R1(config-view)#commands exec include show version
R1(config-view)#commands exec include show interfaces
R1(config-view)#commands exec include show ip interface brief
R1(config-view)#commands exec include show parser view
R1(config-view)#end
```

f. Verify the tech view.

```
R1#enable view tech
Password:techpasswd
*Dec 16 23:13:46.971: %PARSER-6-VIEW_SWITCH: successfully set to view
'tech'
R1#show parser view
R1#Current view is 'tech'
```

g. Examine the commands available in the tech view.

```
R1#?
Exec commands:
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  show        Show running system information
```

h. Examine the show commands available in the tech view.

```
R1#show ?
  flash:      display information about flash: file system
  interfaces  Interface status and configuration
  ip          IP information
  parser      Show parser commands
  version     System hardware and software status
```

i. Issue the **show ip interface brief** command. Were you able to do it as the tech user? Why or why not? _____

j. Issue the **show ip route** command. Were you able to do it as the tech user? _____

k. Return to root view with the **enable view** command.

```
R1# enable view
Password: cisco12345
```

l. Issue the **show run** command to see the views you created. For tech view, why are the **show** and **show ip** commands listed as well as **show ip interface** and **show ip interface brief**?

Step 4: Save the configuration on routers R1 and R3.

Save the running configuration to the startup configuration from the privileged EXEC prompt.

Part 4. Configure IOS Resilience and Management Reporting

In Part 4 of this lab, you will:

- Secure the Cisco IOS image and configuration files.
- Configure a router as a synchronized time source for other devices using NTP.
- Configure syslog support on a router.
- Install a syslog server on a PC and enable it.
- Configure the logging trap level on a router.
- Make changes to the router and monitor syslog results on the PC.

Note: Perform all tasks on both R1 and R3. The procedure and output for R1 is shown here.

Task 1. Secure Cisco IOS Image and Configuration Files on R1 and R3

The Cisco IOS Resilient Configuration feature enables a router to secure the running image and maintain a working copy of the configuration so that those files can withstand malicious attempts to erase the contents of persistent storage (NVRAM and flash). The feature secures the smallest working set of files to preserve persistent storage space. No extra space is required to secure the primary Cisco IOS image file. In this task, you configure the Cisco IOS Resilient Configuration feature.

Step 1: Display the files in flash memory for R1.

```
R1#show flash
-#- --length-- -----date/time------ path
1     37081324 Dec 16 2008 21:57:10 c1841-advipservicesk9-mz.124-20.T1.bin
2      6389760 Dec 16 2008 22:06:56 sdm.tar
3      1505280 Dec 16 2008 22:08:52 common.tar
```

```
4       527849 Dec 16 2008 17:13:40 128MB.sdf
5         1821 Dec 16 2008 00:11:30 sdmconfig-18xx.cfg
6       931840 Dec 16 2008 17:14:42 es.tar
7       112640 Dec 16 2008 17:15:06 home.tar
8         1038 Dec 16 2008 17:15:22 home.shtml
9      1697952 Dec 16 2008 17:17:54 securedesktop-ios-3.1.1.45-k9.pkg
10      415956 Dec 16 2008 17:21:16 sslclient-win-1.1.4.176.pkg

14815232 bytes available (49197056 bytes used)
```

Step 2: Secure the Cisco IOS image and archive a copy of the running configuration.

a. The **secure boot-image** command enables Cisco IOS image resilience, which hides the file from **dir** and **show** commands. The file cannot be viewed, copied, modified, or removed using EXEC mode commands. (It can be viewed in ROMMON mode.) When turned on for the first time, the running image is secured.

```
R1(config)#secure boot-image
.Dec 17 25:40:13.170: %IOS_RESILIENCE-5-IMAGE_RESIL_ACTIVE:
Successfully secured running image
```

b. The **secure boot-config** command takes a snapshot of the router running configuration and securely archives it in persistent storage (flash).

```
R1(config)#secure boot-config
.Dec 17 25:42:18.691: %IOS_RESILIENCE-5-CONFIG_RESIL_ACTIVE:
Successfully secured config archive [flash:.runcfg-20081219-224218.ar]
```

Step 3: Verify that your image and configuration are secured.

a. You can use only the **show secure bootset** command to display the archived filename. Display the status of configuration resilience and the primary bootset filename.

```
R1#show secure bootset
IOS resilience router id FTX1111W0QF

IOS image resilience version 12.4 activated at 25:40:13 UTC Wed Dec 17
2008
Secure archive flash:c1841-advipservicesk9-mz.124-20.T1.bin type is
image (elf)
[]
  file size is 37081324 bytes, run size is 37247008 bytes
  Runnable image, entry point 0x8000F000, run from ram

IOS configuration resilience version 12.4 activated at 25:42:18 UTC Wed
Dec 17 2008
Secure archive flash:.runcfg-20081219-224218.ar type is config
configuration archive size 1986 bytes
```

b. What is the name of the archived running config file and on what is the name based?

_____

Step 4: Display the files in flash memory for R1.

a. Display the contents of flash using the **show flash** command.

```
R1#show flash
-#- --length-- -----date/time------ path
1      6389760 Dec 16 2008 22:06:56 sdm.tar
```

```
2      1505280 Dec 16 2008 22:08:52 common.tar
3       527849 Dec 16 2008 17:13:40 128MB.sdf
4         1821 Dec 16 2008 00:11:30 sdmconfig-18xx.cfg
5       512000 Dec 16 2008 17:14:24 dg_sdm.tar
6       931840 Dec 16 2008 17:14:42 es.tar
7       112640 Dec 16 2008 17:15:06 home.tar
8         1038 Dec 16 2008 17:15:22 home.shtml
10     1697952 Dec 16 2008 17:17:54 securedesktop-ios-3.1.1.45-k9.pkg
11      415956 Dec 16 2008 17:21:16 sslclient-win-1.1.4.176.pkg

14807040 bytes available (49205248 bytes used)
```

b. Is the Cisco IOS image or the archived running config file listed? _____

c. How can you tell that the Cisco IOS image is still there? _____

Step 5: Disable the IOS Resilient Configuration feature.

a. Disable the Resilient Configuration feature for the Cisco IOS image.

```
R1#config t
R1(config)#no secure boot-image
.Dec 17 25:48:23.009: %IOS_RESILIENCE-5-IMAGE_RESIL_INACTIVE: Disabled
secure image archival
```

b. Disable the Resilient Configuration feature for the running config file.

```
R1(config)#no secure boot-config
.Dec 17 25:48:47.972: %IOS_RESILIENCE-5-CONFIG_RESIL_INACTIVE: Disabled
secure config archival [removed flash:.runcfg-20081219-224218.ar]
```

Step 6: Verify that the Cisco IOS image is now visible in flash.

```
R1#show flash
-#- --length-- -----date/time------ path
1      37081324 Dec 16 2008 21:57:10 c1841-advipservicesk9-mz.124-20.T1.bin
2       6389760 Dec 16 2008 22:06:56 sdm.tar
3       1505280 Dec 16 2008 22:08:52 common.tar
4        527849 Dec 16 2008 17:13:40 128MB.sdf
5          1821 Dec 16 2008 00:11:30 sdmconfig-18xx.cfg
6        931840 Dec 16 2008 17:14:42 es.tar
7        112640 Dec 16 2008 17:15:06 home.tar
8          1038 Dec 16 2008 17:15:22 home.shtml
9       1697952 Dec 16 2008 17:17:54 securedesktop-ios-3.1.1.45-k9.pkg
10       415956 Dec 16 2008 17:21:16 sslclient-win-1.1.4.176.pkg

14815232 bytes available (49197056 bytes used)
```

Step 7: Save the configuration on both routers.

Save the running configuration to the startup configuration from the privileged EXEC prompt.

Task 2. Configure a Synchronized Time Source Using NTP

Router R2 will be the master NTP clock source for routers R1 and R3.

Note: R2 could also be the master clock source for switches S1 and S3, but it is not necessary to configure them for this lab.

Step 1: Set up the NTP Master using Cisco IOS commands.

R2 is the master NTP server in this lab. All other routers and switches learn their time from it, either directly or indirectly. For this reason, you must first ensure that R2 has the correct Coordinated Universal Time set.

Note: If you are using SDM to configure R2 to support NTP, skip this step and go to Step 2.

a. Display the current time set on the router using the **show clock** command.

```
R2#show clock
*01:19:02.331 UTC Mon Dec 15 2008
```

b. To set the time on the router, use the **clock set** *time* command.

```
R2#clock set 20:12:00 Dec 17 2008
R2#
*Dec 17 20:12:18.000: %SYS-6-CLOCKUPDATE: System clock has been updated
from 01:20:26 UTC Mon Dec 15 2008 to 20:12:00 UTC Wed Dec 17 2008,
configured from console by admin on console.
```

c. Configure R2 as the NTP master using the **ntp master** *stratum-number* command in global configuration mode. The stratum number indicates the distance from the original source. For this lab, use a stratum number of 3 on R2. When a device learns the time from an NTP source, its stratum number becomes one greater than the stratum number of its source.

```
R2(config)#ntp master 3
```

Step 2: Configure R1 and R3 as NTP clients using the CLI.

a. R1 and R3 will become NTP clients of R2. To configure R1, use the global configuration command **ntp server *hostname***. The host name can also be an IP address. The command **ntp update-calendar** periodically updates the calendar with the NTP time.

```
R1(config)#ntp server 10.1.1.2
R1(config)#ntp update-calendar
```

b. Verify that R1 has made an association with R2 with the **show ntp associations** command. You can also use the more verbose version of the command by adding the **detail** argument. It might take some time for the NTP association to form.

```
R1#show ntp associations

address         ref clock       st   when   poll reach  delay  offset    disp
~10.1.1.2       127.127.1.1      3     14     64     3  0.000  -280073  3939.7
*sys.peer, #selected, +candidate, -outlyer, x falseticker, ~ configured
```

c. Issue the **debug ntp all** command to see NTP activity on R1 as it synchronizes with R2.

```
R1#debug ntp all
NTP events debugging is on
NTP core messages debugging is on
NTP clock adjustments debugging is on
NTP reference clocks debugging is on
NTP packets debugging is on

Dec 17 20.12:18.554: NTP message sent to 10.1.1.2, from interface
'Serial0/0/0' (10.1.1.1).
Dec 17 20.12:18.574: NTP message received from 10.1.1.2 on interface
'Serial0/0/0' (10.1.1.1).
Dec 17 20:12:18.574: NTP Core(DEBUG): ntp_receive: message received
```

```
Dec 17 20:12:18.574: NTP Core(DEBUG): ntp_receive: peer is 0x645A3120,
next action is 1.
Dec 17 20:12:18.574: NTP Core(DEBUG): receive: packet given to
process_packet
Dec 17 20:12:18.578: NTP Core(INFO): system event 'event_peer/strat_chg'
(0x04)
status 'sync_alarm, sync_ntp, 5 events, event_clock_reset' (0xC655)
Dec 17 20:12:18.578: NTP Core(INFO): synchronized to 10.1.1.2, stratum 3
Dec 17 20:12:18.578: NTP Core(INFO): system event 'event_sync_chg' (0x03)
status
 'leap_none, sync_ntp, 6 events, event_peer/strat_chg' (0x664)
Dec 17 20:12:18.578: NTP Core(NOTICE): Clock is synchronized.
Dec 17 20:12:18.578: NTP Core(INFO): system event 'event_peer/strat_chg'
(0x04)
status 'leap_none, sync_ntp, 7 events, event_sync_chg' (0x673)
Dec 17 20:12:23.554: NTP: Calendar updated.
```

d. Issue the **undebug all** or the **no debug ntp all** command to turn off debugging.

```
R1#undebug all
```

e. Verify the time on R1 after it has made an association with R2.

```
R1#show clock
*20:12:24.859 UTC Wed Dec 17 2008
```

Step 3: (Optional) Configure R1 and R3 as NTP clients using SDM.

You can also use SDM to configure the router to support NTP. If you configured R1 as an NTP client using Cisco IOS commands in Step 2, you can skip this step, but read through it to become familiar with the process. If you configured R1 and R3 as NTP clients using Cisco IOS commands in Step 2 you can still perform this step but you need to issue the following commands first on each router.

```
R1(config)#no ntp server 10.1.1.2
R1(config)#no ntp update-calendar
```

a. From the CLI, enable the http server on R1.

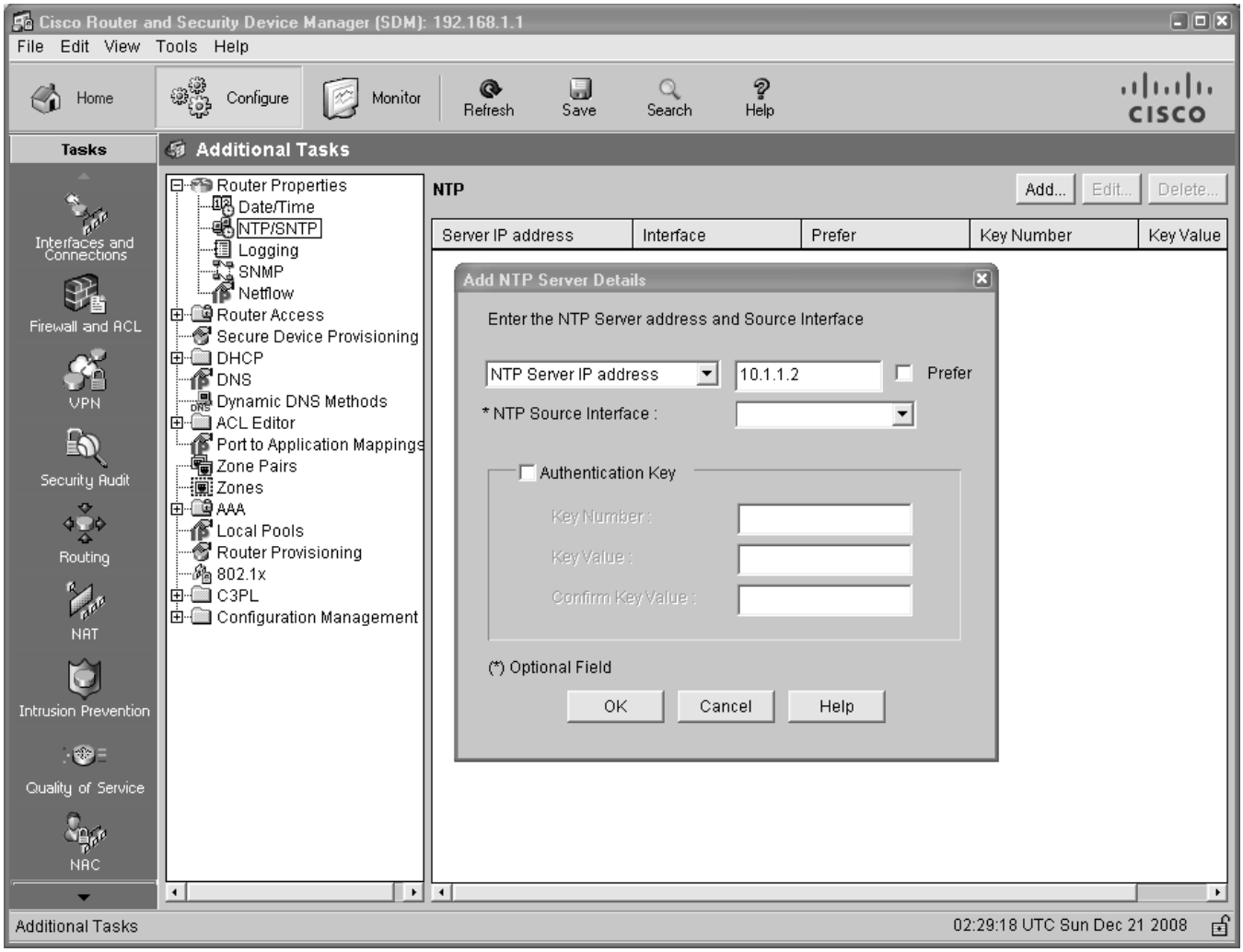
```
R1(config)#ip http server
```

b. Open a browser window on PC-A and start SDM by entering the R1 IP address 192.168.1.1 in the address field. Log in as admin with password cisco12345.

c. To configure SDM to allow you to preview the commands before sending them to the router, select **Edit** > **Preferences.**

d. In the **User Preferences** window, select **Preview commands before delivering to router** and click **OK**.

e. To configure an NTP server, click the **Configure** button and select **Additional Tasks > Router Properties > NTP/SNTP**. Click **Add**.



f. In the NTP Server IP Address field, enter the IP address of the R2 master NTP router (10.1.1.2) and click **OK**.

g. In the Deliver Configuration to Router window, make sure that the **Save running config to router's startup config** check box is checked and click **Deliver**.

h. Click **OK** in the Commands Delivery Status window.

i. Open a console connection to the router, and verify the associations and time on R1 after it has made an association with R2. It might take some time for the NTP association to form.

```
R1#show ntp associations

address         ref clock       st   when   poll reach   delay   offset    disp
~10.1.1.2       127.127.1.1      3     14     64     3    0.000  -280073   3939.7
*sys.peer, #selected, +candidate, -outlyer, x falseticker, ~ configured

R1#show clock
*20:12:24.859 UTC Wed Dec 17 2008
```

Task 3. Configure syslog Support on R1 and PC-A

Step 1: Install the syslog server.

The Kiwi Syslog Daemon is a dedicated syslog server. Another application is Tftpd32, which includes a TFTP server, TFTP client, and a syslog server and viewer. You can use either with this lab. Both are available as a free version and run with Microsoft Windows.

If a syslog server is not currently installed on the host, download the latest version of Kiwi from http://www.kiwisyslog.com or Tftpd32 from http://tftpd32.jounin.net and install it on your desktop. If it is already installed, go to Step 2.

Note: This lab uses the Kiwi syslog server.

Step 2: Configure R1 to log messages to the syslog server using the CLI.

a. Verify that you have connectivity between R1 and the host by pinging the R1 Fa0/1 interface IP address 192.168.1.1. If it is not successful, troubleshoot as necessary before continuing.

b. NTP was configured in Task 2 to synchronize the time on the network. Displaying the correct time and date in syslog messages is vital when using syslog to monitor a network. If the correct time and date of a message is not known, it can be difficult to determine what network event caused the message.

Verify that the timestamp service for logging is enabled on the router using the **show run** command. Use the following command if the timestamp service is not enabled.

```
R1(config)#service timestamps log datetime msec
```

c. Configure the syslog service on the router to send syslog messages to the syslog server.

```
R1(config)#logging 192.168.1.3
```

Step 3: Configure the logging severity level on R1.

Logging traps can be set to support the logging function. A trap is a threshold that when reached triggers a log message. The level of logging messages can be adjusted to allow the administrator to determine what kinds of messages are sent to the syslog server. Routers support different levels of logging. The eight levels range from 0 (emergencies), indicating that the system is unstable, to 7 (debugging), which sends messages that include router information.

Note: The default level for syslog is 6, informational logging. The default for console and monitor logging is 7, debugging.

a. Use the **logging trap** command to determine the options for the command and the various trap levels available.

```
R1(config)#logging trap ?
<0-7>          Logging severity level
alerts         Immediate action needed           (severity=1)
critical       Critical conditions               (severity=2)
debugging      Debugging messages                (severity=7)
emergencies    System is unusable                (severity=0)
errors         Error conditions                  (severity=3)
informational  Informational messages            (severity=6)
notifications  Normal but significant conditions (severity=5)
warnings       Warning conditions                (severity=4)
<cr>
```

b. Define the level of severity for messages sent to the syslog server. To configure the severity levels, use either the keyword or the severity level number (0–7).

Severity level	Keyword	Meaning
0	emergencies	System unusable
1	alerts	Immediate action required
2	critical	Critical conditions
3	errors	Error conditions
4	warnings	Warning conditions
5	notifications	Normal but significant condition
6	informational	Informational messages
7	debugging	Debugging messages

Note: The severity level includes the level specified and anything with a lower severity number. If you set the level to 4 or use the keyword **warnings**, you capture messages with severity level 4, 3, 2, 1, and 0.

c. Use the **logging trap** command to set the severity level for R1.

```
R1(config)#logging trap warnings
```

d. What is the problem with setting the level of severity too high or too low?

_____
_____
_____

e. If the command **logging trap critical** were issued, which severity levels of messages would be logged? _____

Step 4: Display the current status of logging for R1.

a. Use the **show logging** command to see the type and level of logging enabled.

```
R1#show logging
Syslog logging: enabled (0 messages dropped, 1 messages rate-limited,
                0 flushes, 0 overruns, xml disabled, filtering
disabled)

No Active Message Discriminator.
No Inactive Message Discriminator.

    Console logging: level debugging, 271 messages logged, xml
disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  disabled, xml disabled,
                     filtering disabled
    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

ESM: 0 messages dropped

    Trap logging: level warnings, 0 message lines logged
        Logging to 192.168.1.3  (udp port 514,  audit disabled,
```

```
authentication disabled, encryption disabled, link up),
0 message lines logged,
0 message lines rate-limited,
0 message lines dropped-by-MD,
xml disabled, sequence number disabled
filtering disabled
```

b. At what level is console logging enabled? _____

c. At what level is trap logging enabled? _____

d. What is the IP address of the syslog server? _____

e. What port is syslog using? _____

Step 5: (Optional) Configure R1 to log messages to the syslog server using SDM.

You can also use SDM to configure the router for syslog support. If you configured R1 for syslog and trap levels previously, you can skip this step. If you configured R1 syslog and trap levels using Cisco IOS commands in Step 4 you can still perform this step but you need to issue the following commands first on the router:

```
R1(config)#no logging 192.168.1.3
R1(config)#no logging trap warnings
```

a. Open a browser on PC-A, and start SDM by entering the R1 IP address 192.168.1.1 in the address field. Log in as admin with password cisco12345.

b. Select Configure > Additional Tasks > Router Properties > Logging, and double-click Syslog.

c. In the Logging window, click Add and enter the IP address of the syslog server, PC-A (192.168.1.3). Click OK.

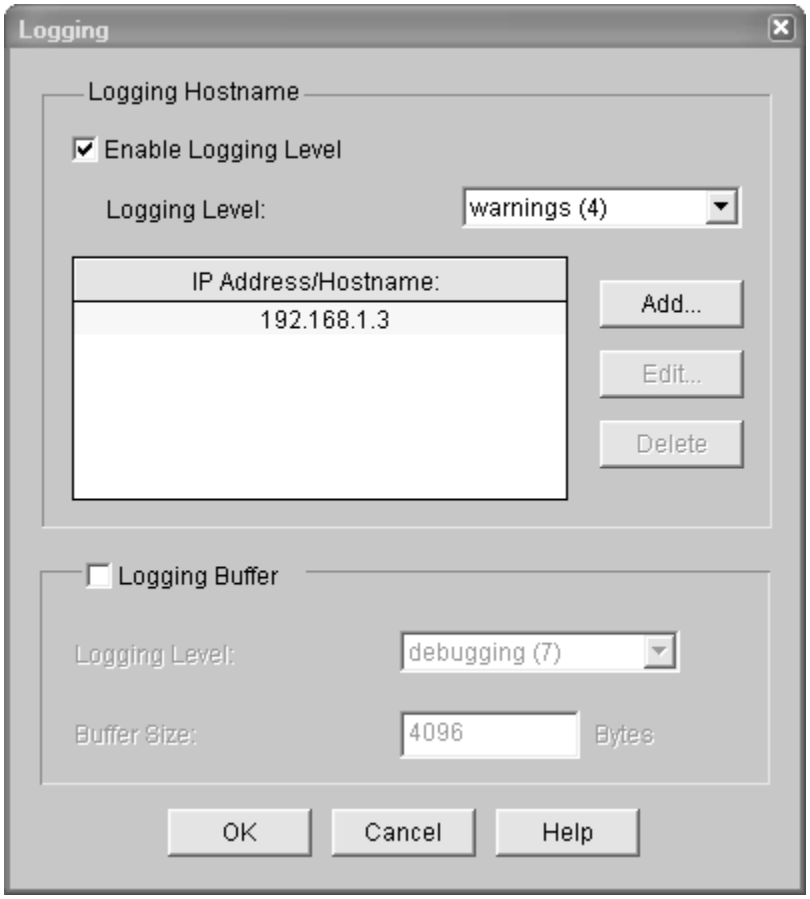
d. From the Logging Level drop-down menu, select the logging level of Warnings (4).

e. Deselect Logging Buffer, and then click OK.

f. Click Yes in the SDM Warning dialog box.

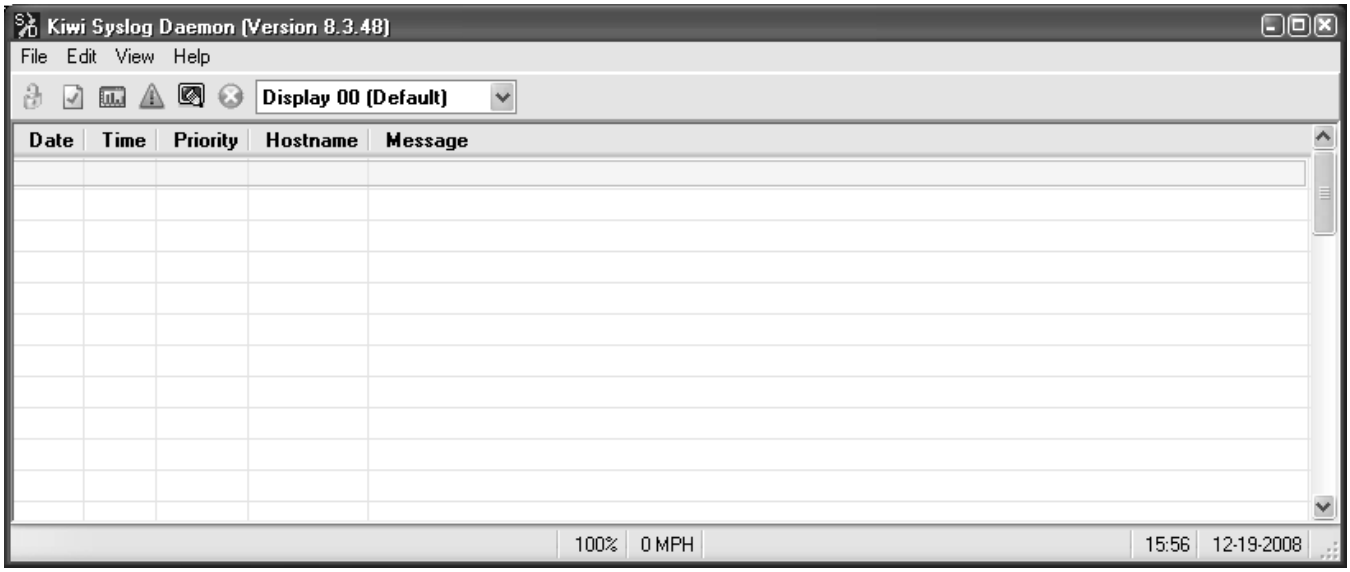
g. In the Deliver Configuration to Router window, click Deliver. Click OK in the Commands Delivery Status window.

h. Click Save on the toolbar. Click Yes in the SDM Write to Startup Config Warning window.



Step 6: Start the Kiwi Syslog Server.

Open the Kiki Syslog Daemon application on your desktop or click the **Start** button and select **Programs > Kiwi Enterprises > Kiwi Syslog Daemon**.



Step 7: Verify that logging to the syslog server is occurring.

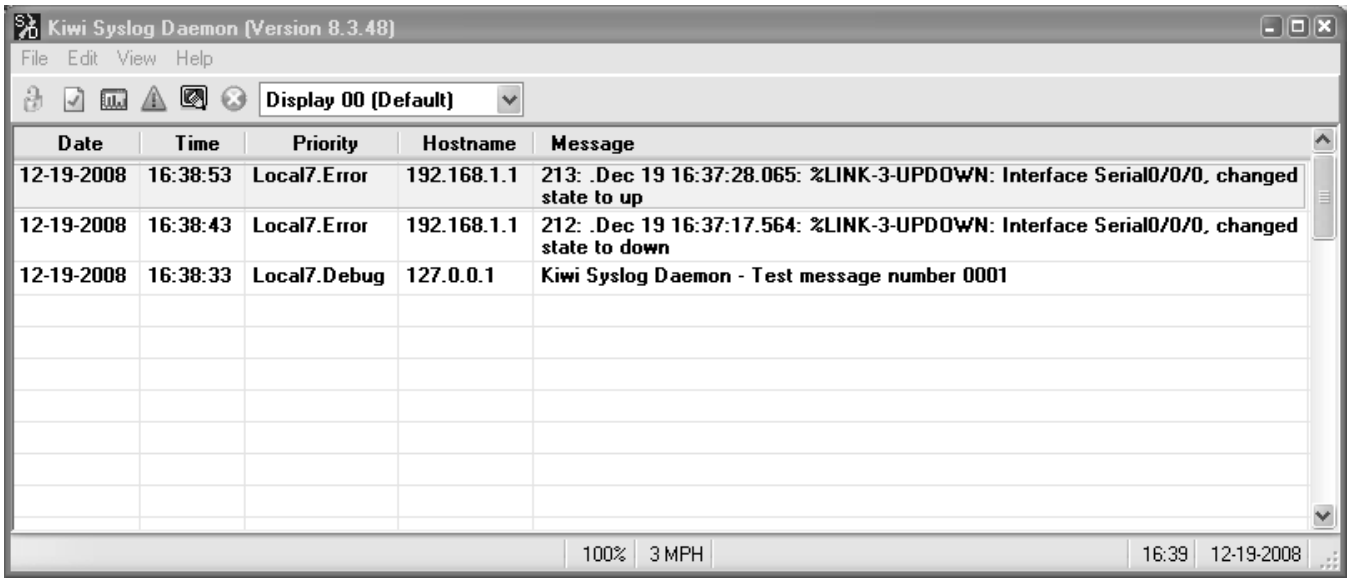
On the syslog server host PC-A, observe messages as they are sent from R1 to the syslog server.

a. Send a test log message to the kiwi syslog server by choosing **File > Send test message to local host**.

b. Generate a logging message by shutting down the Serial0/0/0 interface on R1 or R2 and then re-enabling it.

```
R1(config)#interface S0/0/0
R1(config-if)#shutdown
R1(config-if)#no shutdown
```

The Kiwi syslog screen should look similar to the following one.



c. What would happen if you were shut down the Fa0/1 interface on R1 (do not actually perform this action)? _____

d. From the R1 global configuration mode, enable the logging of user info when enabling privileged mode and reset the trap level to informational.

```
R1(config)#logging userinfo
R1(config)#logging trap informational
```

e. On the Kiwi Syslog Daemon, click **View > Clear Display** to clear the log display.

f. Exit to the login screen, and enable the admin1 view that you created in Part 3 of this lab. Enter the password admin1pass.

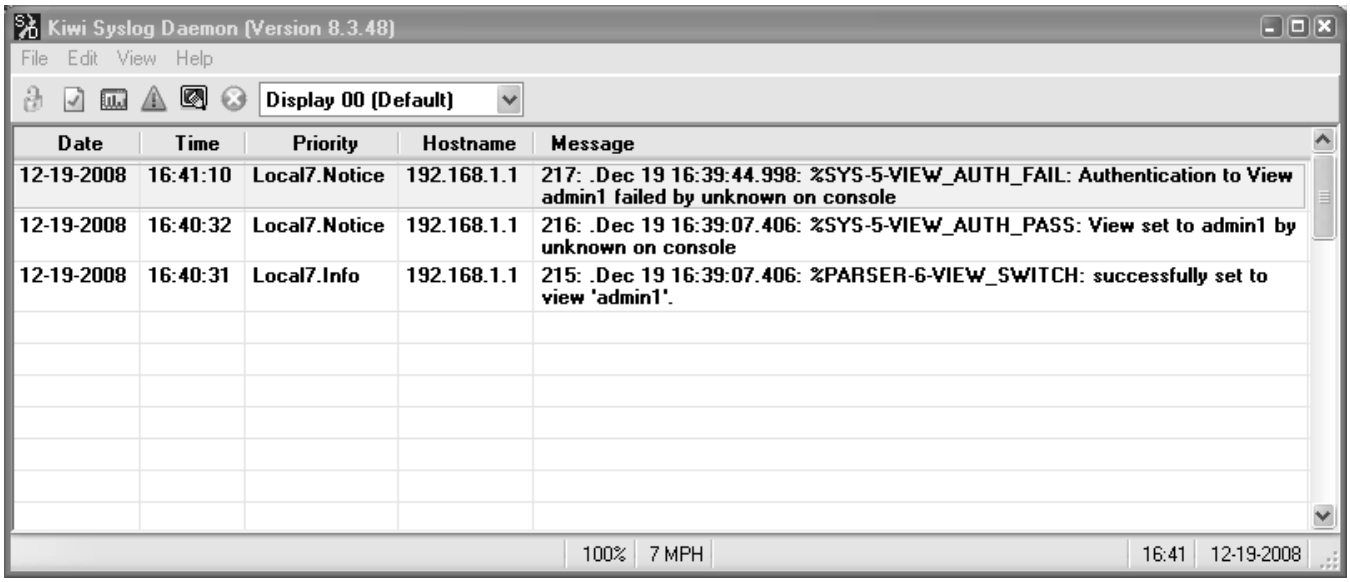
```
R1>enable view admin1
Password:
```

Note: You can enable the desired view from the user EXEC prompt. This allows different users to login without having to know the privileged EXEC mode enable secret password.

g. Exit to the login screen again, and enable the admin1 view. This time enter the password incorrectly. What message was displayed on the syslog server?

```
R1>enable view admin1
Password:
```

Your screen should look similar to the following one.



Part 5. Configure Automated Security Features

In Part 5 of this lab, you will:

- Restore routers R1 and R3 to their basic configuration.
- Use AutoSecure to secure R3.
- Use the SDM Security Audit tool on router R1 to identify security risks.
- Fix security problems on R1 using the Security Audit tool.
- Review router security configurations with SDM and the CLI.

Task 1. Restore Router R3 to Its Basic Configuration

To avoid confusion as to what was already entered and what AutoSecure provides for the router configuration, start by restoring router R3 to its basic configuration.

Step 1: Erase and reload the router.

a. Connect to the R3 console and login as admin.

b. Enter privileged EXEC mode.

c. Erase the startup config and then reload the router.

Step 2: Restore the basic configuration.

a. When the router restarts, restore the basic configuration for R3 that was created and saved in Part 1 of this lab.

b. Issue the **show run** command to view the current running configuration. Are there any security related commands? _____

c. Test connectivity by pinging from host PC-A on the R1 LAN to PC-C on the R3 LAN. If the pings are not successful, troubleshoot the router and PC configurations until they are.

d. Save the running config to the startup config using the **copy run start** command.

Task 2. Use AutoSecure to Secure R3

By using a single command in CLI mode, the AutoSecure feature allows you to disable common IP services that can be exploited for network attacks and enable IP services and features that can aid in the defense of a network when under attack. AutoSecure simplifies the security configuration of a router and hardens the router configuration.

Step 1: Use the AutoSecure Cisco IOS feature.

a. Enter privileged EXEC mode using the **enable** command.

b. Issue the **auto secure** command on R3 to lock down the router. Router R2 represents an ISP router, so assume that R3 S0/0/1 is connected to the Internet when prompted by the AutoSecure questions. Respond to the AutoSecure questions as shown in the following output. The responses are bolded.

```
R3#auto secure
                --- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security of the router, but it will
not make it absolutely resistant to all security attacks ***

AutoSecure will modify the configuration of your device. All configuration
changes will be shown. For a detailed explanation of how the configuration
changes enhance security and any possible side effects, please refer to
Cisco.com for
Autosecure documentation.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]:  yes
   Enter the number of interfaces facing the internet [1]:  Press ENTER to
   accept the default of 1 in square brackets.


   Interface         IP-Address  OK?  Method Status                Protocol

   FastEthernet0/0   unassigned  YES  NVRAM  administratively down   down

   FastEthernet0/1   192.168.3.1 YES  NVRAM  up                     up

   Serial0/0/0       unassigned  YES  NVRAM  administratively down   down

   Serial0/0/1       10.2.2.1    YES  NVRAM  up                     up


   Enter the interface name that is facing the internet: serial0/0/1
```

```
Securing Management plane services...

Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol

Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp

Here is a sample Security Banner to be shown
at every access to device. Modify it to suit your
enterprise requirements.

Authorized Access only
  This system is the property of So-&-So-Enterprise.
  UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.
  You must have explicit permission to access this
  device. All activities performed on this device
  are logged. Any violations of access policy will result
  in disciplinary action.

Enter the security banner {Put the banner between
k and k, where k is any character}:

# Unauthorized Access Prohibited #

Enable secret is either not configured or
 is the same as enable password
Enter the new enable secret: cisco12345
Confirm the enable secret : cisco12345
Enter the new enable password: cisco67890
Confirm the enable password: cisco67890

Configuration of local user database
Enter the username: admin
Enter the password: cisco12345
Confirm the password: cisco12345
Configuring AAA local authentication
Configuring Console, Aux and VTY lines for
local authentication, exec-timeout, and transport
Securing device against Login Attacks
Configure the following parameters

Blocking Period when Login Attack detected: 60

Maximum Login failures with the device: 2

Maximum time period for crossing the failed login attempts: 30

Configure SSH server? [yes]: Press ENTER to accept the default of yes
```

```
Enter the domain-name: ccnasecurity.com

Configuring interface specific AutoSecure services
Disabling the following ip services on all interfaces:

 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
Disabling mop on Ethernet interfaces

Securing Forwarding plane services...

Enabling CEF (This might impact the memory requirements for your platform)
Enabling unicast rpf on all interfaces connected
to internet

Configure CBAC Firewall feature? [yes/no]: no
Tcp intercept feature is used prevent tcp syn attack
on the servers in the network. Create autosec_tcp_intercept_list
to form the list of servers to which the tcp traffic is to
be observed


Enable tcp intercept feature? [yes/no]: yes

This is the configuration generated:

no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
no ip identd
banner motd ^C Unauthorized Access Prohibited ^C
security passwords min-length 6
security authentication failure rate 10 log
enable secret 5 $1$FmV1$.xZUegmNYFJwJv/oFwwvG1
enable password 7 045802150C2E181B5F
username admin password 7 01100F175804575D72
aaa new-model
aaa authentication login local_auth local
line con 0
 login authentication local_auth
 exec-timeout 5 0
 transport output telnet
line aux 0
 login authentication local_auth
```

```
 exec-timeout 10 0
 transport output telnet
line vty 0 4
 login authentication local_auth
 transport input telnet
line tty 1
 login authentication local_auth
 exec-timeout 15 0
login block-for 60 attempts 2 within 30
ip domain-name ccnasecurity.com
crypto key generate rsa general-keys modulus 1024
ip ssh time-out 60
ip ssh authentication-retries 2
line vty 0 4
 transport input ssh telnet
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
interface FastEthernet0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface FastEthernet0/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface Serial0/0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
interface Serial0/0/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
interface Vlan1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
ip cef
access-list 100 permit udp any any eq bootpc
interface Serial0/0/1
```

```
 ip verify unicast source reachable-via rx allow-default 100
ip tcp intercept list autosec_tcp_intercept_list
ip tcp intercept drop-mode random
ip tcp intercept watch-timeout 15
ip tcp intercept connection-timeout 3600
ip tcp intercept max-incomplete low 450
ip tcp intercept max-incomplete high 550
!
end

Apply this configuration to running-config? [yes]: <ENTER>

Applying the config generated to running-config
The name for the keys will be: R3.ccnasecurity.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R3#
000037: *Dec 19 21:18:52.495 UTC: %AUTOSEC-1-MODIFIED: AutoSecure
configuration
has been Modified on this device
```

Step 2: Establish an SSH connection from PC-C to R3.

a. Start PuTTy or another SSH client, and log in with the **admin** account and password **cisco12345** created when AutoSecure was run. Enter the IP address of the R3 Fa0/1 interface 192.168.3.1.

b. Because AutoSecure configured SSH on R3, you will receive a PuTTY security warning. Click **Yes** to connect anyway.

c. Enter privileged EXEC mode, and verify the R3 configuration using the **show run** command.

d. Issue the **show flash** command. Is there a file that might be related to AutoSecure, and if so what is its name and when was it created? _____

e. Issue the command **more flash:pre_autosec.cfg**. What are the contents of this file, and what is its purpose? _____

f. How would you restore this file if AutoSecure did not produce the desired results?

_____

Step 3: Contrast the AutoSecure-generated configuration of R3 with the manual configuration of R1.

a. What security-related configuration changes were performed on R3 by AutoSecure that were not performed in previous sections of the lab on R1?

_____
_____
_____
_____

b. What security-related configuration changes were performed in previous sections of the lab that were not performed by AutoSecure?

_____
_____

c. Identify at least five unneeded services that were locked down by AutoSecure and at least three security measures applied to each interface.

> **Note:** Some of the services listed as being disabled in the AutoSecure output above might not appear in the **`show running-config`** output because they are already disabled by default for this router and Cisco IOS version.

Services disabled include

_____
_____
_____

For each interface, the following were disabled:

_____
_____
_____

Step 4: Test connectivity.

Ping from PC-A on the R1 LAN to PC-C on the router R3 LAN. Were the pings successful? _____

If pings from PC-A to PC-C are not successful, troubleshoot before continuing.

Task 3. Restore R1 to Its Basic Configuration

To avoid confusion as to what was previously configured and what SDM Security Audit tool provides for the router configuration, start by restoring router R1 to its basic configuration.

Step 1: Erase and reload the router.

a. Connect to the R1 console and log in as admin.

b. Enter privileged EXEC mode.

c. Erase the startup config and then reload the router.

Step 2: Restore the basic config.

a. When the router restarts, cut and paste the basic startup config for R1 that was created and saved in Part 1 of this lab.

b. Test connectivity by pinging from host PC-A to R1. If the pings are not successful, troubleshoot the router and PC configurations to verify connectivity before continuing.

c. Save the running config to the startup config using the **`copy run start`** command.

Task 4. Use the SDM Security Audit Tool on R1 to Identify Security Risks

In this task, you use the SDM graphical user interface to analyze security vulnerabilities on router R1. SDM is faster than typing each command and gives you more control than the AutoSecure feature.

Step 1: Verify whether SDM is installed on router R1.

```
R1#show flash
-#- -length-- --date/time------ path
1    37081324   Dec 16 2008 21:57:10 c1841-advipservicesk9-mz.124-20.T1.bin
```

```
2    6389760    Dec 16 2008 22:06:56 sdm.tar
<Output omitted>
```

Note: SDM can be run from the PC or the router. If SDM is not installed on your router, check to see if it is installed on the PC. Otherwise, consult your instructor for directions.

Step 2: Create an SDM user and enable the HTTP secure server on R1.

a. Create a privilege-level 15 username and password on R1.

```
R1(config)#username admin privilege 15 secret 0 cisco12345
```

b. Enable the HTTP secure server on R1.

```
R1(config)#ip http secure-server
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R1(config)#
*Dec 19 17:01:07.763: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Dec 19 17:01:08.731: %PKI-4-NOAUTOSAVE: Configuration was modified.
Issue
"write memory" to save new certificate
```

c. Enable local HTTP authentication on R1.

```
R1(config)#ip http authentication local
R1(config)#end
```

d. Save the running config to the startup config.

```
R1#copy run start
```

Step 3: Start SDM.

a. From PC-A, run the SDM application and enter the IP address of R1 FA0/1 (192.168.1.1) or open a web browser and navigate to https://192.168.1.1.

b. **Note:** Make sure that you have all pop-up blockers turned off in your browser. Also make sure that Java is installed and updated.

c. When the certification error message is displayed, click **Continue to this web site**.

d. Log in with the previously configured username and password.

```
username: admin
password: cisco12345
```

e. At the **Warning Security** messages, click **Yes.**

f. At the **Password Needed – Networking** message, enter the username and password again.

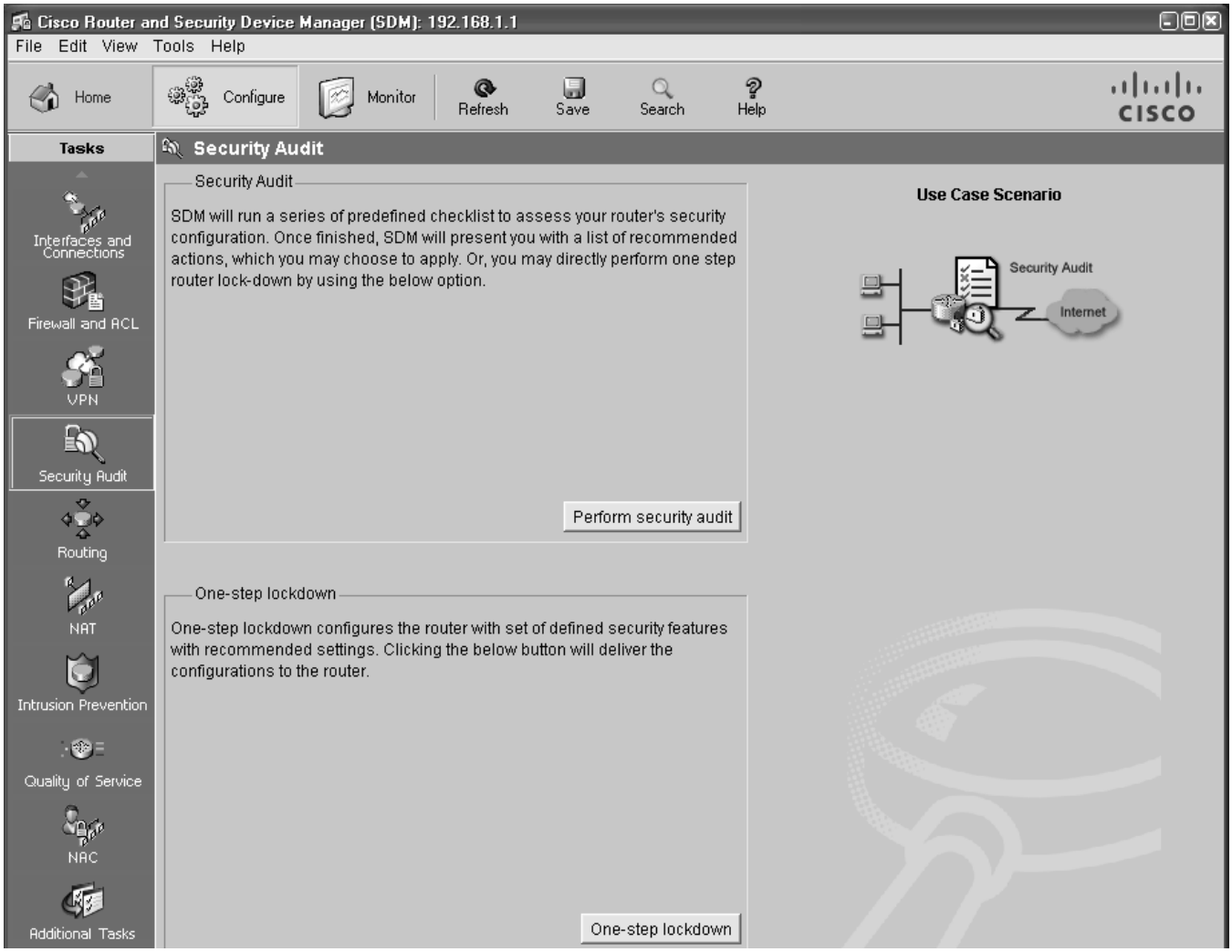
Step 4. Back up the current router configuration.

a. Back up the router configuration from within SDM by choosing **File > Save Running Config to PC**.

b. Save the configuration on the desktop using the default name of SDMConfig.txt.

Step 5. Begin the security audit.

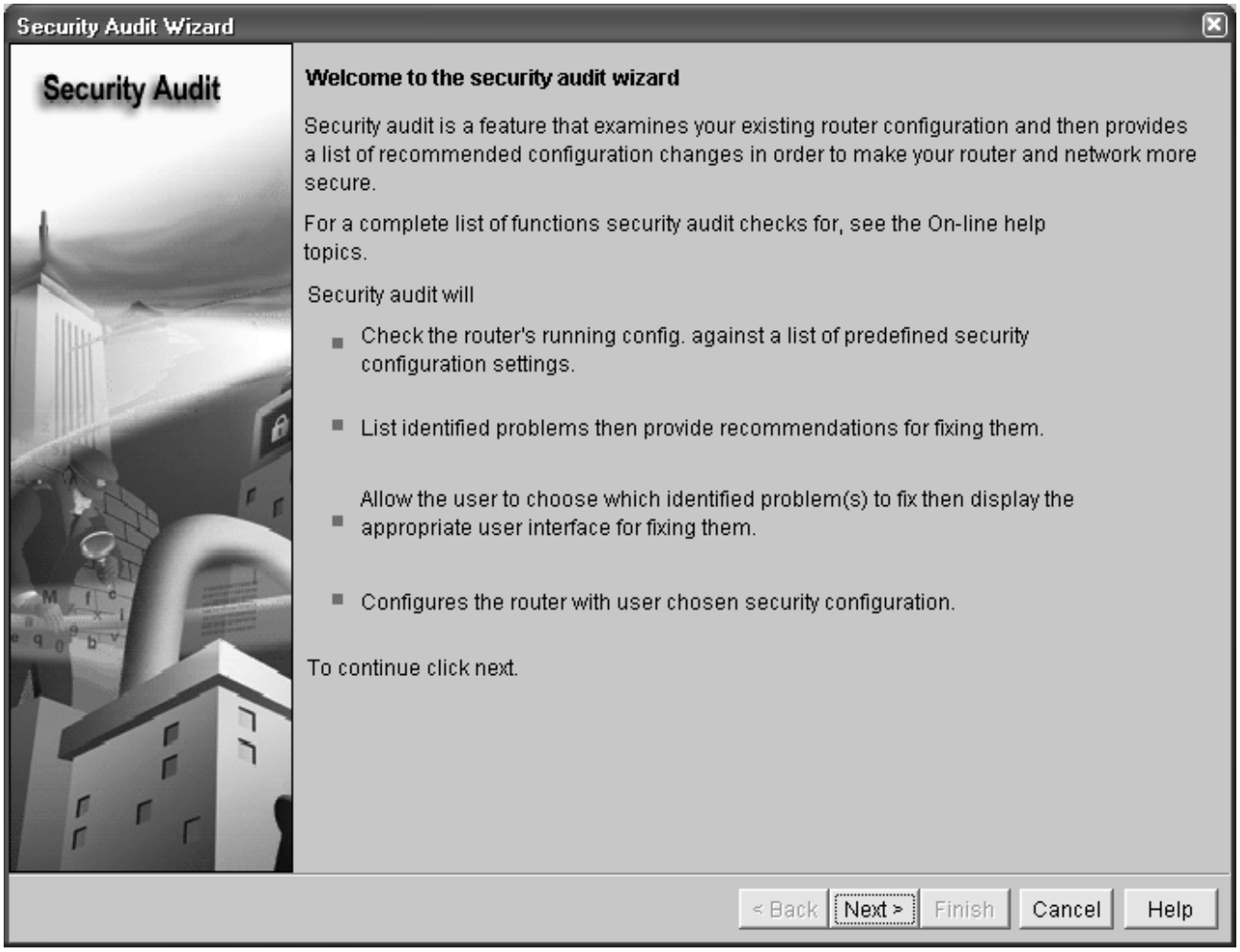
a. Select **Configure > Security Audit**.



b. Click the **Perform Security Audit** button to start the Security Audit wizard, which analyzes potential vulnerabilities. This helps you become familiar with the types of vulnerabilities that **Security Audit** can identify. You will be given an opportunity to fix all or selected security problems after the audit finishes..

Note: The Security Audit tool also provides a **One-Step Lockdown** option that performs a function similar to AutoSecure but does not prompt the user for input.

c**.** After you have familiarized yourself with the wizard instructions, click **Next**.



d. On the Security Audit Interface Configuration window, indicate which of the interfaces that are shown are inside (trusted) and which are outside (untrusted). For interface Fa0/1, select **Inside (trusted)**. For interface S0/0/0, select **Outside (untrusted)**.

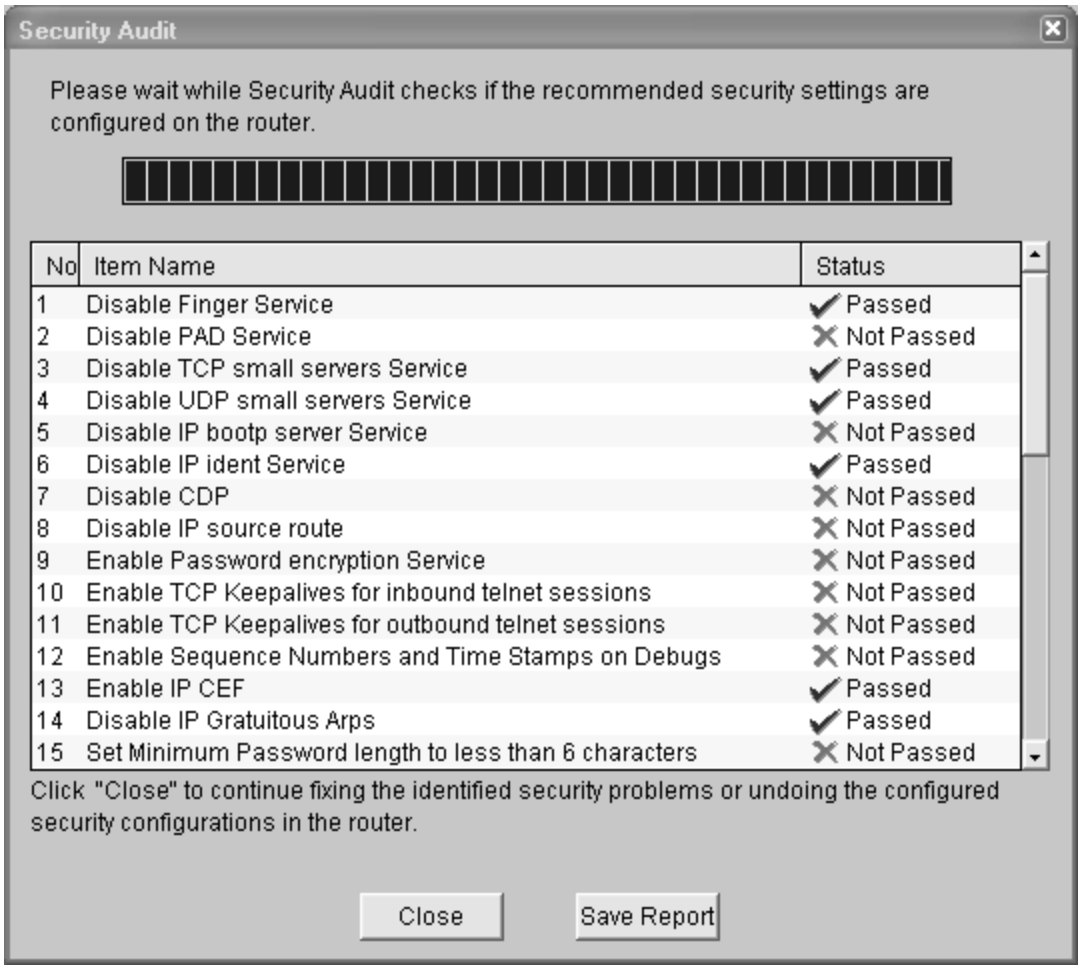
e. Click **Next** to check security configurations. You can watch the security audit progress.

Step 6: Identify Security Audit unneeded services and recommended configurations.

a. Scroll through the Security Audit results screen. What are some of the major vulnerabilities listed as Not Passed?

_____
_____
_____

b. After reviewing the Security Audit report, click **Save Report**. Save it to the desktop using the default name SDMSecurityAuditReportCard.html.



c. Open the report card HTML document you saved on the desktop to view the contents and then close it.

Task 5. Fix Security Problems on R1 Using the Security Audit Tool

In this task, you will use the Security Audit wizard to make the necessary changes to the router configuration.

Step 1: Review the Security Problems Identified window for potential items to fix.

a. In the Security Audit window, click **Close**.

b. A window appears listing the items that did not pass the security audit. Click **Next** without choosing any items. What message did you get? _____

c. Click **OK** to remove the message.

Step 2: Fix security problems.

With the Security Audit tool, you can fix selected problems or all security problems identified.

a. Click **Fix All** and then click **Next** to fix all security problems.

b. When prompted, enter an enable secret password of cisco12345 and confirm it.

c. Enter the text for the login banner: Unauthorized Access Prohibited. Click **Next**.

d. Add the logging host IP address 192.168.1.3, and accept the logging defaults. Click **Next**.

e. Accept the default security settings for inside and outside interfaces and click **Next**.

f. Deselect **URL Filter Server,** and click **Next**.

g. For the security level, select **Low Security** and click **Next**.

h. At the Firewall Configuration Summary, review the configuration and click **Finish**.

i. Scroll through the Summary screen. This screen shows what Security Audit will configure for the router.

j. Click **Finish** to see the actual commands that are delivered to the router. Scroll to review the commands.

k. Make sure that **Save running config to router's startup config** is selected, and click **Deliver**.

l. Click **OK** in the Commands Delivery Status window to exit the Security Audit tool. How many commands were delivered to the router? _____

Task 6. Review Router Security Configurations with SDM and the CLI

In this task, you will use Cisco SDM to review changes made by Security Audit on router R1 and compare them to those made by AutoSecure on R3.

Step 1: View the running configs for R1 and R3.

a. From the PC-A SDM session with R1, click the **View** option from the main menu and select **Running Config**.

b. Using PuTTY, open an SSH connection to router R3, and log in as admin.

c. Enter privileged EXEC mode, and issue the **`show run`** **c**ommand.

Step 2: Contrast AutoSecure with SDM Security Audit.

a. Compare the function and ease of use between AutoSecure and SDM Security Audit. What are some similarities and differences?

_____
_____
_____
_____

b. Refer to the AutoSecure configuration on R3 and the SDM Security Audit configuration on R1. What are some similarities and differences between the configurations generated by AutoSecure and Security Audit?

_____
_____
_____

_____
_____

Step 3: Test connectivity.

a. Ping from router R1 to the router R3 S0/0/1 interface (10.2.2.1). Were the pings successful? Why or why not? _____

Note: Firewalls are covered in detail in Chapter 4.

b. Ping from PC-A on the R1 LAN to PC-C on the router R3 LAN. Were the pings successful? Why or why not? _____

c. Ping from router R3 to the router R2 S0/0/0 interface (10.1.1.2). Were the pings successful? Why or why not? _____

d. Ping from router R3 to the router R1 S0/0/0 interface (10.1.1.1). Were the pings successful? Why or why not? _____

e. Ping from PC-C on the R3 LAN to PC-A on the router R1 LAN. Were the pings successful? Why or why not? _____

Task 7. Reflection

a. How important is securing router access and monitoring network devices to ensure responsibility and accountability and for thwarting potentially malicious activity.

_____
_____
_____

b. What advantages does SSH have over Telnet?

_____
_____

c. What advantages does Telnet have over SSH?

_____
_____

d. How scalable is setting up usernames and using the local database for authentication?

_____
_____
_____

e. Why it is better to have centralized logging servers rather than only have the routers log locally?

_____
_____
_____

f. What are some advantages to using automated security mechanisms like AutoSecure and SDM Security Audit?

_____
_____
_____

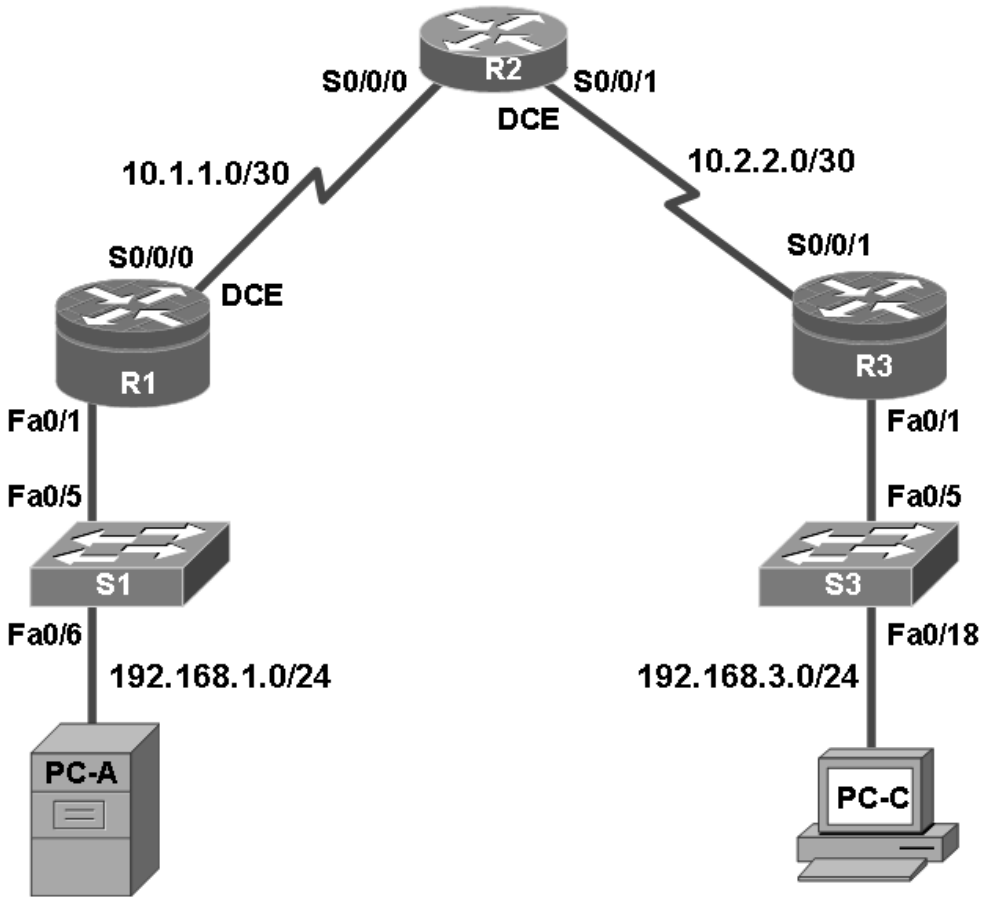
Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1700	Fast Ethernet 0 (FA0)	Fast Ethernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2600	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
2800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Chapter 3: Lab A" Securing Administrative Access Using AAA and RADIUS

Topology



IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	FA0/1	192.168.1.1	255.255.255.0	N/A	S1 FA0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	FA0/1	192.168.3.1	255.255.255.0	N/A	S3 FA0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 FA0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 FA0/18

Objectives

Part 1: Basic Network Device Configuration

- Configure basic settings such as host name, interface IP addresses, and access passwords.
- Configure static routing.

Part 2: Configure Local Authentication

- Configure a local database user and local access for the console, vty, and aux lines.
- Test the configuration.

Part 3: Configure Local Authentication Using AAA

- Configure the local user database using Cisco IOS.
- Configure AAA local authentication using Cisco IOS.
- Configure AAA local authentication using SDM.
- Test the configuration.

Part 4: Configure Centralized Authentication Using AAA and RADIUS

- Install a RADIUS server on a computer.
- Configure users on the RADIUS server.
- Configure AAA services on a router to access the RADIUS server for authentication using Cisco IOS.
- Configure AAA services on a router to access the RADIUS server for authentication using SDM.
- Test the AAA RADIUS configuration.

Background

The most basic form of router access security is to create passwords for the console, vty, and aux lines. A user is prompted for only a password when accessing the router. Configuring a privileged EXEC mode enable secret password further improves security, but still only a basic password is required for each mode of access.

In addition to basic passwords, specific usernames or accounts with varying privilege levels can be defined in the local router database that can apply to the router as a whole. When the console, vty, or aux lines are configured to refer to this local database, the user is prompted for a username and a password when using any of these lines to access the router.

Additional control over the login process can be achieved using Authentication, Authorization, and Accounting (AAA). For basic authentication, AAA can be configured to access the local database for user logins, and fallback procedures can also be defined. However, this approach is not very scalable because it must be configured on every router. To take full advantage of AAA and achieve maximum scalability, it is used in conjunction with an external TACACS+ or RADIUS server database. When a user attempts to login, the router references the external server database to verify that the user is logging in with a valid username and password.

In this lab, you build a multi-router network and configure the routers and hosts. You use various CLI commands and SDM tools to configure routers with basic local authentication and local authentication using AAA. You install RADIUS software on an external computer and use AAA to authenticate users with the RADIUS server.

Note: The router commands and output in this lab are from a Cisco 1841 with Cisco IOS Release 12.4(20)T (Advance IP image). Other routers and Cisco IOS versions can be used. See the Router Interface Summary table at the end of the lab to determine which interface identifiers to use based on the equipment in the lab. Depending on the router model and Cisco IOS version, the commands available and output produced might vary from what is shown in this lab.

Note: Make sure that the routers and switches have been erased and have no startup configurations.

Required Resources

- 3 routers with SDM 2.5 installed (Cisco 1841 with Cisco IOS Release 12.4(20)T1 or comparable)
- 2 switches (Cisco 2960 or comparable)
- PC-A: Windows XP, Vista, or Windows Server with RADIUS server software available
- PC-C: Windows XP or Vista
- Serial and Ethernet cables as shown in the topology
- Rollover cables to configure the routers via the console

Part 1. Basic Network Device Configuration

In Part 1 of this lab, you set up the network topology and configure basic settings, such as the interface IP addresses, static routing, device access, and passwords.

All steps should be performed on routers R1 and R3. Only steps 1, 2, 3 and 6 need to be performed on R2. The procedure for R1 is shown here as an example.

Step 1: Cable the network as shown in the topology.

Attach the devices shown in the topology diagram, and cable as necessary.

Step 2: Configure basic settings for each router.

a. Configure host names as shown in the topology.

b. Configure the interface IP addresses as shown in the IP addressing table.

c. Configure a clock rate for the routers with a DCE serial cable attached to their serial interface.

```
R1(config)#interface S0/0/0
R1(config-if)#clock rate 64000
```

d. To prevent the router from attempting to translate incorrectly entered commands as though they were host names, disable DNS lookup.

```
R1(config)#no ip domain-lookup
```

Step 3: Configure static routing on the routers.

Configure a static default route from R1 to R2 and from R3 to R2.

Configure a static route from R2 to the R1 LAN and from R2 to the R3 LAN.

Step 4: Configure PC host IP settings.

Configure a static IP address, subnet mask, and default gateway for PC-A and PC-C, as shown in the IP addressing table.

Step 5: Verify connectivity between PC-A and R3.

a. Ping from R1 to R3.

Were the ping results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

b. Ping from PC-A on the R1 LAN to PC-C on the R3 LAN.

Were the ping results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Note: If you can ping from PC-A to PC-C, you have demonstrated that static routing is configured and functioning correctly. If you cannot ping but the device interfaces are up and IP addresses are correct, use the **show run** and **show ip route** commands to help identify routing protocol-related problems.

Step 6: Save the basic running configuration for each router.

Use the **Transfer > Capture text** option in HyperTerminal or some other method to capture the running configs for each router. Save the three files so that they can be used to restore configs later in the lab.

Step 7: Configure and encrypt passwords on R1 and R3.

Note: Passwords in this task are set to a minimum of 10 characters but are relatively simple for the benefit of performing the lab. More complex passwords are recommended in a production network.

For this step, configure the same settings for R1 and R3. Router R1 is shown here as an example.

a. Configure a minimum password length.

Use the **security passwords** command to set a minimum password length of 10 characters.

```
R1(config)#security passwords min-length 10
```

b. Configure the enable secret password on both routers.

```
R1(config)#enable secret cisco12345
```

c. Configure the basic console, auxiliary port, and vty lines.

d. Configure a console password and enable login for router R1. For additional security, the **exec-timeout** command causes the line to log out after 5 minutes of inactivity. The **logging synchronous** command prevents console messages from interrupting command entry.

Note: To avoid repetitive logins during this lab, the exec timeout can be set to 0 0, which prevents it from expiring. However, this is not considered a good security practice.

```
R1(config)#line console 0
R1(config-line)#password ciscoconpass
R1(config-line)#exec-timeout 5 0
```

```
R1(config-line)#login
R1(config-line)#logging synchronous
```

e. Configure a password for the aux port for router R1.

```
R1(config)#line aux 0
R1(config-line)#password ciscoauxpass
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
```

f. Configure the password on the vty lines for router R1.

```
R1(config)#line vty 0 4
R1(config-line)#password ciscovtypass
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
```

g. Encrypt the console, aux, and vty passwords.

```
R1(config)#service password-encryption
```

h. Issue the **show run** command. Can you read the console, aux, and vty passwords? Why or why not? _____

Step 8: Configure a login warning banner on routers R1 and R3.

a. Configure a warning to unauthorized uses using a message-of-the-day (MOTD) banner with the **banner motd** command. When a user connects to the router, the MOTD banner appears before the login prompt. In this example, the dollar sign ($) is used to start and end the message.

```
R1(config)#banner motd $Unauthorized access strictly prohibited and
prosecuted to the full extent of the law$
R1(config)#exit
```

b. Issue the **show run** command. What does the $ convert to in the output? _____

c. Exit privileged EXEC mode using the **disable** or **exit** command and press **Enter** to get started. Does the MOTD banner look like what you expected? _____

Note: If it does not, just recreate it using the **banner motd** command.

Step 9: Save the basic configurations.

Save the running configuration to the startup configuration from the privileged EXEC prompt.

```
R1#copy running-config startup-config
```

Part 2. Configure Local Authentication

In Part 2 of this lab, you configure a local username and password and change the access for the console, aux, and vty lines to reference the router's local database for valid usernames and passwords. Perform all steps on R1 and R3. The procedure for R1 is shown here.

Step 1: Configure the local user database.

a. Create a local user account with MD5 hashing to encrypt the password.

```
R1(config)#username user01 secret user01pass
```

b. Exit global configuration mode and display the running configuration. Can you read the user's password? _____

Step 2: Configure local authentication for the console line and login.

a. Set the console line to use the locally defined login usernames and passwords.

```
R1(config)#line console 0
R1(config-line)#login local
```

b. Exit to the initial router screen that displays: **R1 con0 is now available, Press RETURN to get started**.

c. Log in using the user01 account and password previously defined.

d. What is the difference between logging in at the console now and previously?

_____

e. After logging in, issue the **show run** command. Were you able to issue the command? Why or why not? _____

f. Enter privileged EXEC mode using the **enable** command. Were you prompted for a password? Why or why not? _____

Step 3: Test the new account by logging in from a Telnet session.

a. From PC-A, establish a Telnet session with R1.

```
PC-A>telnet 192.168.1.1
```

b. Were you prompted for a user account? Why or why not? _____

c. What password did you use to login? _____

d. Set the vty lines to use the locally defined login accounts.

```
R1(config)#line vty 0 4
R1(config-line)#login local
```

e. From PC-A, telnet R1 to R1 again.

```
PC-A>telnet 192.168.1.1
```

f. Were you prompted for a user account? Why or why not? _____

g. Log in as user01 with a password of user01pass.

h. While connected to R1 via Telnet, access privileged EXEC mode with the **enable** command.

i. What password did you use? _____

j. For added security, set the aux port to use the locally defined login accounts.

```
R1(config)#line aux 0
R1(config-line)#login local
```

k. End the Telnet session with the **exit** command.

Step 4: Save the configuration on R1.

a. Save the running configuration to the startup configuration from the privileged EXEC prompt.

```
R1#copy running-config startup-config
```

b. Use HyperTerminal or another means to save the R1 running configuration from Parts 1 and 2 of this lab and edit it so that it can be used to restore the R1 config later in the lab.

Note: Remove all occurrences of "- - More - -." Remove any commands that are not related to the items you configured in Parts 1 and 2 of the lab, such as the Cisco IOS version number, no service pad, and so on. Many commands are entered automatically by the Cisco IOS software. Also replace the encrypted passwords with the correct ones specified previously.

Step 5: Perform steps 1 through 4 on R3 and save the configuration.

a. Save the running configuration to the startup configuration from the privileged EXEC prompt.

```
R3#copy running-config startup-config
```

b. Use HyperTerminal or another means to save the R3 running configuration from Parts 1 and 2 of this lab and edit it so that it can be used to restore the R3 config later in the lab.

Part 3. Configure Local Authentication Using AAA on R3

Task 1. Configure the Local User Database Using Cisco IOS

Note: If you want to configure AAA using SDM, go to Task 3.

Step 1: Configure the local user database.

a. Create a local user account with MD5 hashing to encrypt the password.

```
R3(config)#username Admin01 privilege 15 secret Admin01pass
```

b. Exit global configuration mode and display the running configuration. Can you read the user's password?

_____

Task 2. Configure AAA Local Authentication Using Cisco IOS

Step 1: Enable AAA services.

a. On R3, enable services with the global configuration command **aaa new-model**. Because you are implementing local authentication, use local authentication as the first method, and no authentication as the secondary method.

If you were using an authentication method with a remote server, such as TACACS+ or RADIUS, you would configure a secondary authentication method for fallback if the server is unreachable. Normally, the secondary method is the local database. In this case, if no usernames are configured in the local database, the router allows all users login access to the device.

b. Enable AAA services.

```
R3(config)#aaa new-model
```

Step 2: Implement AAA services for console access using the local database.

a. Create the default login authentication list by issuing the **aaa authentication login default *method1[method2][method3]*** command with a method list using the **local** and **none** keywords.

```
R3(config)#aaa authentication login default local none
```

Note: If you do not set up a default login authentication list, you could get locked out of the router and be forced to use the password recovery procedure for your specific router.

b. Exit to the initial router screen that displays: **R3 con0 is now available, Press RETURN to get started**.

c. Log in to the console as Admin01 with a password of Admin01pass. Remember that passwords are case-sensitive. Were you able to log in? Why or why not?

_____

Note: If your session with the console port of the router times out, you might have to log in using the default authentication list.

d. Exit to the initial router screen that displays: **R3 con0 is now available, Press RETURN to get started**.

e. Attempt to log in to the console as baduser with any password. Were you able to log in? Why or why not? _____

f. If no user accounts are configured in the local database, which users are permitted to access the device? _____

Step 3: Create a AAA authentication profile for Telnet using the local database.

a. Create a unique authentication list for Telnet access to the router. This does not have the fallback of no authentication, so if there are no usernames in the local database, Telnet access is disabled. To create an authentication profile that is not the default, specify a list name of TELNET_LINES and apply it to the vty lines.

```
R3(config)#aaa authentication login TELNET_LINES local
R3(config)#line vty 0 4
R3(config-line)#login authentication TELNET_LINES
```

b. Verify that this authentication profile is used by opening a Telnet session from PC-C to R3.

```
PC-C>telnet 192.168.3.1
Trying 192.168.10.1 ... Open
```

c. Log in as Admin01 with a password of Admin01pass. Were you able to login? Why or why not?

_____

d. Exit the Telnet session with the **exit** command, and telnet to R3 again.

e. Attempt to log in as baduser with any password. Were you able to login? Why or why not?

_____

Task 3. (Optional) Configure AAA Local Authentication Using Cisco SDM

You can also use SDM to configure the router to support AAA.

Note: If you configured R3 AAA authentication using Cisco IOS commands in Tasks 1 and 2, you can skip this task. If you performed Tasks 1 and 2 and you want to perform this task, you should restore R3 to its basic configuration. See Part 4, Step 1 for the procedure to restore R3 to its basic configuration.

Even if you do not perform this task, read through the steps to become familiar with the SDM process.

Step 1: Implement AAA services and HTTP router access prior to starting SDM.

a. From the CLI global config mode, enable a new AAA model.

```
R3(config)#aaa new-model
```

b. Enable the HTTP server on R3 for SDM access.

```
R3(config)#ip http server
```

Note: For maximum security, enable secure http server using the **ip http secure-server** command.

Step 2: Access SDM and set command delivery preferences.

a. Open a browser on PC-C and start SDM by entering the R3 IP address 192.168.3.1 in the address field.

b. Log in with no username and the enable secret password cisco12345.

c. In the Password Needed – Networking dialog box, enter **cisco12345** in the Password field and click **Yes**.

d. Configure SDM to allow you to preview the commands before sending them to the router. Select **Edit** > **Preferences.**

e. In the User Preferences window, check the **Preview commands before delivering to router** check box and click **OK**.

Step 3: Create an administrative user with SDM.

a. Click the **Configure** button at the top of the screen**.**

b. Select **Additional Tasks > Router Access > User Accounts/View**.

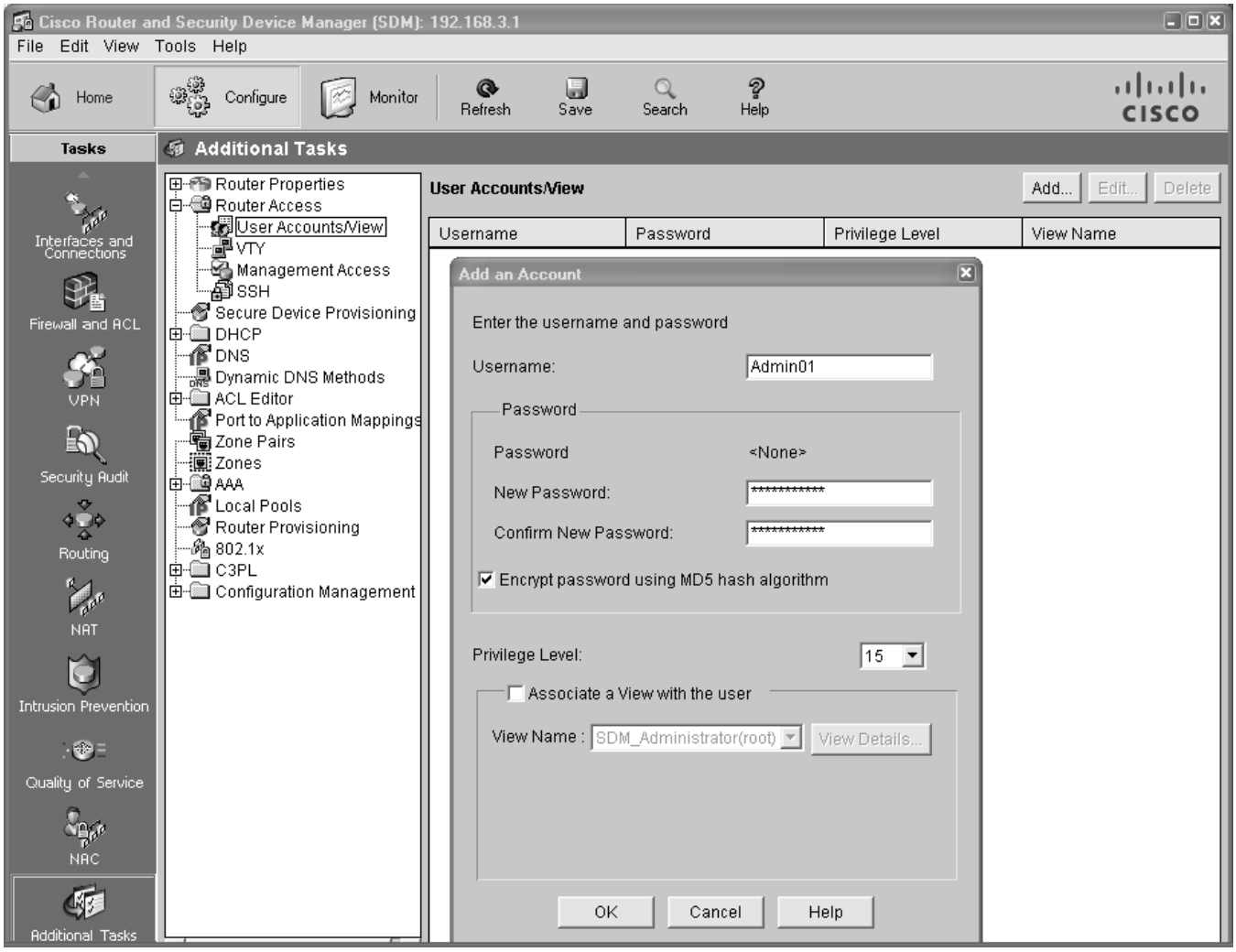
c. In the User Accounts/View window, click **Add**.

d. In the Add an Account window, enter **Admin01** in the Username field.

e. Enter the password **Admin01pass** in the New Password and Confirm New Password fields. (Remember, passwords are case-sensitive.)

f. Confirm that the **Encrypt Password using MD5 Hash Algorithm** check box is checked.

g. Select **15** from the Privilege Level drop-down list and click **OK**.



h. In the Deliver Configuration to Router window, make sure that the **Save running config to router's startup config** check box is checked, and click **Deliver**.

i. In the Commands Delivery Status window, click **OK**.

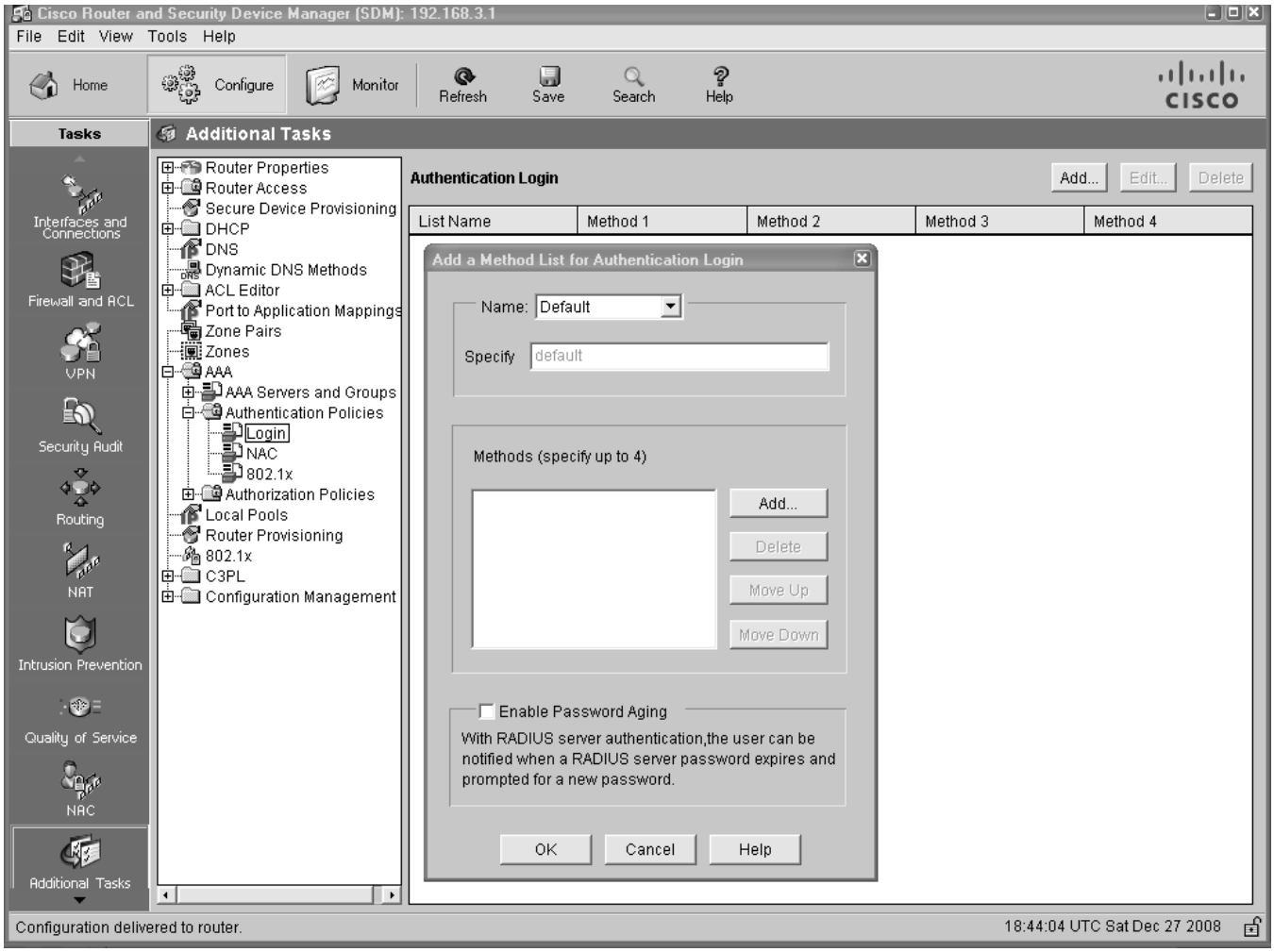
Step 4: Create a AAA method list for login.

a. Click the **Configure** button at the top of the screen**.**

b. Select **Additional Tasks > AAA > Authentication Policies > Login**.

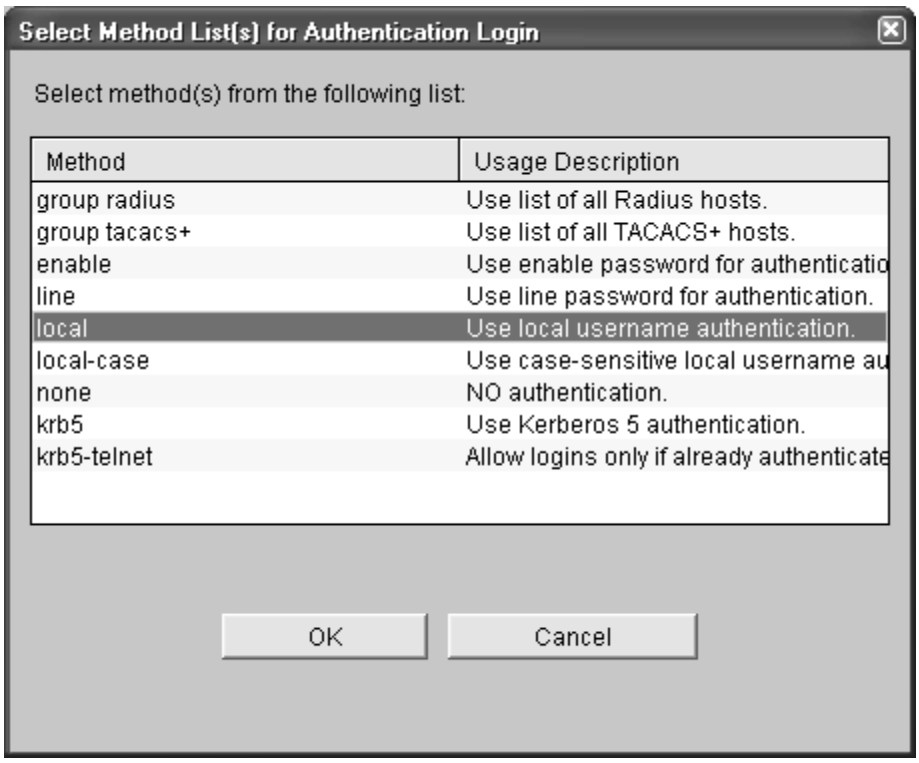
c. In the Authentication Login window, click **Add**.

d. In the Add a Method List for Authentication Login window, verify that **Default** is in the Name field.



e. Click **Add** in the Methods section.

f. In the Select Method List(s) for Authentication Login window, choose **local** and click **OK**. Take note of the other methods listed, which include RADIUS (group radius) and TACACS+ (group tacacs+).



g. Click **OK** to close the window.

h. Repeat steps 4f and 4g, and choose none as a second authentication method.

i. In the Deliver Configuration to Router window, make sure that the Save running config to router's startup config checkbox is checked, and click Deliver. In the Commands Delivery Status window, click **OK**.

j. What command was delivered to the router?

_____

Step 5: Verify the AAA username and profile for console login.

a. Exit to the initial router screen that displays: **R3 con0 is now available, Press RETURN to get started**.

b. Log in to the console as Admin01 with a password of Admin01pass. Were you able to login? Why or why not? _____

c. Exit to the initial router screen that displays: **R3 con0 is now available, Press RETURN to get started**.

d. Attempt to log in to the console as baduser. Were you able to login? Why or why not?

_____

e. If no user accounts are configured in the local database, which users are permitted to access the device?

_____

f. Log in to the console as Admin01 with a password of Admin01pass. Access privileged EXEC mode using the enable secret password cisco12345 and then show the running config. What commands are associated with the SDM session?

_____
_____
_____

Task 4. Observe AAA Authentication Using Cisco IOS Debug

In this task, you use the **debug** command to observe successful and unsuccessful authentication attempts.

Step 1: Verify that the system clock and debug time stamps are configured correctly.

a. From the R3 user or privileged EXEC mode prompt, use the **show clock** command to determine what the current time is for the router. If the time and date are incorrect, set the time from privileged EXEC mode with the command **clock set HH:MM:SS DD month YYYY.** An example is provided here for R3.

```
R3#clock set 14:15:00 26 December 2008
```

b. Verify that detailed time-stamp information is available for your debug output using the **show run** command. This command displays all lines in the running config that include the text "timestamps".

```
R3#show run | include timestamps

service timestamps debug datetime msec
service timestamps log datetime msec
```

c. If the **service timestamps debug** command is not present, enter it in global config mode.

```
R3(config)#service timestamps debug datetime msec
R3(config)#exit
```

d. Save the running configuration to the startup configuration from the privileged EXEC prompt.

```
R3#copy running-config startup-config
```

Step 2: Use debug to verify user access.

a. Activate debugging for AAA authentication.

```
R3#debug aaa authentication
AAA Authentication debugging is on
```

b. Start a Telnet session from PC-C to R3.

c. Log in with username Admin01 and password Admin01pass. Observe the AAA authentication events in the console session window. Debug messages similar to the following should be displayed.

```
R3#
Dec 26 14:36:42.323: AAA/BIND(000000A5): Bind i/f
Dec 26 14:36:42.323: AAA/AUTHEN/LOGIN (000000A5): Pick method list
'default'
```

d. From the Telnet window, enter privileged EXEC mode. Use the enable secret password of cisco12345. Debug messages similar to the following should be displayed. In the third entry, note the username (Admin01), virtual port number (tty194), and remote Telnet client address (192.168.3.3). Also note that the last status entry is "PASS."

```
R3#
Dec 26 14:40:54.431: AAA: parse name=tty194 idb type=-1 tty=-1
Dec 26 14:40:54.431: AAA: name=tty194 flags=0x11 type=5 shelf=0 slot=0
adapter=0 port=194 channel=0
```

```
Dec 26 14:40:54.431: AAA/MEMORY: create_user (0x64BB5510)
user='Admin01' ruser=' NULL' ds0=0 port='tty194' rem_addr='192.168.3.3'
authen_type=ASCII service=ENABLE priv=15 initial_task_id='0', vrf=
(id=0)
Dec 26 14:40:54.431: AAA/AUTHEN/START (2467624222): port='tty194'
list='' action=LOGIN service=ENABLE
Dec 26 14:40:54.431: AAA/AUTHEN/START (2467624222): non-console enable
- default to enable password
Dec 26 14:40:54.431: AAA/AUTHEN/START (2467624222): Method=ENABLE
R3#
Dec 26 14:40:54.435: AAA/AUTHEN(2467624222): Status=GETPASS
R3#
Dec 26 14:40:59.275: AAA/AUTHEN/CONT (2467624222): continue_login
(user='(undef)')
Dec 26 14:40:59.275: AAA/AUTHEN(2467624222): Status=GETPASS
Dec 26 14:40:59.275: AAA/AUTHEN/CONT (2467624222): Method=ENABLE
Dec 26 14:40:59.287: AAA/AUTHEN(2467624222): Status=PASS
Dec 26 14:40:59.287: AAA/MEMORY: free_user (0x64BB5510) user='NULL'
ruser='NULL' port='tty194' rem_addr='192.168.3.3' authen_type=ASCII
service=ENABLE priv=15 v
rf= (id=0)
```

e. From the Telnet window, exit privileged EXEC mode using the `disable` command. Try to enter privileged EXEC mode again, but use a bad password this time. Observe the debug output on R3, noting that the status is “FAIL” this time.

```
Dec 26 15:46:54.027: AAA/AUTHEN(2175919868): Status=GETPASS
Dec 26 15:46:54.027: AAA/AUTHEN/CONT (2175919868): Method=ENABLE
Dec 26 15:46:54.039: AAA/AUTHEN(2175919868): password incorrect
Dec 26 15:46:54.039: AAA/AUTHEN(2175919868): Status=FAIL
Dec 26 15:46:54.039: AAA/MEMORY: free_user (0x6615BFE4) user='NULL'
ruser='NULL'
 port='tty194' rem_addr='192.168.3.3' authen_type=ASCII service=ENABLE
priv=15 v
rf= (id=0)
```

f. From the Telnet window, exit the Telnet session to the router. Then try to open a Telnet session to the router again, but this time try to log in with the username Admin01 and a bad password. From the console window, the debug output should look similar to the following.

```
Dec 26 15:49:32.339: AAA/AUTHEN/LOGIN (000000AA): Pick method list
'default'
```

What message was displayed on the Telnet client screen? _____

g. Turn off all debugging using the `undebug all` command at the privileged EXEC prompt.

Part 4. Configure Centralized Authentication Using AAA and RADIUS.

In Part 4 of the lab, you install RADIUS server software on PC-A. You then configure router R1 to access the external RADIUS server for user authentication. The freeware server WinRadius is used for this section of the lab.

Task 1. Restore Router R1 to Its Basic Settings

To avoid confusion as to what was already entered and the AAA RADIUS configuration, start by restoring router R1 to its basic configuration as performed in Parts 1 and 2 of this lab.

Step 1: Erase and reload the router.

a. Connect to the R1 console, and log in with the username Admin01 and password Admin01pass.

b. Enter privileged EXEC mode with the password cisco12345.

c. Erase the startup config and then issue the **reload** command to restart the router.

Step 2: Restore the basic configuration.

a. When the router restarts, enter privileged EXEC mode with the **enable** command, and then enter global config mode. Use the HyperTerminal **Transfer > Send File** function, cut and paste or use another method to load the basic startup config for R1 that was created and saved in Part 2 of this lab.

b. Test connectivity by pinging from host PC-A to PC-C. If the pings are not successful, troubleshoot the router and PC configurations until they are.

c. If you are logged out of the console, log in again as user01 with password user01pass, and access privileged EXEC mode with the password cisco12345.

d. Save the running config to the startup config using the **copy run start** command.

Task 2. Download and Install a RADIUS Server on PC-A

There are a number of RADIUS servers available, both freeware and for cost. This lab uses WinRadius, a freeware standards-based RADIUS server that runs on Windows XP and most other Windows operating systems. The free version of the software can support only five usernames.

Step 1: Download the WinRadius software.

a. Create a folder named WinRadius on your desktop or other location in which to store the files.

b. Download the latest version from http://www.suggestsoft.com/soft/itconsult2000/winradius/.

The publisher asks that you provide your email address and send them feedback after you install and try WinRadius. You may skip the survey if desired.

c. Save the downloaded zip file in the folder you created in Step 1a, and extract the zipped files to the same folder. There is no installation setup. The extracted WinRadius.exe file is executable.

d. You may create a shortcut on your desktop for WinRadius.exe.

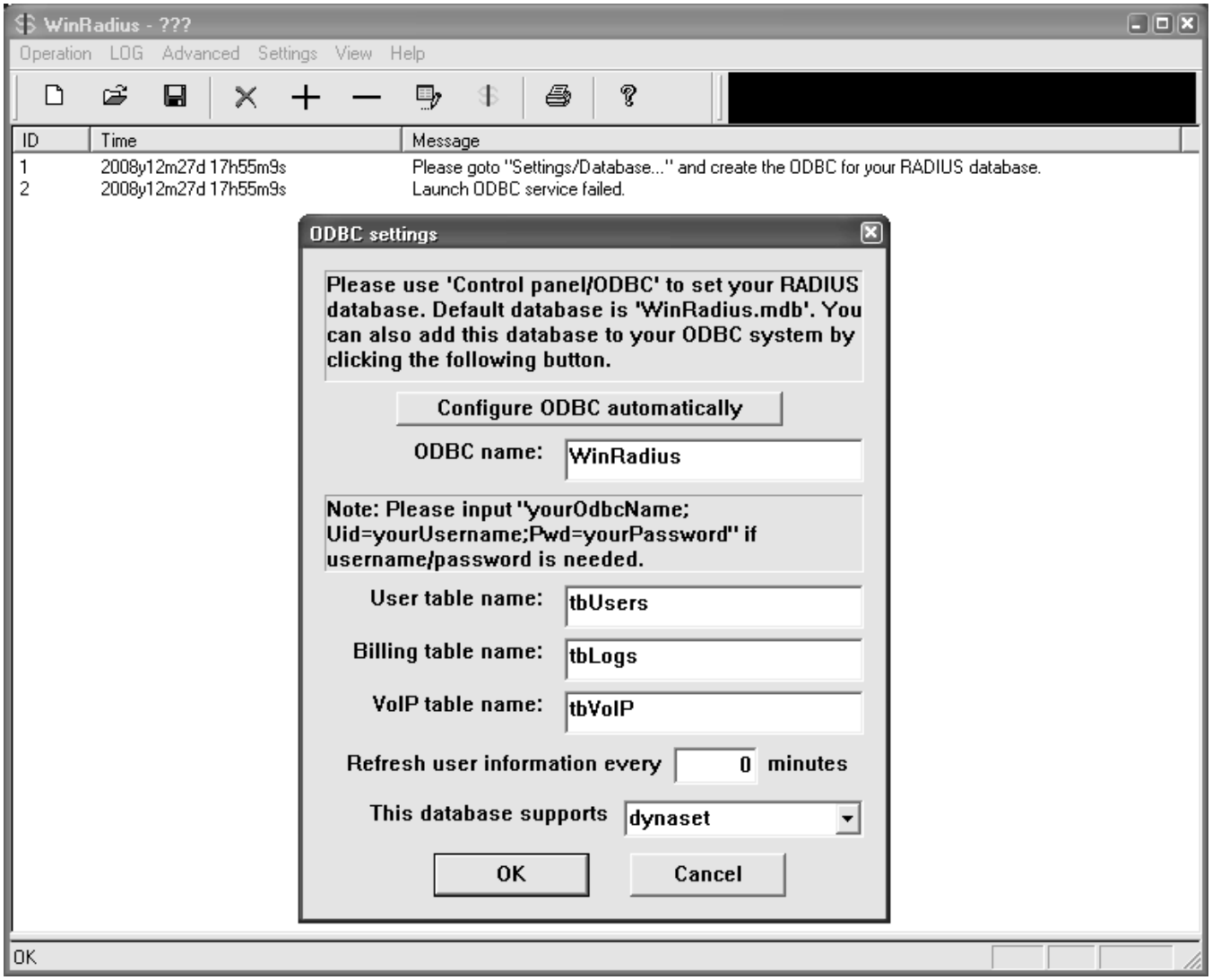
Step 2: Configure the WinRadius server database.

a. Start the WinRadius.exe application. WinRadius uses a local database in which it stores user information. When the application is started for the first time, the following messages are displayed

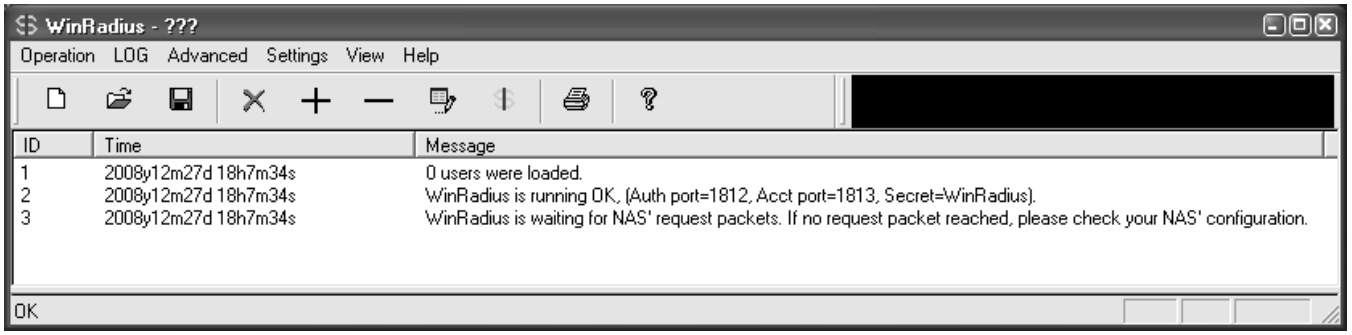
```
Please go to "Settings/Database and create the ODBC for your RADIUS
database.

Launch ODBC failed.
```

b. Select **Settings > Database** from the main menu and the following screen is displayed. Click the **Configure ODBC automatically** button and then click **OK**. You should see a message that the ODBC was created successfully. Exit WinRadius and restart the application for the changes to take effect.



c. When WinRadius starts again, you should see messages similar to the following displayed.



d. On which ports is WinRadius listening for authentication and accounting?

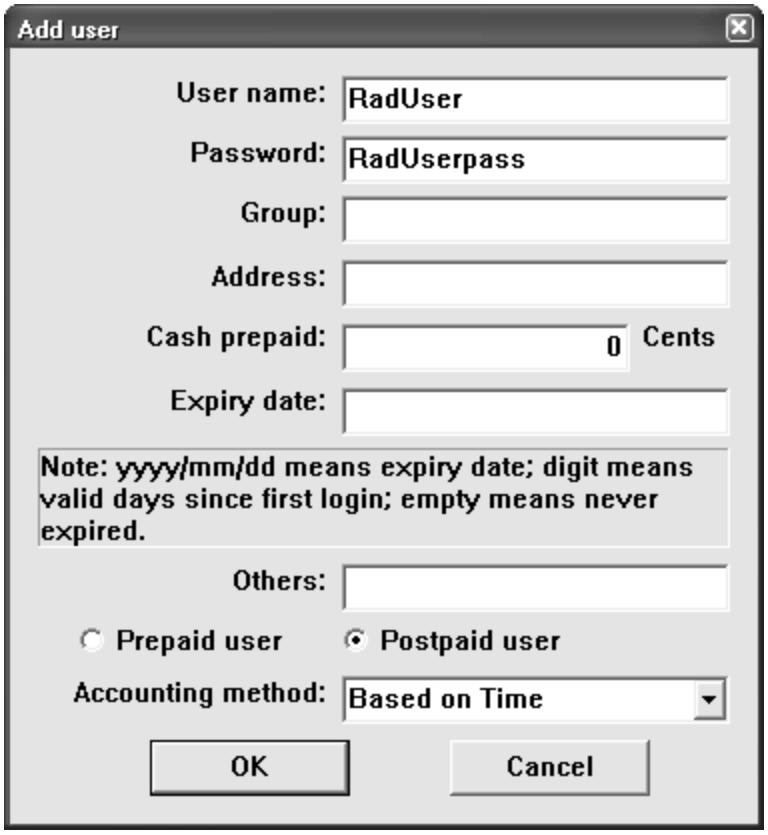
_____

Step 3: Configure users and passwords on the WinRadius server.

Note: The free version of WinRadius can support only five usernames. The usernames are lost if you exit the application and restart it. Any usernames created in previous sessions must be recreated. Note that the first message in the previous screen shows that zero users were loaded. No users had been created prior to this, but this message is displayed each time WinRadius is started, regardless of whether users were created or not.

a. From the main menu, select **Operation > Add User.**

b. Enter the username RadUser with a password of RadUserpass. Remember that passwords are case-sensitive.



c. Click **OK**. You should see a message on the log screen that the user was added successfully.

Step 4: Clear the log display.

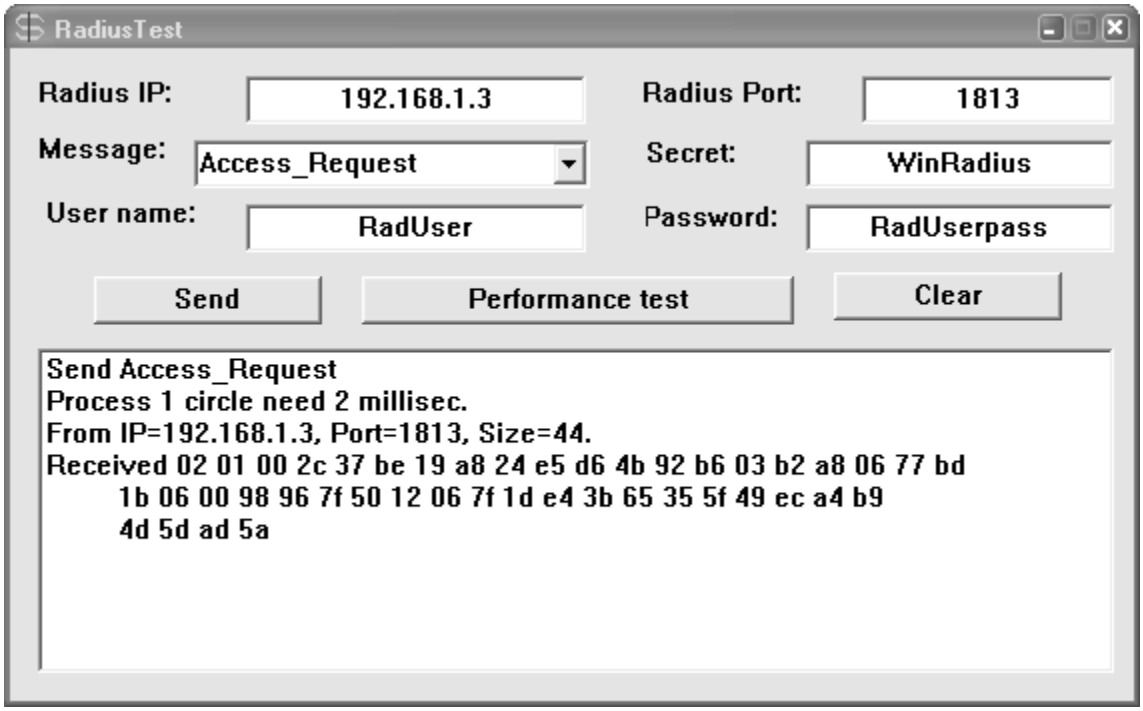
From the main menu, select **Log > Clear**.

Step 5: Test the new user added using the WinRadius test utility.

a. A WinRadius testing utility is included in the downloaded zip file. Navigate to the folder where you unzipped the WinRadius.zip file and locate the file named RadiusTest.exe.

b. Start the RadiusTest application, and enter the IP address of this RADIUS server (192.168.1.3), username RadUser, and password RadUserpass as shown. Do not change the default RADIUS port number of 1813 and the RADIUS password of WinRadius.

c. Click **Send** and you should see a Send Access_Request message indicating the server at 192.168.1.3, port number 1813, received 44 hexadecimal characters. On the WinRadius log display, you should also see a message indicating that user RadUser was authenticated successfully.



d. Close the RadiusTest application.

Task 3. Configure R1 AAA Services and Access the RADIUS Server Using Cisco IOS

Note: If you want to configure AAA using SDM, go to Task 5.

Step 1: Enable AAA on R1.

Use the **aaa new-model** command in global configuration mode to enable AAA.

```
R1(config)#aaa new-model
```

Step 2: Configure the default login authentication list.

a. Configure the list to first use RADIUS for the authentication service, and then none. If no RADIUS server can be reached and authentication cannot be performed, the router globally allows access without authentication. This is a safeguard measure in case the router starts up without connectivity to an active RADIUS server.

```
R1(config)#aaa authentication login default group radius none
```

b. You could alternatively configure local authentication as the backup authentication method instead.

Note: If you do not set up a default login authentication list, you could get locked out of the router and need to use the password recovery procedure for your specific router.

Step 3: Specify a RADIUS server.

Use the **radius-server host *hostname* key *key*** command to point to the RADIUS server. The *hostname* parameter accepts either a host name or an IP address. Use the IP address of the RADIUS server, PC-A (192.168.1.3). The key is a secret password shared between the RADIUS server and the RADIUS client (R1 in this case) and used to authenticate the connection between the router and the server before the user authentication process takes place. The RADIUS client may be a Network Access Server (NAS), but router R1 plays that role in this lab. Use the default NAS secret password of WinRadius specified on the RADIUS server (see Task 2, Step 5). Remember that passwords are case-sensitive.

```
R1(config)#radius-server host 192.168.1.3 key WinRadius
```

Task 4. Test the AAA RADIUS Configuration

Step 1: Verify connectivity between R1 and the computer running the RADIUS server.

Ping from R1 to PC-A.

```
R1#ping 192.168.1.3
```

If the pings were not successful, troubleshoot the PC and router configuration before continuing.

Step 2: Test your configuration.

a. If you restarted the WinRadius server, you must recreate the user RadUser with a password of RadUserpass by selecting **Operation > Add User.**

b. Clear the log on the WinRadius server by selecting **Log > Clear** from the main menu.

c. On R1, exit to the initial router screen that displays: **R1 con0 is now available, Press RETURN to get started**.

d. Test your configuration by logging in to the console on R1 using the username RadUser and the password of RadUserpass. Were you able to gain access to the user EXEC prompt and, if so, was there any delay? _____

e. Exit to the initial router screen that displays: **R1 con0 is now available, Press RETURN to get started.**

f. Test your configuration again by logging in to the console on R1 using the nonexistent username of Userxxx and the password of Userxxxpass. Were you able to gain access to the user EXEC prompt? Why or why not? _____

g. Were any messages displayed on the RADIUS server log for either login? _____

h. Why was a nonexistent username able to access the router and no messages are displayed on the RADIUS server log screen? _____

i. When the RADIUS server is unavailable, messages similar to the following are typically displayed after attempted logins.

```
*Dec 26 16:46:54.039: %RADIUS-4-RADIUS_DEAD: RADIUS server
192.168.1.3:1645,1646 is not responding.
*Dec 26 15:46:54.039: %RADIUS-4-RADIUS_ALIVE: RADIUS server
192.168.1.3:1645,1646 is being marked alive.
```

Step 3: Troubleshoot router-to-RADIUS server communication.

a. Check the default Cisco IOS RADIUS UDP port numbers used on R1 with the **radius-server host** command and the Cisco IOS Help function.

```
R1(config)#radius-server host 192.168.1.3 ?
  acct-port   UDP port for RADIUS accounting server (default is 1646)
  alias         1-8 aliases for this server (max. 8)
  auth-port   UDP port for RADIUS authentication server (default is 1645)
```

< Output omitted >

b. Check the R1 running configuration for lines containing the command **radius**. The following command display all running config lines that include the text “radius”.

```
R1#show run | incl radius
aaa authentication login default group radius none
radius-server host 192.168.1.3 auth-port 1645 acct-port 1646 key 7
097B47072B04131B1E1F
```

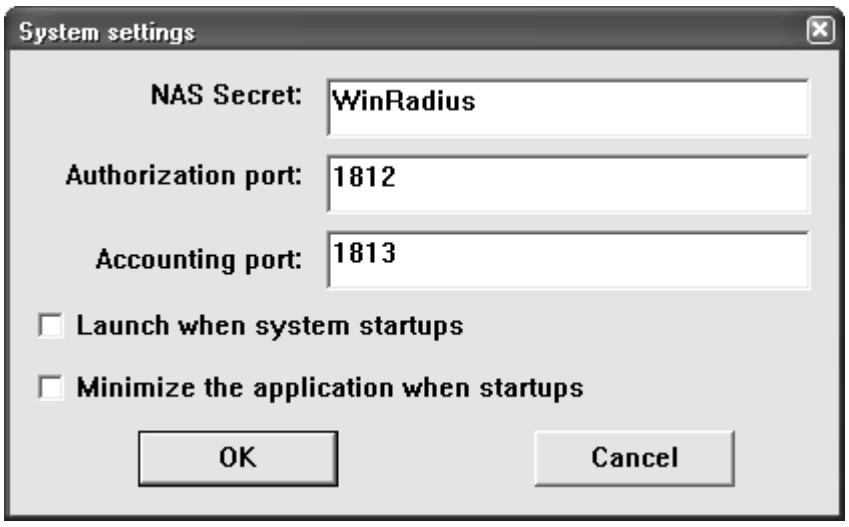
< Output omitted >

c. What are the default R1 Cisco IOS UDP port numbers for the RADIUS server?

_____

Step 4: Check the default port numbers on the WinRadius server on PC-A.

From the WinRadius main menu select **Settings > System**.



What are the default WinRadius UDP port numbers? _____

Note: The early deployment of RADIUS was done using UDP port number 1645 for authentication and 1646 for accounting, which conflicts with the datametrics service. Because of this conflict, RFC 2865 officially assigned port numbers 1812 and 1813 for RADIUS.

Step 5: Change the RADIUS port numbers on R1 to match the WinRadius server.

Unless specified otherwise, the Cisco IOS RADIUS configuration defaults to UDP port numbers 1645 and 1646. Either the router Cisco IOS port numbers must be changed to match the port number of the RADIUS

server or the RADIUS server port numbers must be changed to match the port numbers of the Cisco IOS router. In this step, you modify the IOS port numbers to those of the RADIUS server, which are specified in RFC 2865.

Remove the previous configuration using the following command.

```
R1(config)#no radius-server host 192.168.1.3 auth-port 1645 acct-port
1646
```

Issue the **`radius-server host`** command again and this time specify port numbers 1812 and 1813, along with the IP address and secret key for the RADIUS server.

```
R1(config)#radius-server host 192.168.1.3 auth-port 1812 acct-port 1813
key WinRadius
```

Step 6: Test your configuration by logging into the console on R1.

a. Exit to the initial router screen that displays: R1 con0 is now available, Press RETURN to get started.

b. Log in again with the username of RadUser and password of RadUserpass. Were you able to login? Was there any delay this time?

_____

c. The following message should display on the RADIUS server log.

```
User (RadUser) authenticate OK.
```

d. Exit to the initial router screen that displays: R1 con0 is now available, Press RETURN to get started.

e. Log in again using an invalid username of Userxxx and the password of Userxxxpass. Were you able to login?

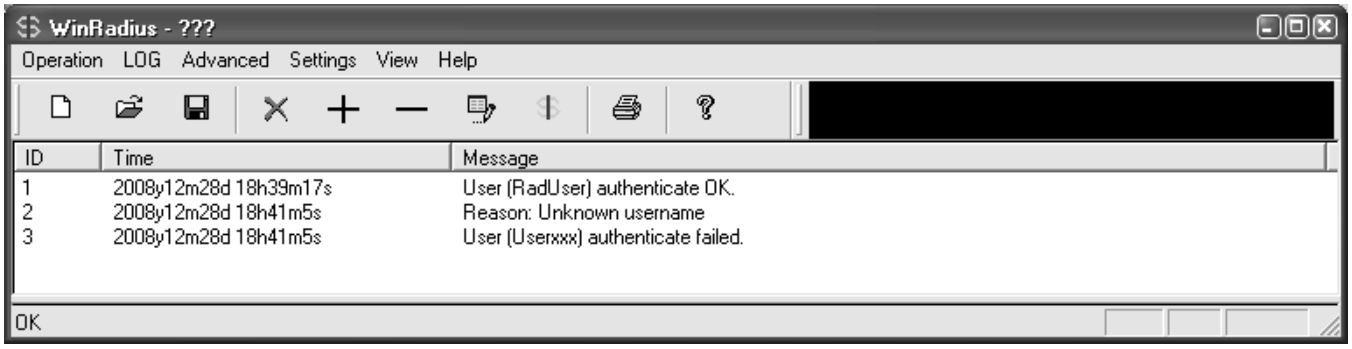
_____

What message was displayed on the router? _____

The following messages should display on the RADIUS server log.

Reason: Unknown username

User (Userxxx) authenticate failed



Step 7: Create an authentication method list for Telnet and test it.

a. Create a unique authentication method list for Telnet access to the router. This does not have the fallback of no authentication, so if there is no access to the RADIUS server, Telnet access is disabled. Name the authentication method list TELNET_LINES.

```
R1(config)#aaa authentication login TELNET_LINES group radius
```

b. Apply the list to the vty lines on the router using the login authentication command.

```
R1(config)#line vty 0 4
R1(config-line)#login authentication TELNET_LINES
```

c. Telnet from PC-A to R1, and log in with the username RadUser and the password of RadUserpass. Were you able to gain access to log in? _____

d. Exit the Telnet session, and telnet from PC-A to R1 again. Log in with the username Userxxx and the password of Userxxxpass. Were you able to log in? _____

Task 5. (Optional) Configure R1 AAA Services and Access the RADIUS Server Using SDM

You can also use SDM to configure the router to access the external RADIUS server.

Note: If you configured R1 to access the external RADIUS server using Cisco IOS in Task 3, you can skip this task. If you performed Task 3 and you want to perform this task, restore the router to its basic configuration as described Task 1 of this part, except log in initially as RadUser with the password RadUserpass**.** If the RADIUS server is unavailable at this time, you will still be able to log in to the console.

If you do not perform this task, read through the steps to become familiar with the SDM process.

Step 1: Implement AAA services and HTTP router access prior to starting SDM.

a. From the CLI global config mode, enable a new AAA model.

```
R1(config)#aaa new-model
```

b. Enable the HTTP server on R1.

```
R1(config)#ip http server
```

Step 2: Access SDM and enable the command preview option.

a. Open a browser on PC-A. Start SDM by entering the R1 IP address 192.168.1.1 in the address field.

b. Log in with no username and the enable secret password cisco12345.

c. In the Password Needed – Networking dialog box, enter **cisco12345** in the Password field and click **Yes**.

d. Configure SDM to allow you to preview commands before sending them to the router. Select **Edit** > **Preferences.**

e. In the User Preferences window, check the **Preview commands before delivering to router** check box and click **OK**.

Step 3: Configure R1 AAA to access the WinRADIUS server.

a. Click the **Configure** button at the top of the screen**.**

b. Select **Additional Tasks > AAA > AAA Servers and Groups > AAA Servers**.

c. In the AAA Servers window, click **Add**.

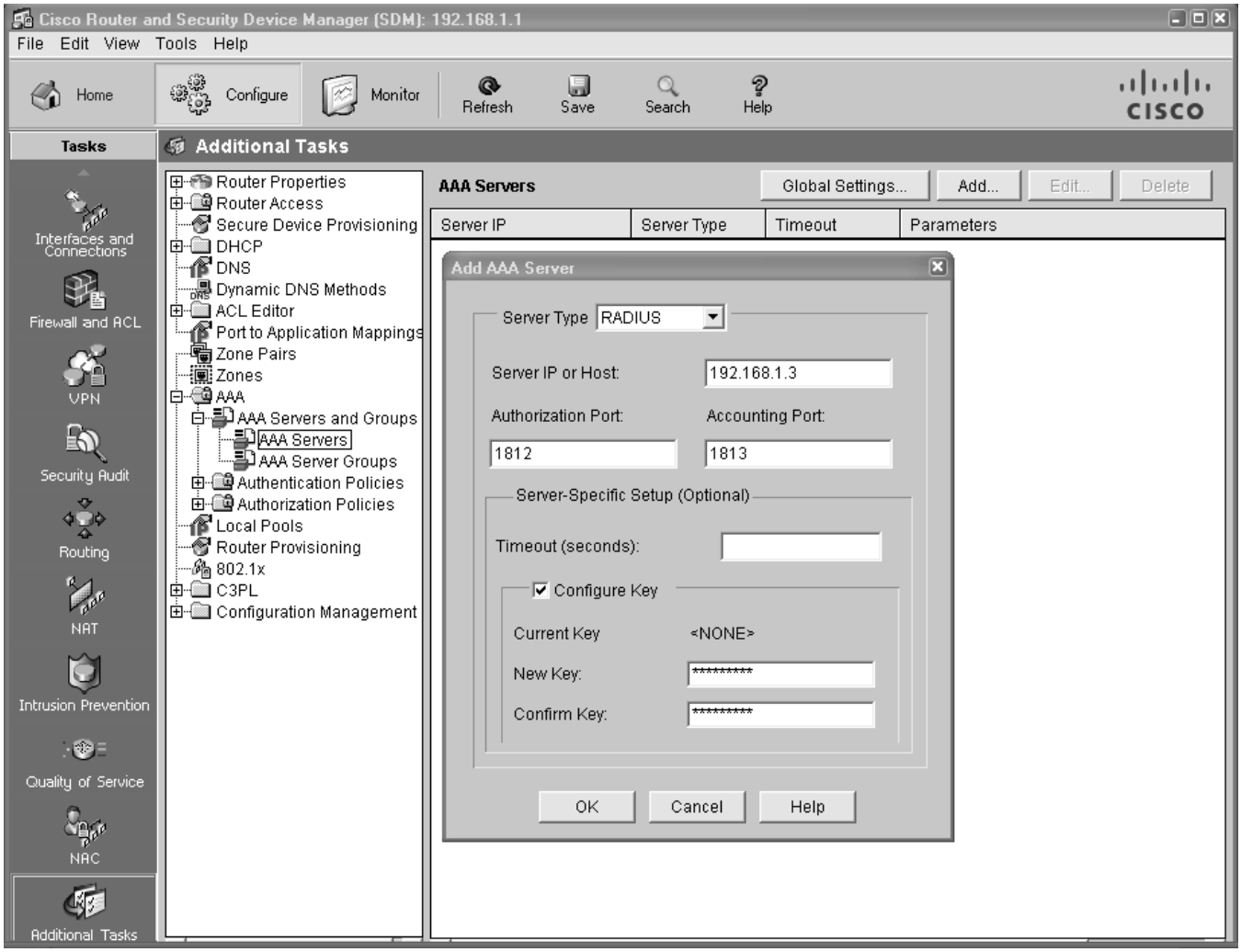
d. In the Add AAA Server window, verify that **RADIUS** is in the Server Type field.

e. In the Server IP or Host field, enter the IP address of PC-A, **192.168.1.3**.

f. Change the **Authorization Port** from 1645 to 1812, and change the **Accounting Port** from 1646 to 1813 to match the RADIUS server port number settings.

g. Check the **Configure Key** check box.

h. Enter **WinRadius** in both the New Key and Confirm Key fields.



i. In the Deliver Configuration to Router window, click **Deliver,** and in the Commands Delivery Status window, click **OK**.

j. What command was delivered to the router?

_____

Step 4: Configure the R1 AAA login method list for RADIUS.

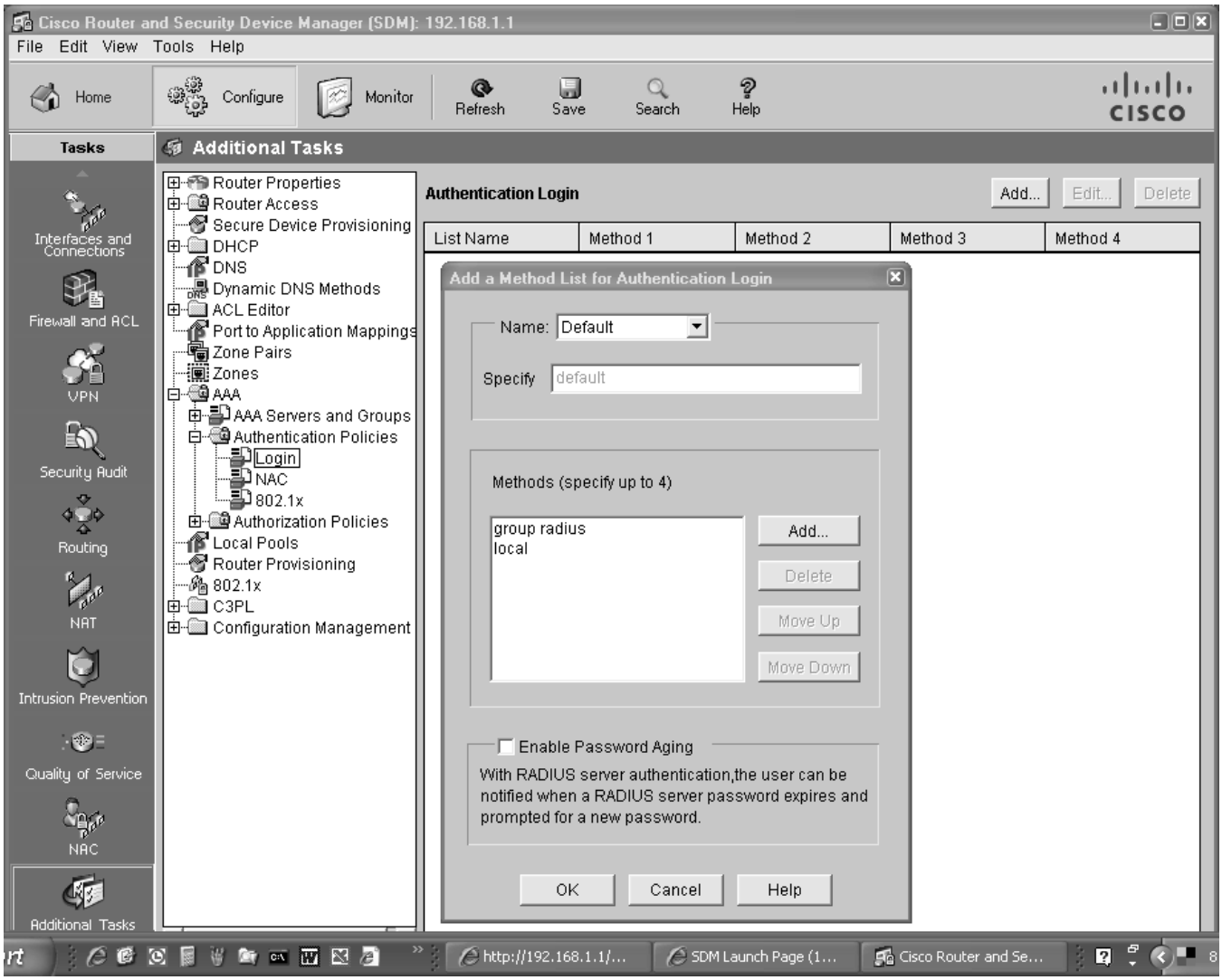
a. Click the **Configure** button at the top of the screen**.**

b. Select **Additional Tasks > AAA > Authentication Policies > Login.**

c. In the **Authentication Login** window, click **Add**.

d. In the **Select Method List(s) for Authentication Login** window, choose **group radius** and click **OK**.

e. In the **Select Method List(s) for Authentication Login** window, choose **local** as a second method and click **OK**.



f. In the Deliver Configuration to Router window, click Deliver and in the Commands Delivery Status window, click OK.

g. What command(s) were delivered to the router?

_____

Step 5: Test your configuration.

If you restarted the RADIUS server, you must recreate the user **RadUser** with a password of **RadUserpass** by selecting **Operation > Add Use**r.

a. Clear the log on the WinRadius server by selecting **Log > Clear**.

b. Test your configuration by opening a Telnet session from PC-A to R1.

```
C:>telnet 192.168.1.1
```

c. At the login prompt, enter the username **RadUser** defined on the RADIUS server and a password of **RadUserpass**.

d. Were you able to login to R1? _____

Task 6. Reflection

Why would an organization want to use a centralized authentication server rather than configuring users and passwords on each individual router?

_____
_____
_____
_____

Contrast local authentication and local authentication with AAA.

_____
_____
_____
_____

Based on the Academy online course content, web research, and the use of RADIUS in this lab, compare and contrast RADIUS with TACACS+.

_____
_____
_____
_____
_____
_____

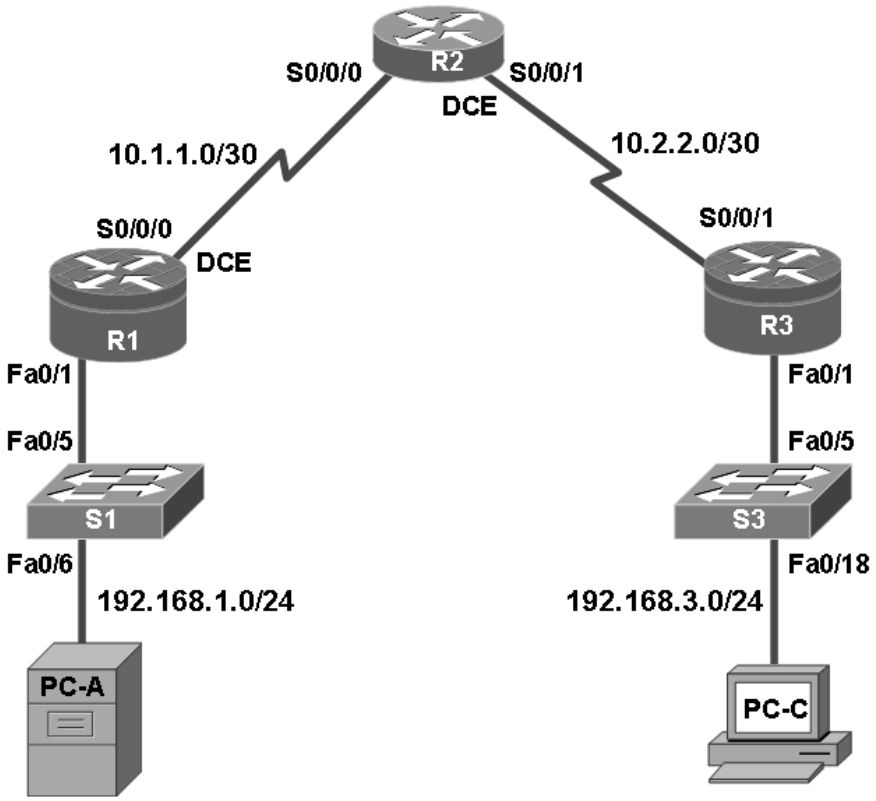
Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1700	Fast Ethernet 0 (FA0)	Fast Ethernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2600	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
2800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Chapter 4: Lab A: Configuring CBAC and Zone-Based Firewalls

Topology



IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	FA0/1	192.168.1.1	255.255.255.0	N/A	S1 FA0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	FA0/1	192.168.3.1	255.255.255.0	N/A	S3 FA0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 FA0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 FA0/18

Objectives

Part 1: Basic Router Configuration

- Configure host names, interface IP addresses, and access passwords.

- Configure the EIGRP dynamic routing protocol.
- Use the Nmap port scanner to test for router vulnerabilities

Part 2: Configuring a Context-Based Access Control (CBAC) Firewall

- Configure CBAC using AutoSecure.
- Examine the resulting CBAC configuration.
- Verify the firewall functionality.

Part 3: Configuring a Zone-Based Policy Firewall (ZBF, ZPF or ZFW)

- Configure a Zone-Based Policy Firewall using SDM.
- Examine the resulting CBAC configuration.
- Use SDM Monitor to verify configuration.

Background

The most basic form of a Cisco IOS firewall uses access control lists (ACLs) with filtering IP traffic and monitoring established traffic patterns. This is referred to as a traditional Cisco IOS firewall. In more recent Cisco IOS versions, this approach has evolved into a method called context-based access control (CBAC) or Inspect/CBAC, which is based on Stateful Packet Inspection (SPI). CBAC makes creating firewalls easier and gives the administrator greater control over various types of application traffic originating from inside and outside of the protected network. When Cisco IOS AutoSecure is run, it prompts to create a CBAC firewall and generates a basic configuration. For simple networks with a single inside and outside interface, CBAC is easier to configure than traditional Cisco IOS firewalls. Configurations with multiple interfaces and DMZ requirements can become complex and difficult to manage using CBAC.

The current method used with SDM for securing router is called a zone-based policy firewall (may be abbreviated as ZBF, ZPF or ZFW). A zone-based policy firewall provides the same type of functionally as CBAC, but is better suited for multiple interfaces that have similar or varying security requirements. While AutoSecure generates a CBAC firewall, SDM generates a ZBF firewall by default.

In this lab, you build a multi-router network and configure the routers and hosts. You use AutoSecure to configure a CBAC firewall and SDM to configure a zone-based policy firewall.

Note: The router commands and output in this lab are from a Cisco 1841 with Cisco IOS Release 12.4(20)T (Advanced IP image). Other routers and Cisco IOS versions can be used. See the Router Interface Summary table at the end of the lab to determine which interface identifiers to use based on the equipment in the lab. Depending on the router model and Cisco IOS version, the commands available and output produced might vary from what is shown in this lab.

Note: Make sure that the routers and the switches have been erased and have no startup configurations.

Required Resources

- 3 routers with SDM 2.5 installed (Cisco 1841 with Cisco IOS Release 12.4(20)T1 or comparable)
- 2 switches (Cisco 2960 or comparable)
- PC-A (Windows XP or Vista)
- PC-C (Windows XP or Vista)
- Serial and Ethernet cables as shown in the topology

- Rollover cables to configure the routers via the console

Part 1. Basic Router Configuration

In Part 1 of this lab, you set up the network topology and configure basic settings, such as the interface IP addresses, dynamic routing, device access, and passwords.

Note: All tasks should be performed on routers R1, R2 and R3. The procedure for R1 is shown here as an example.

Task 1. Configure Basic Router Settings

Step 1: Cable the network as shown in the topology.

Attach the devices shown in the topology diagram, and cable as necessary.

Step 2: Configure basic settings for each router.

a. Configure host names as shown in the topology.

b. Configure the interface IP addresses as shown in the IP addressing table.

c. Configure a clock rate for the serial router interfaces with a DCE serial cable attached.

```
R1(config)#interface S0/0/0
R1(config-if)#clock rate 64000
```

Step 3: Disable DNS lookup.

To prevent the router from attempting to translate incorrectly entered commands, disable DNS lookup.

```
R1(config)#no ip domain-lookup
```

Step 4: Configure the EIGRP routing protocol on R1, R2, and R3.

On R1, use the following commands.

```
R1(config)#router eigrp 101
R1(config-router)#network 192.168.1.0 0.0.0.255
R1(config-router)#network 10.1.1.0 0.0.0.3
R1(config-router)#no auto-summary
```

On R2, use the following commands.

```
R2(config)#router eigrp 101
R2(config-router)#network 10.1.1.0 0.0.0.3
R2(config-router)#network 10.2.2.0 0.0.0.3
R2(config-router)#no auto-summary
```

On R3, use the following commands.

```
R3(config)#router eigrp 101
R3(config-router)#network 192.168.3.0 0.0.0.255
R3(config-router)#network 10.2.2.0 0.0.0.3
R3(config-router)#no auto-summary
```

Step 5: Configure PC host IP settings.

a. Configure a static IP address, subnet mask, and default gateway for PC-A, as shown in the IP addressing table.

b, Configure a static IP address, subnet mask, and default gateway for PC-C, as shown in the IP addressing table.

Step 6: Verify basic network connectivity.

a. Ping from R1 to R3.

Were the results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

b. Ping from PC-A on the R1 LAN to PC-C on the R3 LAN.

Were the results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Note: If you can ping from PC-A to PC-C, you have demonstrated that the EIGRP routing protocol is configured and functioning correctly. If you cannot ping but the device interfaces are up and IP addresses are correct, use the **show run** and **show ip route** commands to help identify routing protocol-related problems.

Step 7: Configure a minimum password length.

Note: Passwords in this lab are set to a minimum of 10 characters but are relatively simple for the benefit of performing the lab. More complex passwords are recommended in a production network.

Use the **security passwords** command to set a minimum password length of 10 characters.

```
R1(config)# security passwords min-length 10
```

Step 8: Configure basic console, auxiliary port, and vty lines.

a. Configure a console password and enable login for router R1. For additional security, the **exec-timeout** command causes the line to log out after 5 minutes of inactivity. The **logging synchronous** command prevents console messages from interrupting command entry.

Note: To avoid repetitive logins during this lab, the **exec-timeout** can be set to 0 0, which prevents it from expiring. However, this is not considered a good security practice.

```
R1(config)#line console 0
R1(config-line)#password ciscoconpass
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
R1(config-line)#logging synchronous
```

b. Configure a password for the aux port for router R1.

```
R1(config)#line aux 0
R1(config-line)#password ciscoauxpass
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
```

c. Configure the password on the vty lines for router R1.

```
R1(config)#line vty 0 4
R1(config-line)#password ciscovtypass
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
```

d. Repeat these configurations on both R2 and R3.

Step 9: Enable HTTP server and HTTP server secure.

Enabling these services allows the router to be managed using the GUI and a web browser.

```
R1(config)#ip http server
```

Step 10: Encrypt clear text passwords.

a. Use the **service password-encryption** command to encrypt the console, aux, and vty passwords.

- `R1(config)#` **service password-encryption**

b. Issue the **show run** command. Can you read the console, aux, and vty passwords? Why or why not?

_____

c. Repeat this configuration on both R2 and R3.

Step 11: Save the basic running configuration for all three routers.

Save the running configuration to the startup configuration from the privileged EXEC prompt.

```
R1#copy running-config startup-config
```

Task 2. Use the Nmap Port Scanner to Determine Router Vulnerabilities

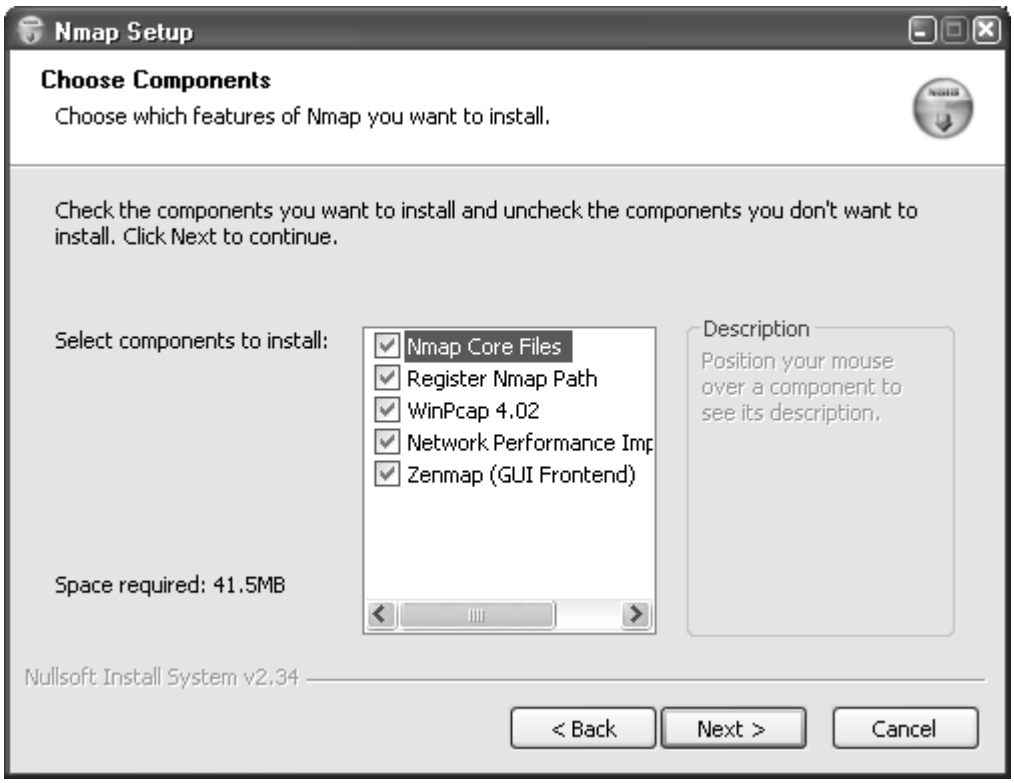
In this task you determine open ports or services running on R1 using Nmap, before configuring a firewall.

Step 1: (Optional) Download and install Nmap and the Zenmap GUI front-end.

Nmap ("Network Mapper") is a free and open source utility for network exploration or security auditing.

If Nmap is already installed on PC-A and PC-C, go to Step 2. Otherwise, download the latest Windows version from http://nmap.org/download.html.

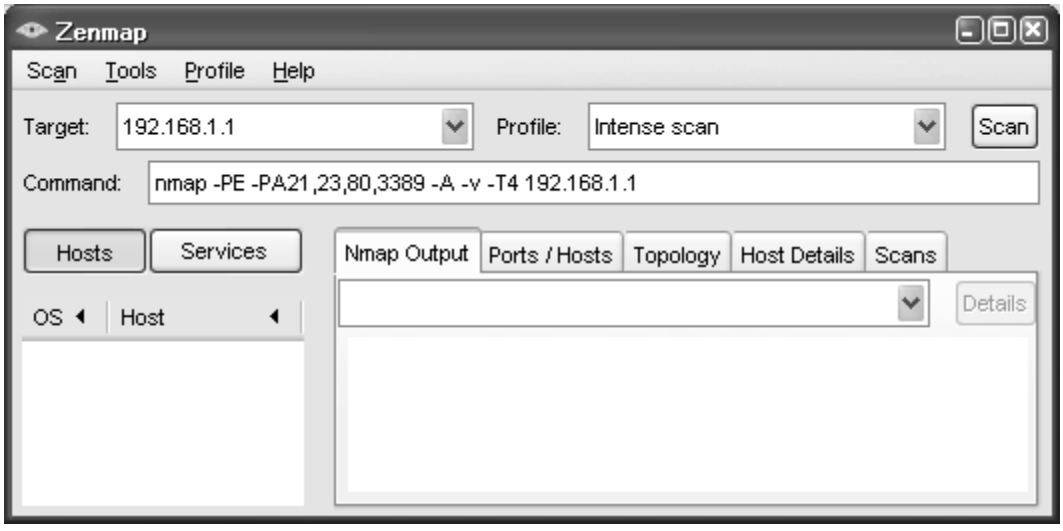
On PC-A and PC-C, run the Nmap setup utility and install all components listed, including the Zenmap GUI front-end. Click **Next** to accept the defaults when prompted.



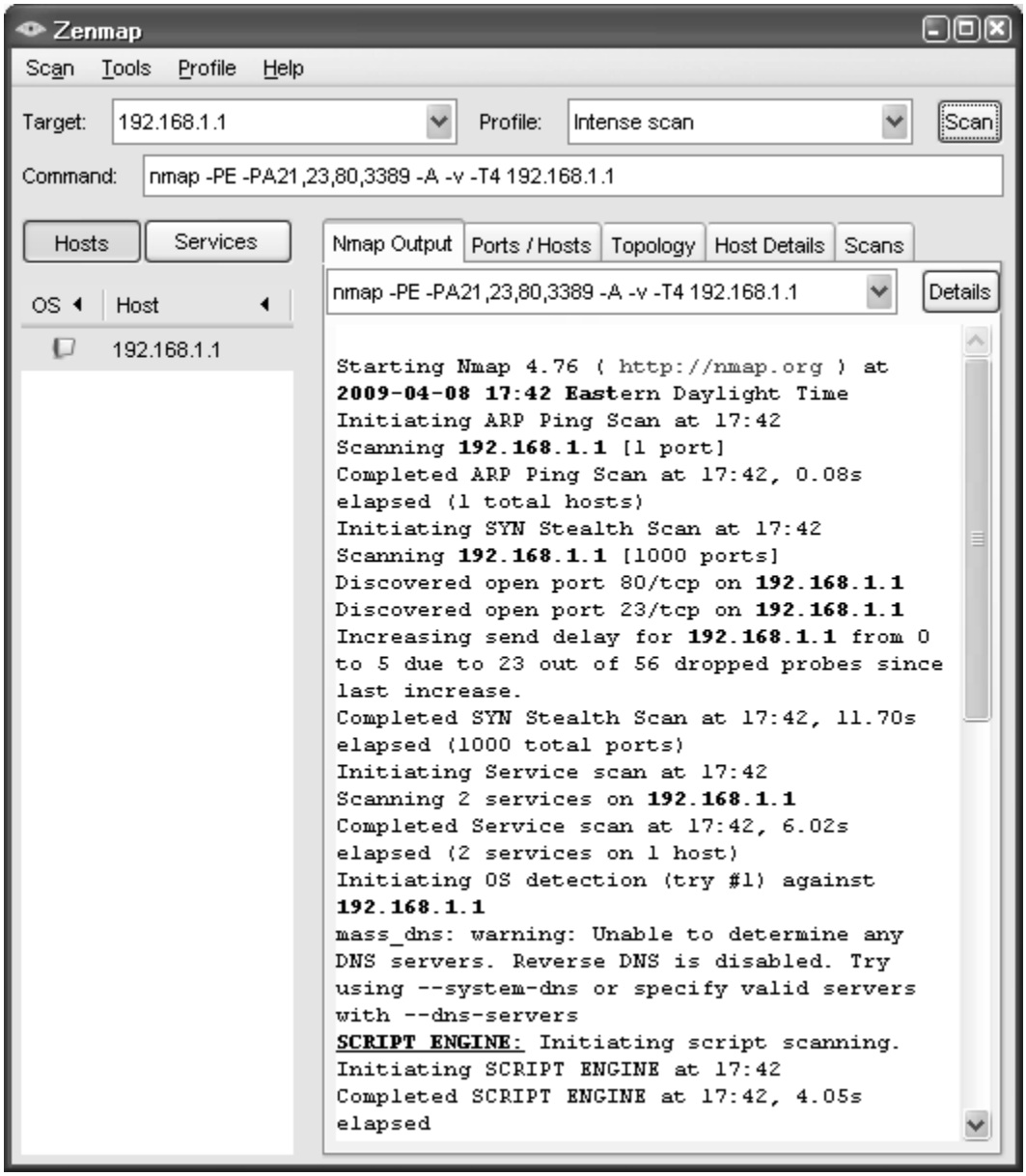
Step 2: Scan for open ports on R1 using Nmap from internal host PC-A.

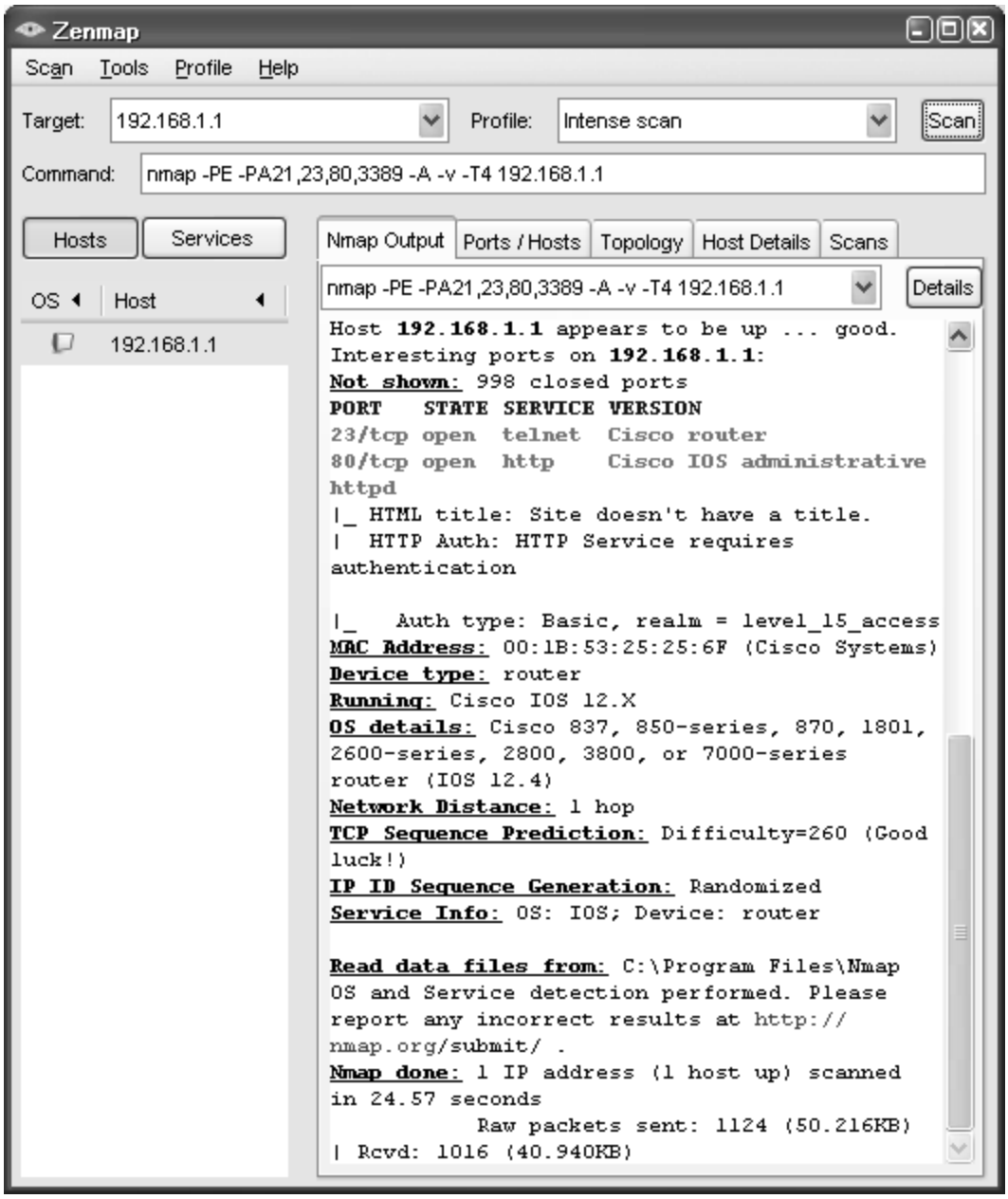
From internal host PC-A, start the Nmap-Zenmap application and enter the IP address of the default gateway, R1 Fa0/1 (192.168.1.1), as the **Target**. Accept the default Nmap command entered for you in the **Command** window and use the **Intense scan** profile.

Note: If the PC is running a personal firewall it may be necessary to turn it off temporarily to obtain accurate test results.



a. Click the **Scan** button to begin the scan of R1 from internal host PC-A. Allow some time for the scan to complete. The next two screens show the entire output of the scan after scrolling.


Zenmap
Scan Tools Profile Help
Target: 192.168.1.1
Profile: Intense scan
Scan
Command: nmap -PE -PA21,23,80,3389 -A -v -T4 192.168.1.1
Hosts
Services
OS
Host
192.168.1.1
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -PE -PA21,23,80,3389 -A -v -T4 192.168.1.1
Details
Starting Nmap 4.76 (http://nmap.org) at
2009-04-08 17:42 Eastern Daylight Time
Initiating ARP Ping Scan at 17:42
Scanning 192.168.1.1 [1 port]
Completed ARP Ping Scan at 17:42, 0.08s
elapsed (1 total hosts)
Initiating SYN Stealth Scan at 17:42
Scanning 192.168.1.1 [1000 ports]
Discovered open port 80/tcp on 192.168.1.1
Discovered open port 23/tcp on 192.168.1.1
Increasing send delay for 192.168.1.1 from 0
to 5 due to 23 out of 56 dropped probes since
last increase.
Completed SYN Stealth Scan at 17:42, 11.70s
elapsed (1000 total ports)
Initiating Service scan at 17:42
Scanning 2 services on 192.168.1.1
Completed Service scan at 17:42, 6.02s
elapsed (2 services on 1 host)
Initiating OS detection (try #1) against
192.168.1.1
mass_dns: warning: Unable to determine any
DNS servers. Reverse DNS is disabled. Try
using --system-dns or specify valid servers
with --dns-servers
SCRIPT ENGINE: Initiating script scanning.
Initiating SCRIPT ENGINE at 17:42
Completed SCRIPT ENGINE at 17:42, 4.05s
elapsed



b. Click the **Service** button in the upper left side of the screen. What ports are open on R1 Fa0/1 from the perspective of internal host PC-A? _____

What is the MAC address of the R1 Fa0/1 interface? _____

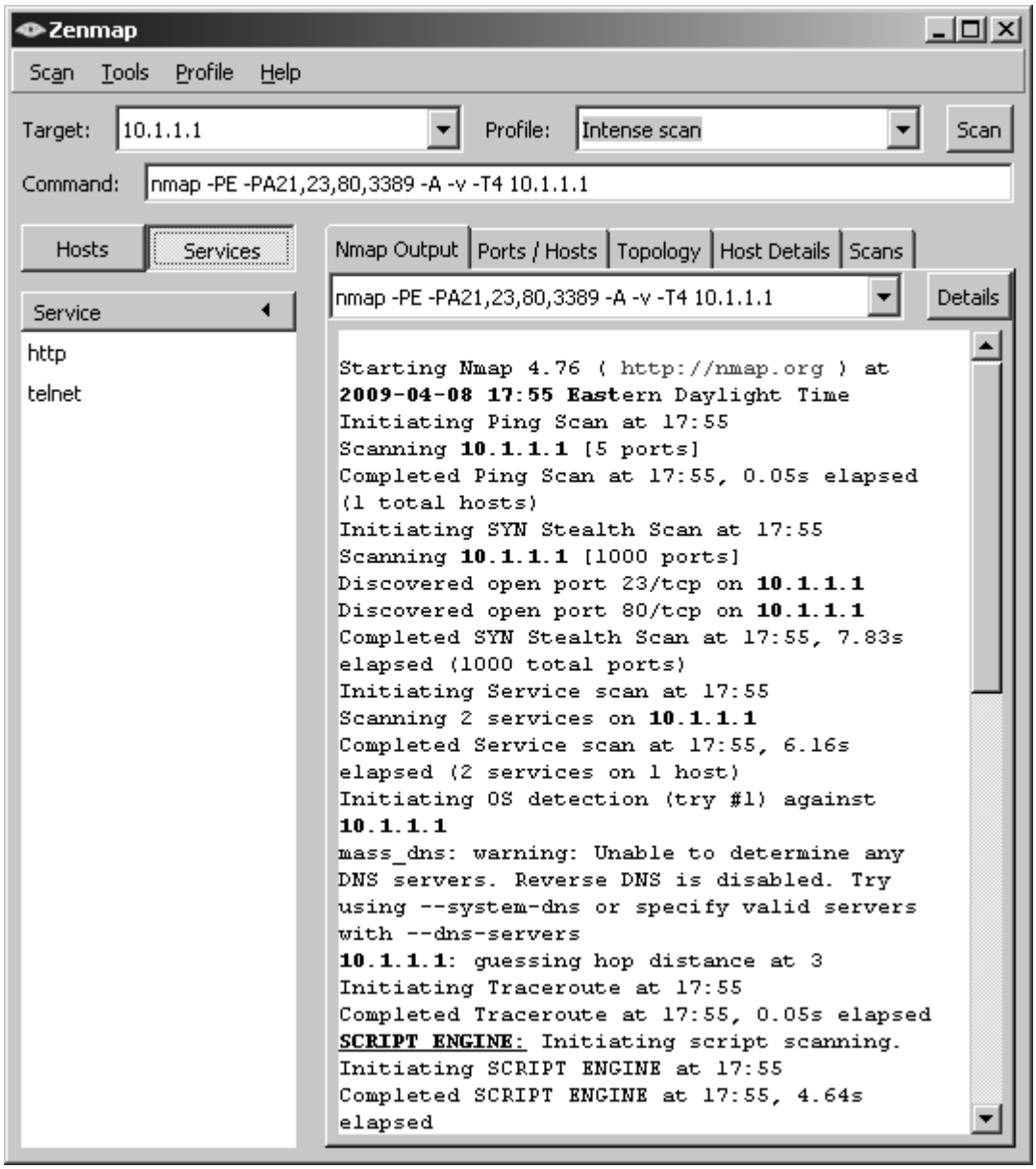
For R1, what type of device and what OS version does Nmap detect?

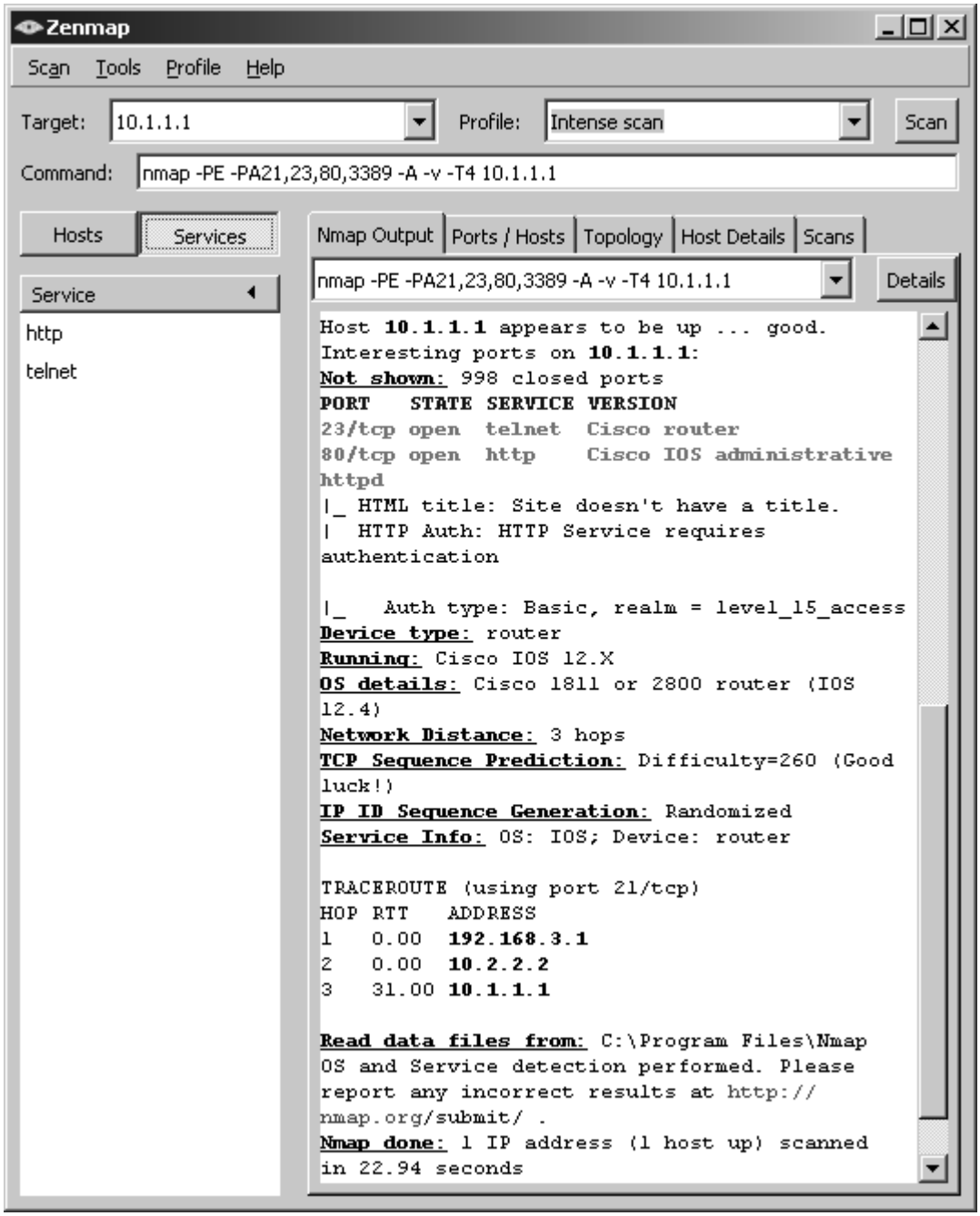
_____

Step 3: Scan for open ports on R1 using Nmap from external host PC-C.

From external host PC-C, start the Nmap-Zenmap application and enter the IP address of R1 S0/0/0 (10.1.1.1) as the Target. Accept the default Nmap command entered for you in the **Command** window and use the **Intense scan** profile.

a. Click the **Scan** button. Allow some time for the scan to complete. The next two screens show the entire output of the scan after scrolling.





a. Click the **Services** button below the **Command** entry field. What services are running and available on R1 from the perspective of PC-C? _____

b. In the Nmap scan output, refer to the TRACEROUTE information. How many hops are between PC-C and R1 and through what IP addresses did the scan have to go to reach R1?

_____

Note: In Part 2 of this lab you will configure a CBAC firewall on R1 and then run Nmap again to test access from external host PC-C to R1.

Part 2. Configuring a Context-Based Access Control (CBAC) Firewall

In Part 2 of this lab, you configure CBAC on R1 using AutoSecure. You then review and test the resulting configuration.

Task 1. Verify Access to the R1 LAN from R2

In this task, you verify that with no firewall in place, the external router R2 can ping the R1 S0/0/0 interface and PC-A on the R1 internal LAN.

Step 1: Ping from R2 to R1.

From R2, ping the R1 interface S0/0/0 at IP address 10.1.1.1.

```
R2#ping 10.1.1.1
```

Were the results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Step 2: Ping from R2 to PC-A on the R1 LAN.

From R2, ping PC-A on the R1 LAN at IP address 192.168.1.3.

```
R2#ping 192.168.1.3
```

Were the results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Step 3: Display the R1 running config prior to using AutoSecure.

a. Issue the **show run** command to review the current basic configuration on R1.

b. Are there any security commands related to access control?

_____

Task 2. Use AutoSecure to Secure R1 and Enable CBAC

AutoSecure simplifies the security configuration of a router and hardens the router configuration. In this task, you run AutoSecure and enable CBAC during the process.

Step 1: Use the AutoSecure IOS feature to enable CBAC.

a. Enter privileged EXEC mode using the **enable** command.

b. Issue the **auto secure** command on R1. Respond as shown in the following AutoSecure output to the AutoSecure questions and prompts. The responses are bolded.

Note: The focus here is the commands generated by AutoSecure for CBAC, so you do not enable all the potential security features that AutoSecure can provide, such as SSH access. Be sure to respond “yes” to the prompt **Configure CBAC Firewall feature?.**

```
R1#auto secure
                --- AutoSecure Configuration ---
```

```
*** AutoSecure configuration enhances the security of the router, but it will
not make it absolutely resistant to all security attacks ***

AutoSecure will modify the configuration of your device. All configuration
changes will be shown. For a detailed explanation of how the configuration
changes enhance security and any possible side effects, please refer to
Cisco.com for
Autosecure documentation.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]:  yes

   Enter the number of interfaces facing the internet [1]: 1

   Interface         IP-Address    OK? Method Status                Protocol
   FastEthernet0/0   unassigned    YES unset  administratively down down

   FastEthernet0/1   192.168.1.1   YES manual up                    up

   Serial0/0/0       10.1.1.1      YES SLARP  up                    up

   Serial0/0/1       unassigned    YES unset  administratively down down


   Enter the interface name that is facing the internet: serial0/0/0


   Securing Management plane services...

   Disabling service finger
   Disabling service pad
   Disabling udp & tcp small servers
   Enabling service password encryption
   Enabling service tcp-keepalives-in
   Enabling service tcp-keepalives-out
   Disabling the cdp protocol

   Disabling the bootp server
   Disabling the http server
   Disabling the finger service
   Disabling source routing
   Disabling gratuitous arp

   Here is a sample Security Banner to be shown
   at every access to device. Modify it to suit your
   enterprise requirements.

   Authorized Access only
     This system is the property of So-&-So-Enterprise.
     UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.
     You must have explicit permission to access this
     device. All activities performed on this device
     are logged. Any violations of access policy will result
     in disciplinary action.

   Enter the security banner {Put the banner between
   k and k, where k is any character}:
```

$ Unauthorized Access Prohibited $

```
Enable secret is either not configured or
 is the same as enable password
Enter the new enable secret: cisco12345
Confirm the enable secret : cisco12345
Enter the new enable password: cisco67890
Confirm the enable password: cisco67890

Configuration of local user database
Enter the username: admin
Enter the password: cisco12345
Confirm the password: cisco12345
Configuring AAA local authentication
Configuring Console, Aux and VTY lines for
local authentication, exec-timeout, and transport
Securing device against Login Attacks
Configure the following parameters

Blocking Period when Login Attack detected: 60

Maximum Login failures with the device: 2

Maximum time period for crossing the failed login attempts: 30

Configure SSH server? [yes]: no

Configuring interface specific AutoSecure services
Disabling the following ip services on all interfaces:

 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
Disabling mop on Ethernet interfaces

Securing Forwarding plane services...

Enabling CEF (This might impact the memory requirements for your platform)
Enabling unicast rpf on all interfaces connected
to internet

Configure CBAC Firewall feature? [yes/no]: yes

This is the configuration generated:

no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
no ip bootp server
```

```
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
no ip identd
banner motd ^C Unauthorized Access Prohibited ^C
security authentication failure rate 10 log
enable secret 5 $1$m.de$Mp5tQr/I8W5VhuQoG6AoA1
enable password 7 05080F1C2243185E415C47
username admin password 7 02050D4808095E731F1A5C
aaa new-model
aaa authentication login local_auth local
line con 0
 login authentication local_auth
 exec-timeout 5 0
 transport output telnet
line aux 0
 login authentication local_auth
 exec-timeout 10 0
 transport output telnet
line vty 0 4
 login authentication local_auth
 transport input telnet
line tty 1
 login authentication local_auth
 exec-timeout 15 0
login block-for 60 attempts 2 within 30
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
interface FastEthernet0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface FastEthernet0/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface Serial0/0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
interface Serial0/0/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
```

```
 no ip directed-broadcast
 no ip mask-reply
interface Vlan1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
access-list 100 permit udp any any eq bootpc
interface Serial0/0/0
 ip verify unicast source reachable-via rx allow-default 100
ip inspect audit-trail
ip inspect dns-timeout 7
ip inspect tcp idle-time 14400
ip inspect udp idle-time 1800
ip inspect name autosec_inspect cuseeme timeout 3600
ip inspect name autosec_inspect ftp timeout 3600
ip inspect name autosec_inspect http timeout 3600
ip inspect name autosec_inspect rcmd timeout 3600
ip inspect name autosec_inspect realaudio timeout 3600
ip inspect name autosec_inspect smtp timeout 3600
ip inspect name autosec_inspect tftp timeout 30
ip inspect name autosec_inspect udp timeout 15
ip inspect name autosec_inspect tcp timeout 3600
ip access-list extended autosec_firewall_acl
 permit udp any any eq bootpc
 deny ip any any
interface Serial0/0/0
 ip inspect autosec_inspect out
 ip access-group autosec_firewall_acl in
!
end

Apply this configuration to running-config? [yes]: yes

Applying the config generated to running-config

R1#
000043: *Dec 29 21:28:59.223 UTC: %AUTOSEC-1-MODIFIED: AutoSecure
configuration has been Modified on this device
```

Step 2: Configure the R1 firewall to allow EIGRP updates.

The AutoSecure CBAC firewall on R1 does not permit EIGRP hellos and neighbor associations to occur and, therefore, no updates can be sent or received. Because EIGRP updates are blocked, R1 does not know of the 10.2.2.0/30 or the 192.168.3.0/24 networks, and R2 does not know of the 192.168.1.0/24 network.

Note: When you configure the ZBF firewall on R3 in Part 3 of this lab, SDM gives the option of allowing EIGRP routing updates to be received by R3.

Display the Extended ACL named **autosec_firewall_acl**, which is applied to S0/0/0 inbound.

```
R1#show access-list autosec_firewall_acl
Extended IP access list autosec_firewall_acl
    10 permit udp any any eq bootpc
    20 deny ip any any (10)
```

Notice the 10 matches on ACL line 20. What is this a result of?

_____

Configure R1 to allow EIGRP updates by adding a statement to the Extended ACL autosec_firewall_acl that permits the EIGRP protocol.

```
R1(config)#ip access-list extended autosec_firewall_acl
R1(config-ext-nacl)#15 permit eigrp any any
R1(config-ext-nacl)#end
```

Display the Extended ACL autosec_firewall_acl again.

```
R1#show access-list autosec_firewall_acl
Extended IP access list autosec_firewall_acl
    10 permit udp any any eq bootpc
    15 permit eigrp any any (5)
    20 deny ip any any (10)
```

Notice that there is now some EIGRP packet activity for ACL statement 15.

Step 3: Save the running configuration.

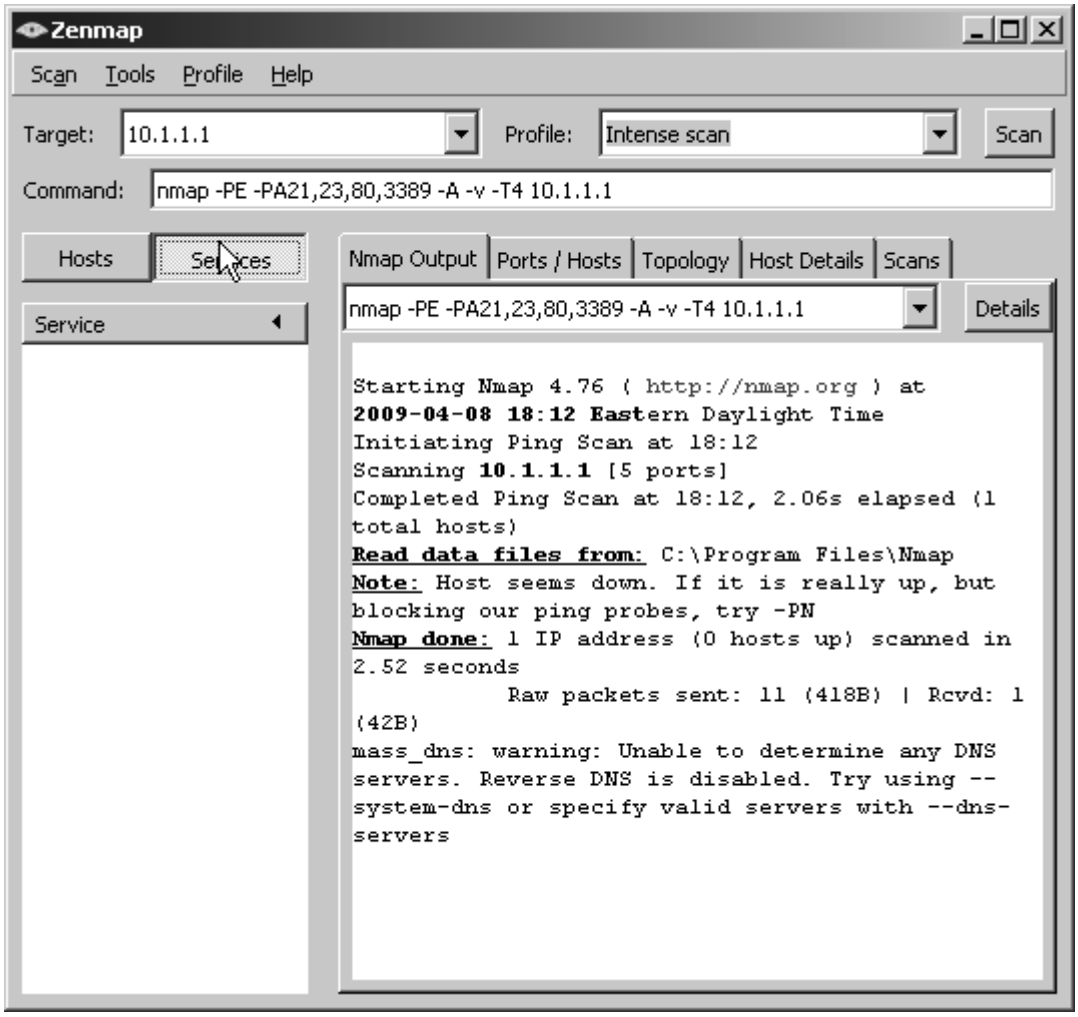
Enter privileged EXEC mode using the **enable** command and provide the enable password cisco12345.

```
R1#copy run start
```

Step 4: Scan for open ports on R1 using Nmap from external host PC-C.

From external host PC-C, use Nmap-Zenmap to scan R1 at Target IP address 10.1.1.1. Accept the default Nmap command entered for you in the **Command** window. Use the **Intense scan** profile.

a. Click the **Scan** button to being scanning R1.



Now that the R1 CBAC firewall is in place, what services are available on R1 and what is the status of R1 from the perspective of external PC-C? _____

Task 3. Review the AutoSecure CBAC Configuration

Step 1: Review the commands that were delivered to router R1.

Display the running configuration for R1. The AutoSecure output should look similar to that shown in Task 2, Step 1.

a. What is the most common command issued that is related to CBAC?

_____

b. CBAC creates rules to track TCP and UDP flows using the **ip inspect name** *name* **protocol** command. To what interface is the autosec_inspect name applied and in what direction?

_____

Step 2: Display the protocols available with the `ip inspect` command.

To see the protocols available, enter the **ip inspect name** *name* command in global config mode, followed by a question mark (?).

Note: Most of the protocols listed are application layer protocols. Newer Cisco IOS versions have more protocols listed.

```
R1(config)# ip inspect name autosec_inspect ?
802-11-iapp       IEEE 802.11 WLANs WG IAPP
ace-svr           ACE Server/Propagation
appfw             Application Firewall
appleqtc          Apple QuickTime
bgp               Border Gateway Protocol
biff              Bliff mail notification
bittorrent        bittorrent
<Output Omitted>
```

a. How many protocols can be configured for inspection?

_____

b. Refer to the running configuration output or the AutoSecure output in Task 2, Step 1. Which protocols did AutoSecure configure to be inspected as they leave the S0/0/0 interface?

_____

c. To which interface is the ACL autosec_firewall_acl applied and in which direction? _____

d. What is the purpose of the ACL autosec_firewall_acl?

_____

Task 4. Verify CBAC Functionality

For the protocols identified to be inspected, the CBAC firewall allows return traffic for connections initiated from the inside, but blocks all other connections from the outside.

Step 1: From PC-A, ping the R1 internal LAN interface.

From PC-A, ping R1 interface Fa0/1 at IP address 192.168.1.1.

C:\>**ping 192.168.1.1**

Were the pings successful? Why or why not? _____

Step 2: From PC-A, ping the R2 external WAN interface.

From PC-A, ping the R2 interface S0/0/0 at IP address 10.1.1.2.

C:\>**ping 10.1.1.2**

Were the pings successful? Why or why not?

_____

Step 3: Add ICMP to the autosec_inspect list.

From global config mode, configure R1 to inspect ICMP and allow ICMP echo replies from outside hosts.

```
R1(config)#ip inspect name autosec_inspect icmp timeout 5
```

Step 4: From PC-A, ping the R2 external WAN interface.

From PC-A, ping the R2 interface S0/0/0 at IP address 10.1.1.2.

```
C:\>ping 10.1.1.2
```

Were the pings successful? Why or why not? _____

Remove ICMP from the inspect list. This restores the CBAC configuration to the one generated by AutoSecure.

```
R1(config)#no ip inspect name autosec_inspect icmp timeout 5
```

Step 5: Test Telnet access from R2 to R1.

From external router R2, telnet to R1 at IP address 10.1.1.1.

```
R2>telnet 10.1.1.1
Trying 10.1.1.1 ...
% Connection timed out; remote host not responding
```

Was the telnetting successful? Why or why not? _____

Step 6: Configure R1 to allow Telnet access from external hosts.

Display the Extended ACL named **autosec_firewall_acl** that is applied to S0/0/0 inbound.

```
R1#show access-list autosec_firewall_acl
Extended IP access list autosec_firewall_acl
    10 permit udp any any eq bootpc
    15 permit eigrp any any (15)
    20 deny ip any any (57 matches)
```

Notice the 57 matches on ACL line 20. What is this a result of? _____

Configure R1 to allow Telnet access by adding a statement to the Extended ACL autosec_firewall_acl that permits TCP port 23 (Telnet).

```
R1(config)#ip access-list extended autosec_firewall_acl
R1(config-ext-nacl)#18 permit tcp any any eq 23
R1(config-ext-nacl)#end
```

From external router R2, telnet again to R1 at IP address 10.1.1.1.

```
R2>telnet 10.1.1.1
Trying 10.1.1.1 ... Open

Unauthorized Access Prohibited

User Access Verification

Username: admin
Password: cisco12345

R1>
```

From the Telnet session on R1, display the modified Extended ACL autosec_firewall_acl.

```
R1>show access-list autosec_firewall_acl
Extended IP access list autosec_firewall_acl
  10 permit udp any any eq bootpc
  15 permit eigrp any any (25)
```

```
18 permit tcp any any eq telnet (12 matches)
20 deny ip any any (57 matches)
```

Notice the new line 18 in the ACL and the 12 matches. What is this a result of?

_____

Remove Telnet external access from the R1 firewall ACL.

```
R1(config)#ip access-list extended autosec_firewall_acl
R1(config-ext-nacl)#no 18 permit tcp any any eq telnet
R1(config-ext-nacl)#end
```

Note: SSH is recommended instead of Telnet, because it provides a more secure way to allow remote administration access to a router or other networking device. SSH provides encrypted communication, however, some additional configuration is required to support the SSH connection. Refer to Chapter 2 Lab A for the procedure to enable SSH. For added security, configure SSH as the only input transport on the vty lines and remove Telnet as an input transport. Allowing SSH access to R1 from external hosts also requires adding a statement to the Extended ACL autosec_firewall_acl that permits TCP port 22 (SSH).

Step 7: Test Telnet access from internal PC-A to external router R2.

From PC-A, telnet to R2 at IP address 10.1.1.2.

```
C:\>telnet 10.1.1.2
```

a. Was the telnet attempt successful? Why or why not? _____

b. Log in to R2 by providing the vty password of ciscovtypass.

c. Leave the Telnet session open.

Task 5. Verify CBAC Configuration and Operation

Step 1: Display CBAC inspection information.

Use the **show ip inspect all** command to see the configuration and inspection status.

Note: The end of the command output shows the established sessions and the inspected TCP Telnet connection between PC-A and R2.

```
R1#show ip inspect all
Session audit trail is enabled
Session alert is enabled
one-minute (sampling period) thresholds are [unlimited : unlimited]
connections
max-incomplete sessions thresholds are [unlimited : unlimited]
max-incomplete tcp connections per host is unlimited. Block-time 0 minute.
Tcp synwait-time is 30 sec – tcp finwait-time is 5 sec
tcp idle-time is 14400 sec – udp idle-time is 1800 sec
tcp reassembly queue length 16; timeout 5 sec; memory-limit 1024 kilo bytes
dns-timeout is 7 sec
Inspection Rule Configuration
 Inspection name autosec_inspect
    cuseeme alert is on audit-trail is on timeout 3600
    ftp alert is on audit-trail is on timeout 3600
    http alert is on audit-trail is on timeout 3600
    rcmd alert is on audit-trail is on timeout 3600
```

```
    rcmd alert is on audit-trail is on timeout 3600
    smtp max-data 20000000 alert is on audit-trail is on timeout 3600
    tftp alert is on audit-trail is on timeout 30
    udp alert is on audit-trail is on timeout 15
    tcp alert is on audit-trail is on timeout 3600

Interface Configuration
 Interface Serial0/0/0
  Inbound inspection rule is not set
  Outgoing inspection rule is autosec_inspect
    cuseeme alert is on audit-trail is on timeout 3600
    ftp alert is on audit-trail is on timeout 3600
    http alert is on audit-trail is on timeout 3600
    rcmd alert is on audit-trail is on timeout 3600
    realaudio alert is on audit-trail is on timeout 3600
    smtp max-data 20000000 alert is on audit-trail is on timeout 3600
    tftp alert is on audit-trail is on timeout 30
    udp alert is on audit-trail is on timeout 15
    tcp alert is on audit-trail is on timeout 3600
  Inbound access list is autosec_firewall_acl
  Outgoing access list is not set

Established Sessions
 Session 6556C128 (192.168.1.3:1185)=>(10.1.1.2:23) tcp SIS_OPEN
```

a. In the Established Sessions section, what is the source IP address and port number for Session 655C128? _____

b. What is the destination IP address and port number for Session 655C128?

_____

Step 2: View detailed session information.

a. View detailed session information using the **show ip inspect sessions detail** command on R1.

```
R1#show ip inspect sessions detail
Established Sessions
 Session 6556C128 (192.168.1.3:1185)=>(10.1.1.2:23) tcp SIS_OPEN
  Created 00:00:09, Last heard 00:00:02
  Bytes sent (initiator:responder) [45:154]
  In  SID 10.1.1.2[23:23]=>192.168.1.3[1185:1185] on ACL autosec_firewall_acl
(19 matches)
```

b. Close the Telnet connection when you are finished verifying CBAC operation.

Part 3. Configuring a Zone-Based Firewall (ZBF) Using SDM

In Part 3 of this lab, you configure a zone-based firewall (ZBF) on R3 using SDM.

Task 1. Verify Access to the R3 LAN from R2

In this task, you verify that with no firewall in place, external router R2 can access the R3 S0/0/1 interface and PC-C on the R3 internal LAN.

Step 1: Ping from R2 to R3.

a. From R2, ping the R3 interface S0/0/1 at IP address 10.2.2.1.

```
R2#ping 10.2.2.1
```

b. Were the results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Step 2: Ping from R2 to PC-C on the R3 LAN.

a. From R2, ping PC-C on the R3 LAN at IP address 192.168.3.3.

```
R2#ping 192.168.3.3
```

b. Were the results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Step 3: Display the R3 running config prior to starting SDM.

a. Issue the **show run** command to review the current basic configuration on R3.

b. Verify the R3 basic configuration as performed in Part 1 of the lab. Are there any security commands related to access control? _____

Task 2. Create a Zone-Based Policy Firewall

In this task, you use Cisco SDM to create a zone-based policy firewall on R3.

Step 1: Configure the enable secret password and HTTP router access prior to starting SDM.

a. From the CLI, configure the enable secret password for use with SDM on R3.

```
R3(config)#enable secret cisco12345
```

b. Enable the HTTP server on R3.

```
R3(config)#ip http server
```

Step 2: Access SDM and set command delivery preferences.

a. Run the SDM application or open a browser on PC-C and start SDM by entering the R3 IP address 192.168.3.1 in the address field.

b. Log in with no username and the enable secret password cisco12345.

c. In the Password Needed – Networking dialog box, enter **cisco12345** in the Password field and click **Yes**.

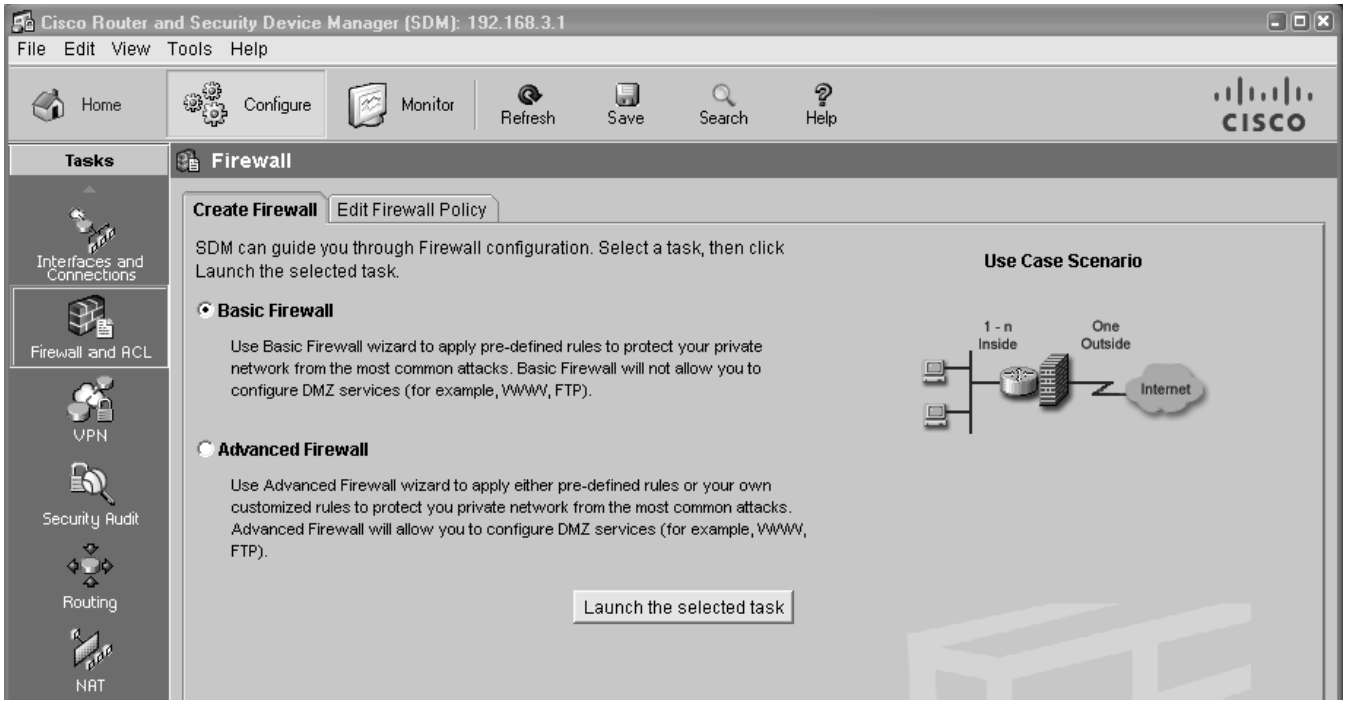
d. Select **Edit** > **Preferences** to configure SDM to allow you to preview the commands before sending them to the router. In the User Preferences window, check the **Preview commands before delivering to router** check box and click **OK**.

Step 3: Use the SDM Firewall wizard to configure a zone-based firewall.

a. On the SDM Home page, refer to the Configuration Overview portion of the screen. What is the state of the Firewall Policies? _____

b. Click the **Configure** button at the top of the SDM screen, and then click **Firewall and ACL.** Read through the overview descriptions for the Basic and Advanced Firewall options. What are some of the key differences? _____

_____

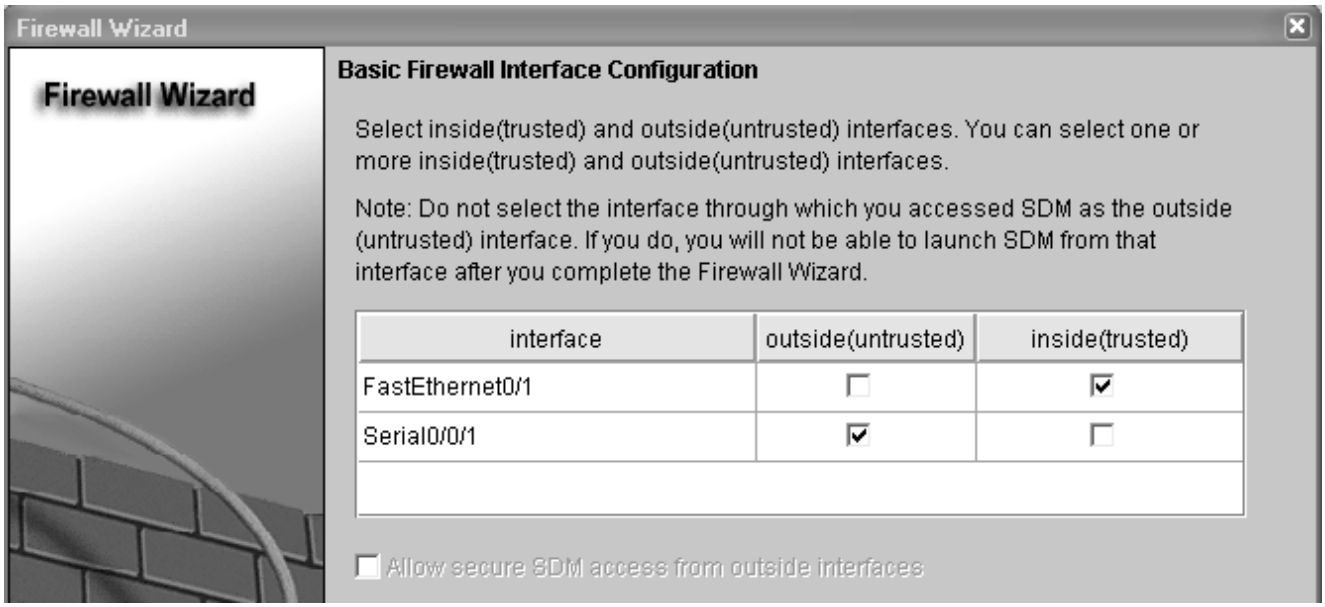


c. Select **Basic Firewall** and click the **Launch the selected task** button.

d. In the Basic Firewall Configuration Wizard window, familiarize yourself with what the Basic Firewall does. What does the Basic Firewall do with traffic from outside zones to inside zones? _____

e. Click **Next** to continue.

f. Check the **Inside (trusted)** check box for **FastEthernet0/1** and the **Outside (untrusted)** check box for **Serial0/0/1.** Click **Next**.



g. Click **OK** when the warning is displayed telling you that you cannot launch SDM from the S0/0/1 interface after the Firewall wizard completes.

h. Move the slider between High, Medium, and Low security to familiarize yourself with what each provides. What is the main difference between High security and Medium or Low security?

_____
_____
_____
_____

i. Move the slider to Low Security and click the **Preview Commands** button to preview the commands that are delivered to the router. When you are finished reviewing the commands, click **Close** and then click **Next**.

j. Review the Firewall Configuration Summary. What does this display provide?

_____

k. Click **Finish** to complete the Firewall wizard.

l. When the Routing traffic configuration window displays, ensure that the check box **Allow EIGRP updates to come through the firewall** is checked and click **OK**.

Note: This screen only displays if a dynamic routing protocol is configured.

m. What would happen if this box was not checked? _____
_____

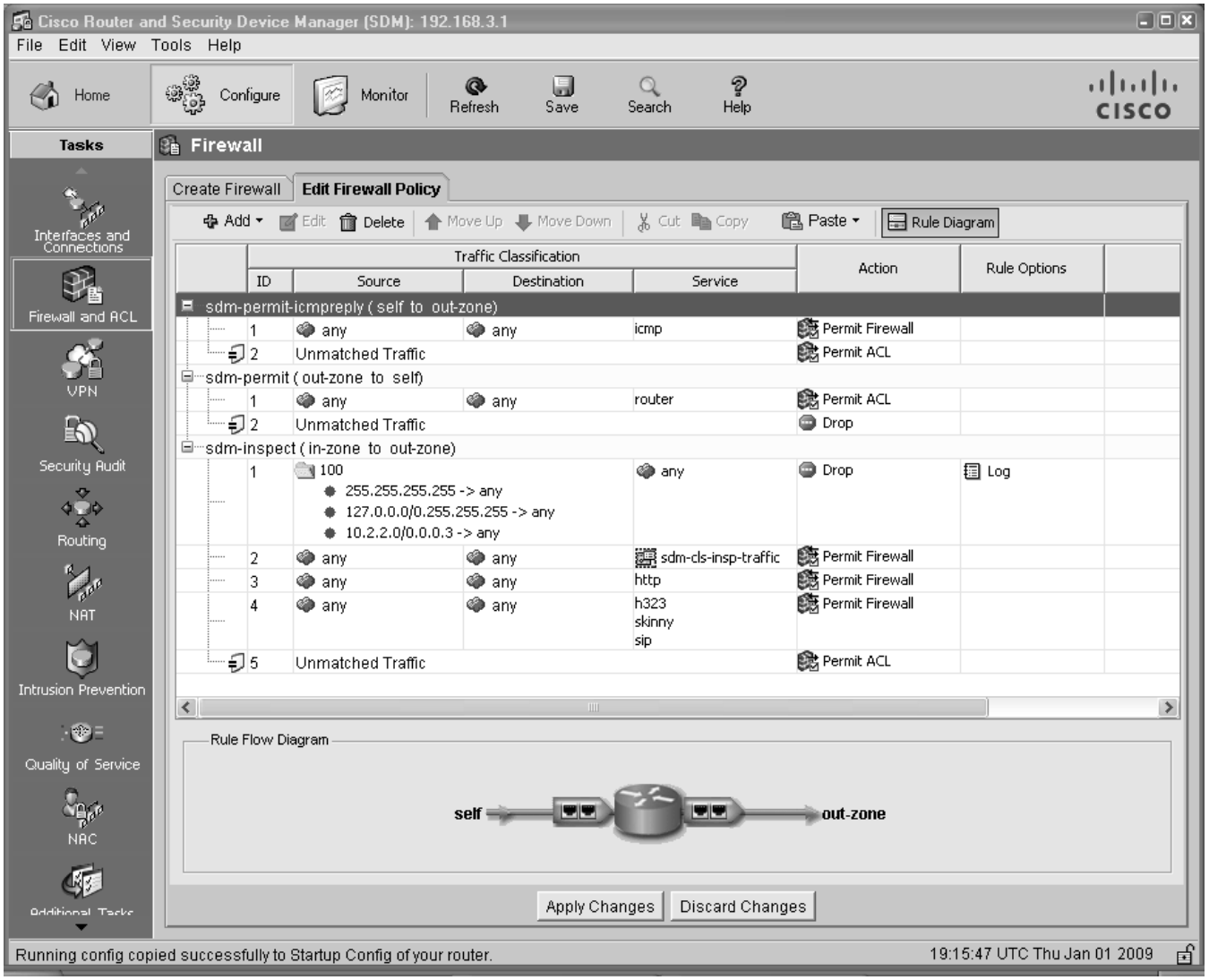
n. In addition to EIGRP, for what other routing protocols does the firewall allow updates?
_____

o. In the Deliver Configuration to Router window, make sure that the **Save running config to router's startup config** check box is checked and click **Deliver**.

p. Click **OK** in the Commands Delivery Status window. How many commands were generated by the Firewall wizard? _____

q. Click **OK** to display the message that you have successfully configured a firewall on the router. Click **OK** to close the message window.

r. The Edit Firewall Policy window displays with the Rule Diagram.



s. In the Rule Diagram, locate access list 100 (folder icon). What action is taken and what rule options are applied for traffic with an invalid source address in the 127.0.0.0/8 address range?

_____

Task 3. Review the Zone-Based Firewall Configuration

Step 1: Examine the R3 running configuration with the CLI.

a. From the R3 CLI, display the running configuration to view the changes that the SDM Basic Firewall wizard made to the router.

b. The following commands are related to ACL 100 and class-map sdm-invalid-source.

```
Class-map type inspect match-all sdm-invalid-src
 match access-group 100

policy-map type inspect sdm-inspect
 class type inspect sdm-invalid-src
  drop log
<output omitted>
```

```
access-list 100 remark SDM_ACL Category=128
access-list 100 permit ip host 255.255.255.255 any
access-list 100 permit ip 127.0.0.0 0.255.255.255 any
access-list 100 permit ip 10.2.2.0 0.0.0.3 any
```

c. In ACL 100, notice that the source addresses listed are permitted. The ACL uses permit statements to identify these addresses as a group so that they can be matched with the **`class-map type inspect match-all sdm-invalid-src`** command and then dropped and logged by the **`class type inspect sdm-invalid-src`** command, which is one of the class types specified for the **sdm-inspect** policy-map.

d. Issue the command **`show run | beg EIGRP`** to display the running configuration beginning with the line that contains the first occurrence of the text "EIGRP". Continue to press **Enter** until you see all the commands in the firewall configuration that are related to EIGRP routing protocol updates on R3. You should see the following commands:

```
class-map type inspect match-any SDM_EIGRP
 match access-group name SDM_EIGRP
class-map type inspect match-any SDM_EIGRP_TRAFFIC
 match class-map SDM_EIGRP
class-map type inspect match-all SDM_EIGRP_PT

policy-map type inspect sdm-permit
 class type inspect SDM_EIGRP_PT
  pass
 class class-default
  drop
```

Step 2: Examine the R3 firewall configuration using SDM.

a. Return to the SDM Home page. Refer to the Configuration Overview portion of the screen. What is the state of Firewall Policies? _____

b. Click the double down arrow on the right of the Firewall Policies section. What is displayed?

_____

c. Click the **Configure** button and select **Additional Tasks > ACL Editor > Firewall Rules**. There should be an ACL that lists fake source addresses, such as the broadcast address of 255.255.255.255 and the 127.0.0.0/8 network. These were identified in the running configuration output in Task 3, Step 1b.

d. Click the **Configure** button and select **Additional Tasks > Zones** to verify the zones configuration. What interfaces are listed and in what zone is each?

_____

e. Click **Configure** and select **Additional Tasks > Zones Pairs** to verify the zone pairs configuration. Fill in the following information.

Zone Pair	Source	Destination	Policy

f. Click **Configure** and select **Additional Tasks > C3PL**.

g. What is C3PL short for? _____

h. Expand the C3PL menu and select **Class Map > Inspection.** How many class maps were created by the SDM Firewall wizard? _____

i. Select **C3PL > Policy Map > Protocol Inspection**. How many policy maps were created by the SDM Firewall wizard? _____

j. Examine the details for the policy map sdm-permit that is applied to the sdm-zp-out-self zone pair. Fill in the information below. List the action for the traffic matching each of the class maps referenced within the sdm-permit policy map.

Match Class Name: _____ **Action: _____**
Match Class Name: _____ **Action: _____**

Task 4. Verify EIGRP Routing Functionality on R3

Step 1: Display the R3 routing table using the CLI.

a. In Task 2, Step 3, the Firewall wizard configured the router to allow EIGRP updates. Verify that EIGRP messages are still being exchanged using the **show ip route** command and verify that there are still EIGRP learned routes in the routing table.

```
R3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
<Output omitted>

Gateway of last resort is not set

     10.0.0.0/30 is subnetted, 2 subnets
C       10.2.2.0 is directly connected, Serial0/0/1
D       10.1.1.0 [90/21024000] via 10.2.2.2, 00:34:12, Serial0/0/1
D    192.168.1.0/24 [90/21026560] via 10.2.2.2, 00:32:16, Serial0/0/1
C    192.168.3.0/24 is directly connected, FastEthernet0/1
```

b. Which networks has R3 learned via the EIGRP routing protocol? _____

Task 5. Verify Zone-Based Firewall Functionality

Step 1: From PC-C, ping the R3 internal LAN interface.

a. From PC-C, ping the R3 interface Fa0/1 at IP address 192.168.3.1.

C:\>**ping 192.168.3.1**

b. Were the pings successful? Why or why not?

_____

Step 2: From PC-C, ping the R2 external WAN interface.

a. From PC-C, ping the R2 interface S0/0/1 at IP address 10.2.2.2.

C:\>**ping 10.2.2.2**

b. Were the pings successful? Why or why not?

_____

Step 3: From R2 ping PC-C.

a. From external router R2, ping PC-C at IP address 192.168.3.3.

```
R2#ping 192.168.3.3
```

b. Were the pings successful? Why or why not?

_____

Step 4: Telnet from R2 to R3.

a. From router R2, telnet to R3 at IP address 10.2.2.1.

```
R2#telnet 10.2.2.1
Trying 10.2.2.1 ... Open

Trying 10.2.2.1 ...
% Connection timed out; remote host not responding
```

b. Why was telnetting unsuccessful? _____

Step 5: Telnet from internal PC-C to external router R2.

From PC-C on the R3 internal LAN, telnet to R2 at IP address 10.2.2.2 and log in.

C:\>**telnet 10.2.2.2**

User Access verification
Password: **ciscovtypass**

With the Telnet session open from PC-C to R2, enter privileged EXEC mode with the **enable** command and password cisco12345.

Issue the command **show policy-map type inspect zone-pair session** on R3. Continue pressing enter until you see an Inspect Established session section toward the end. Your output should look similar to the following.

```
Inspect

   Number of Established Sessions = 1
   Established Sessions
     Session 657344C0 (192.168.3.3:1274)=>(10.2.2.2:23) tacacs:tcp
SIS_OPEN
        Created 00:01:20, Last heard 00:01:13
        Bytes sent (initiator:responder) [45:65]
```

In the Established Sessions in the output, what is the source IP address and port number for Session 657344C0? _____

What is the destination IP address and port number for Session 657344C0?

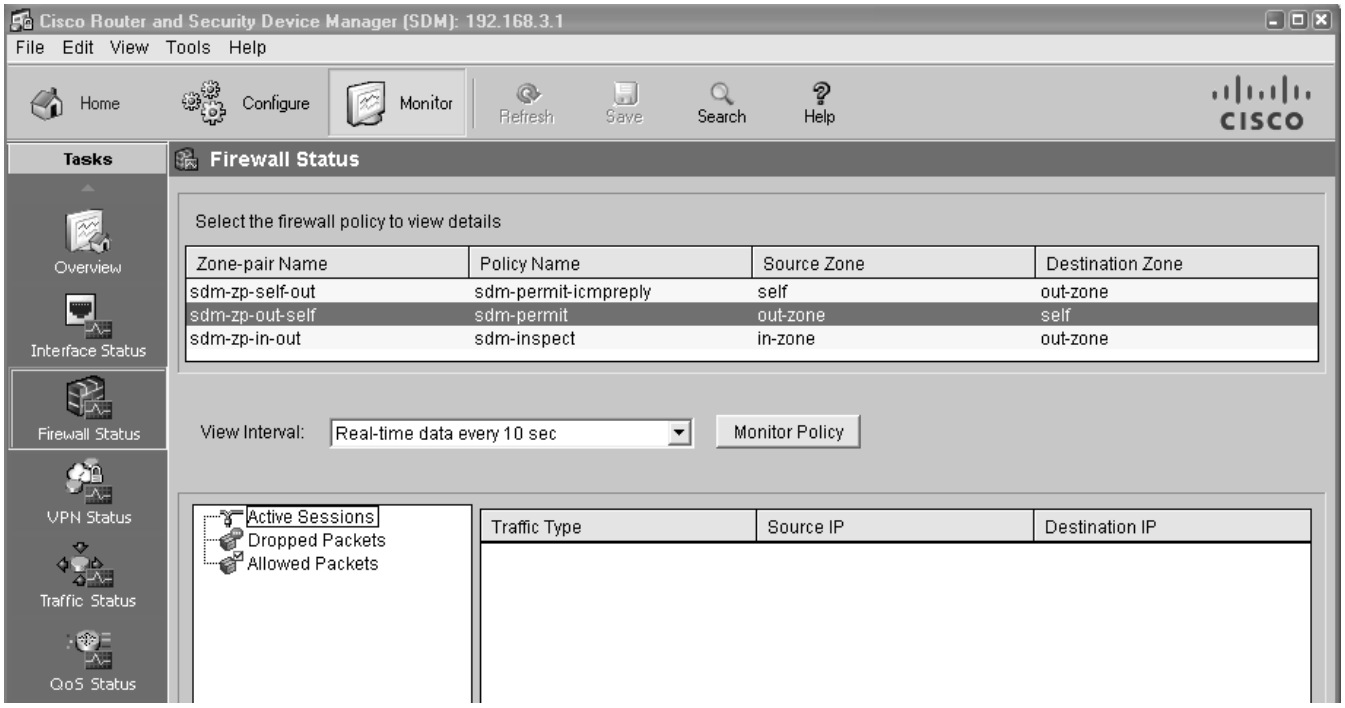
_____

Step 6: Verify the ZBF function using SDM Monitor.

From SDM, click the **Monitor** button at the top of the screen and select **Firewall Status**.

Select the **sdm-zp-out-self** policy from the list of policies. This policy applies to traffic from the outside zone to the router (self) zone.

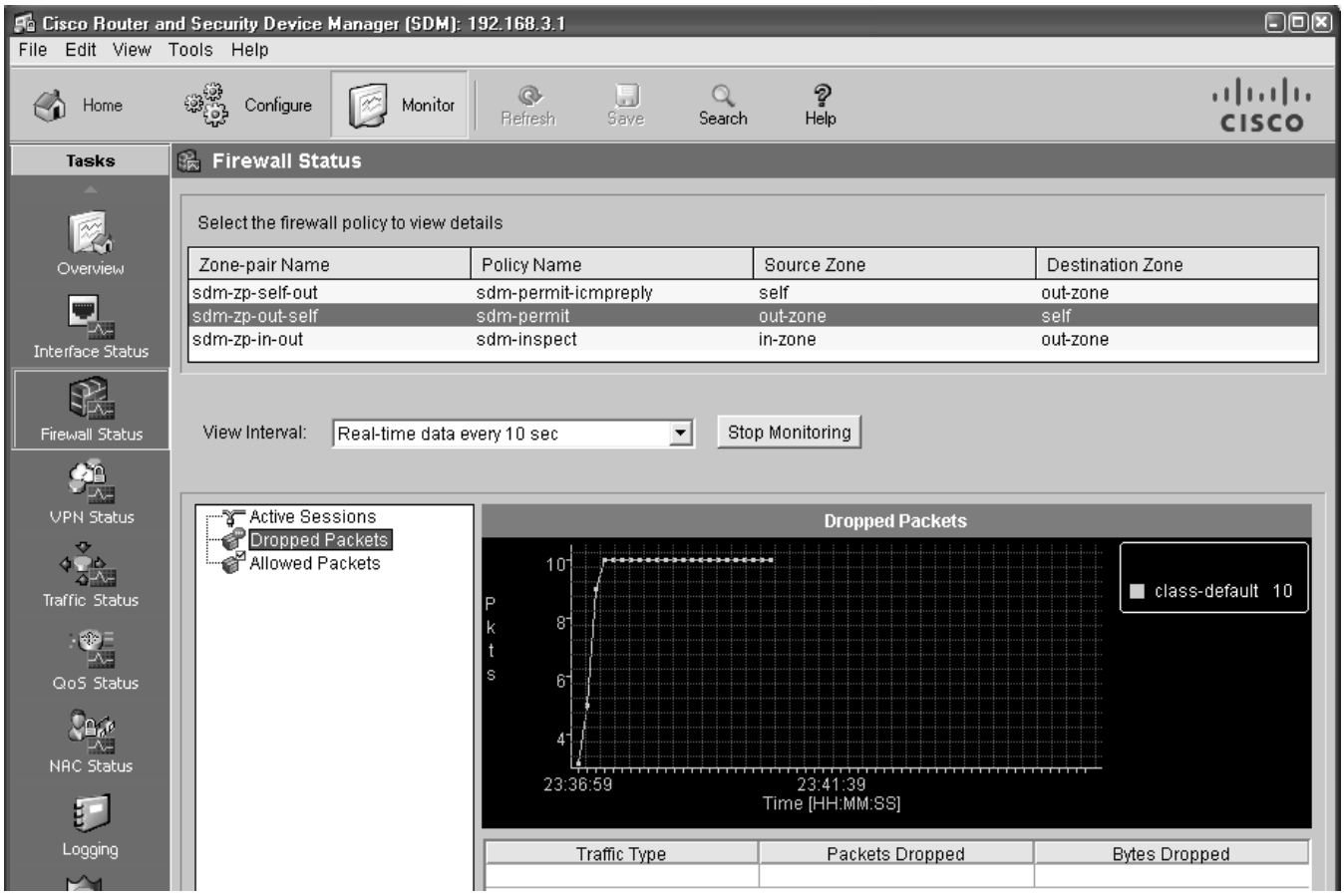
Verify that **Active Sessions** is selected and that the view interval is set to **Real-time data every 10 sec**. Click the **Monitor Policy** button to start monitoring traffic from outside the zone to inside the zone.



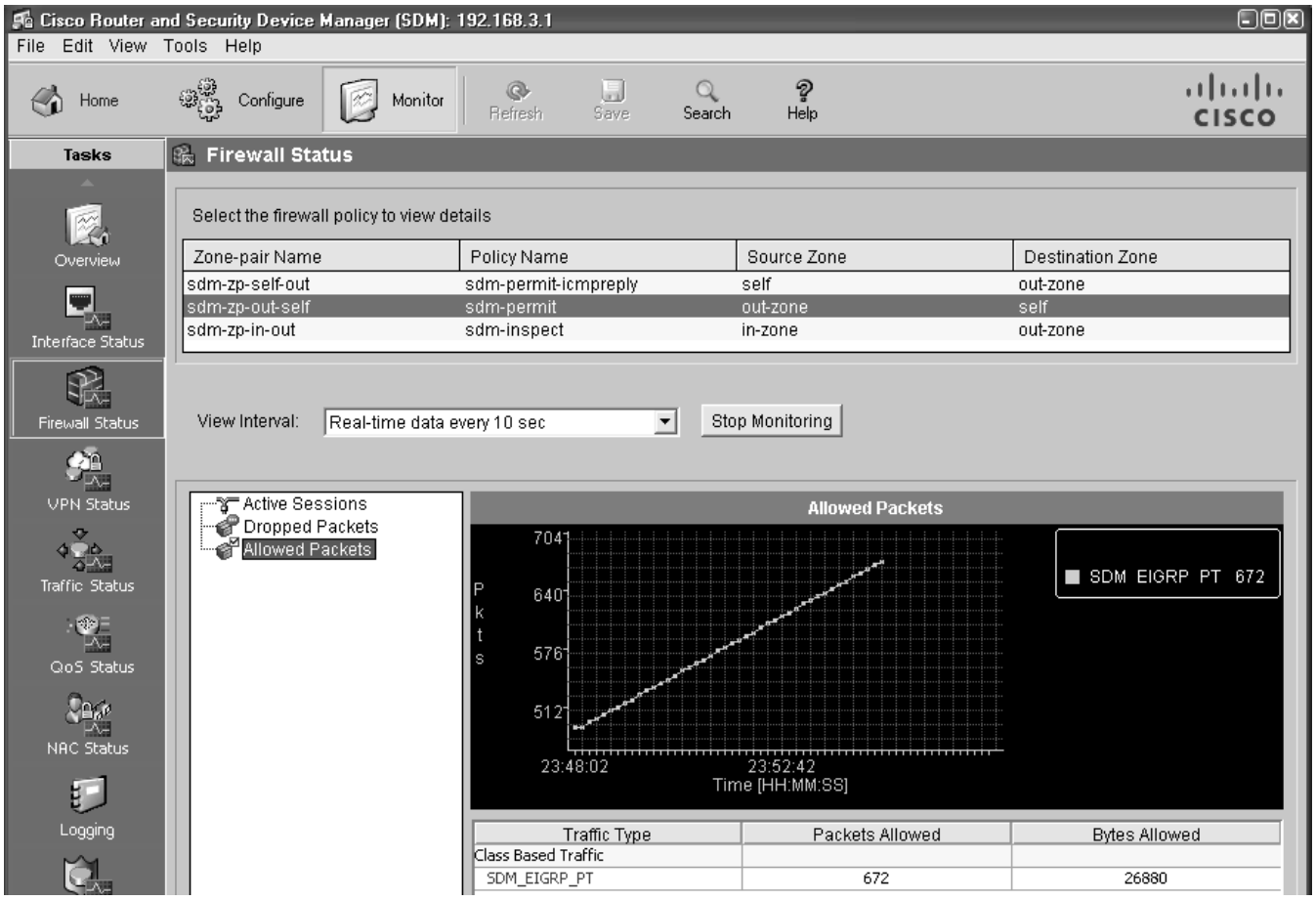
From the R2 CLI, ping the R3 S0/0/1 interface at IP address 10.2.2.1. The pings should fail.

From the R2 CLI, telnet to the R3 S0/0/1 interface at IP address 10.2.2.1. The telnet attempt should fail.

Click the **Dropped Packets** option and observe the graph showing the number of dropped packets resulting from the failed ping and telnet attempts. Your screen should look similar to the one below.



Click the **Allowed Packets** option and observe the graph showing the number of EIGRP packets received from router R3. This number will continue to grow at a steady pace as EIGRP updates are received from R2.



Click the **Stop Monitoring** button and close SDM.

Task 6. Reflection

What are some factors to consider when configuring firewalls using traditional manual CLI methods compared to using the automated AutoSecure CBAC and the SDM Firewall wizard GUI methods?

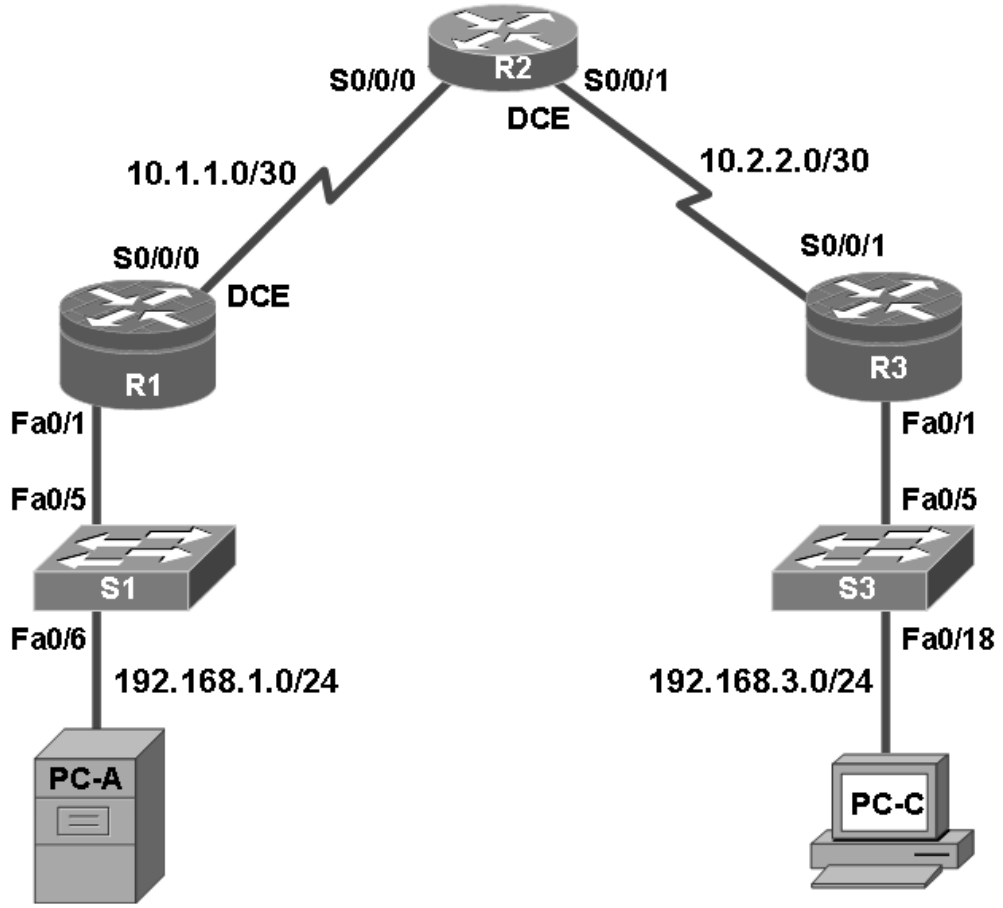
Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1700	Fast Ethernet 0 (FA0)	Fast Ethernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2600	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
2800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Chapter 5: Lab A: Configuring an Intrusion Prevention System (IPS) Using the CLI and SDM

Topology



IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	FA0/1	192.168.1.1	255.255.255.0	N/A	S1 FA0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	FA0/1	192.168.3.1	255.255.255.0	N/A	S3 FA0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 FA0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 FA0/18

Objectives

Part 1: Basic Router Configuration

- Configure hostname, interface IP addresses, and access passwords.
- Configure the static routing.

Part 2: Configuring an IOS Intrusion Prevention System (IPS) using CLI

- Configure IOS IPS using CLI.
- Modify IPS Signatures.
- Examine the resulting IPS configuration.
- Verify IPS functionality.
- Log IPS messages to a Syslog server.

Part 3: Configuring an Intrusion Prevention System (IPS) using SDM

- Configure IPS using SDM.
- Modify IPS Signatures.
- Examine the resulting IPS configuration.
- Use a scanning tool to simulate an attack.
- Use the SDM Monitor to verify IPS functionality.

Background

In this lab, you configure the Cisco IOS Intrusion Prevention System (IPS), which is part of the Cisco IOS Firewall feature set. IPS examines certain attack patterns and alerts or mitigates when those patterns occur. IPS alone is not enough to make a router into a secure Internet firewall, but in addition to other security features, it can be a powerful defense.

You will configure the IPS using the Cisco IOS CLI on one router and SDM on another router, and then test IPS functionality on both routers. You will load the IPS Signature package from a TFTP server and configure the public crypto key using the Cisco IOS CLI and SDM.

Note: The router commands and output in this lab are from a Cisco 1841 using Cisco IOS Release 12.4(20)T (Advanced IP image). Other routers and Cisco IOS versions can be used. See the Router Interface Summary table at the end of the lab to determine which interface identifiers to use based on the equipment in the lab. Depending on the model of the router and Cisco IOS version, the available commands and the output produced might vary from what is shown in this lab.

Note: Make sure that the routers and the switches have been erased and have no startup configurations.

Required Resources

- 2 routers (R1 and R3) with SDM 2.5 installed (Cisco 1841 with Cisco IOS Release 12.4(20)T1 and 192MB DRAM or comparable routers)

Note: The above requirement is critical to successful completion of this lab. The routers that run IPS (R1 and R3) require a minimum of 192MB DRAM and at least 2MB free flash memory. They must also be running T-Train Cisco IOS Release 12.4(11)T1 or later (preferably 12.4(20)T or later) to support the version 5.x format signature package.

- 1 router (R2) Cisco 1841 with Cisco IOS Release 12.4(20)T1 or comparable
- 2 switches (Cisco 2960 or comparable)
- PC-A (Windows XP or Vista with syslog and TFTP servers and the SuperScan tool installed)
- PC-C (Windows XP or Vista with Java 6 Standard Edition, syslog and TFTP servers, and the SuperScan tool installed)

Note: To support SDM IPS on PC-C, you must be able to set the Java heap size to 256MB, which requires Java 6.

- Serial and Ethernet cables as shown in the topology
- Rollover cables to configure the routers via the console
- IPS Signature package and public crypto key files on PC-A and PC-C (provided by instructor)

Part 1. Basic Router Configuration

In Part 1 of this lab, you set up the network topology and configure basic settings such as host names, interface IP addresses, static routing, device access, and passwords.

Note: Perform all tasks on routers R1, R2, and R3. The procedure for R1 is shown here as an example.

Step 1: Cable the network as shown in the topology.

Attach the devices shown in the topology diagram and cable as necessary.

Step 2: Configure the basic settings for each router.

Configure the host names as shown in the topology.

Configure the interface IP addresses as shown in the IP addressing table.

a. Configure a clock rate for serial router interfaces with a DCE serial cable attached.

```
R1(config)#interface S0/0/0
R1(config-if)#clock rate 64000
```

b. To prevent the router from attempting to translate incorrectly entered commands, disable DNS lookup.

```
R1(config)#no ip domain-lookup
```

Step 3: Configure static routing on the routers.

Configure a static default route from R1 to R2 and from R3 to R2.

a. Configure a static route from R2 to the R1 LAN and from R2 to the R3 LAN.

Step 4: Configure PC host IP settings.

Configure a static IP address, subnet mask, and default gateway for PC-A and PC-C, as shown in the IP addressing table.

Step 5: Verify basic network connectivity.

a. Ping from R1 to R3.

Were the results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

b. Ping from PC-A on the R1 LAN to PC-C on the R3 LAN.

Were the results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Note: If you can ping from PC-A to PC-C, you have demonstrated that the static routing protocol is configured and functioning correctly. If you cannot ping but the device interfaces are up and IP addresses are correct, use the **show run** and **show ip route** commands to identify routing protocol-related problems.

Step 6: Configure and encrypt passwords.

Note: Passwords in this task are set to a minimum of 10 characters but are relatively simple for the benefit of performing the lab. More complex passwords are recommended in a production network.

a. Configure a minimum password length using the **security passwords** command to set a minimum password length of 10 characters.

```
R1(config)#security passwords min-length 10
```

b. Configure a console password and enable login for router R1. For additional security, the **exec-timeout** command causes the line to log out after 5 minutes of inactivity. The **logging synchronous** command prevents console messages from interrupting command entry.

Note: To avoid repetitive logins during this lab, the **exec-timeout** command can be set to 0 0, which prevents it from expiring. However, this is not considered to be a good security practice.

```
R1(config)#line console 0
R1(config-line)#password ciscoconpass
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
R1(config-line)#logging synchronous
```

c. Configure a password for the aux port for router R1.

```
R1(config)#line aux 0
R1(config-line)#password ciscoauxpass
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
```

d. Configure the password on the vty lines for router R1.

```
R1(config)#line vty 0 4
R1(config-line)#password ciscovtypass
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
```

e. Encrypt the console, aux, and vty clear text passwords.

```
R1(config)#service password-encryption
```

Issue the **show run** command. Can you read the console, aux, and vty passwords? Why or why not?

_____

Step 7: Save the basic configurations for all three routers.

Save the running configuration to the startup configuration from the privileged EXEC prompt.

```
R1#copy running-config startup-config
```

Part 2. Configuring IPS Using the Cisco IOS CLI

In Part 2 of this lab, you configure IPS on R1 using the Cisco IOS CLI. You then review and test the resulting configuration.

Task 1. Verify Access to the R1 LAN from R2

In this task, you verify that without IPS configured, the external router R2 can ping the R1 S0/0/0 interface and PC-A on the R1 internal LAN.

Step 1: Ping from R2 to R1.

From R2, ping R1 interface S0/0/0 at IP address 10.1.1.1.

```
R2#ping 10.1.1.1
```

Were the results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Step 2: Ping from R2 to PC-A on the R1 LAN.

From R2, ping PC-A on the R1 LAN at IP address 192.168.1.3.

```
R2#ping 192.168.1.3
```

Were the results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Step 3: Display the R1 running config prior to configuring IPS.

a. Issue the **show run** command to review the current basic configuration on R1.

b. Are there any security commands related to IPS?

_____

Task 2. Prepare the Router and TFTP Server

Step 1: Verify the availability of Cisco IOS IPS files.

To configure Cisco IOS IPS 5.x, the IOS IPS Signature package file and public crypto key file must be available on PC-A. Check with your instructor if these files are not on the PC. These files can be downloaded from Cisco.com with a valid user account that has proper authorization.

a. Verify that the IOS-S*xxx*-CLI.pkg file is in a TFTP folder. This is the signature package. The *xxx* is the version number and varies depending on which file was downloaded.

b. Verify that the realm-cisco.pub.key.txt file is available and note its location on PC-A. This is the public crypto key used by IOS IPS.

Step 2: Verify or create the IPS directory in router flash on R1.

In this step, you verify the existence of or create a directory in the router flash memory where the required signature files and configurations will be stored.

Note: Alternatively, you can use a USB flash drive connected to the router's USB port to store the signature files and configurations. The USB flash drive needs to remain connected to the router's USB port if it is used as the IOS IPS configuration directory location. IOS IPS also supports any Cisco IOS file system as its configuration location with proper write access.

a. From the R1 CLI, display the content of flash memory using the **show flash** command and check for the ipsdir directory.

```
R1#show flash
```

b. If the ipsdir directory is not listed, create it in privileged EXEC mode.

```
R1#mkdir ipsdir
Create directory filename [ipsdir]? Press Enter
Created dir flash:ipsdir
```

Note: If the directory already exists, the following message displays.

```
%Error Creating dir flash:ipsdir (Can't create a file that exists)
```

c. From the R1 CLI, verify that the directory is present using the **dir flash:** or **dir flash:ipsdir** command.

```
R1#dir flash:
Directory of flash:/

    5  -rw-    37081324  Dec 17 2008 21:57:10 +00:00  c1841-
advipservicesk9-mz.124-20.T1.bin
    6  drw-           0   Jan 6 2009 11:19:14 +00:00  ipsdir
```

or

```
R1#dir flash:ipsdir

Directory of flash:/ipsdir/

No files in directory
```

Note: The directory exists, but there are currently no files in it.

Task 3. Configuring the IPS Crypto Key

The crypto key verifies the digital signature for the master signature file (sigdef-default.xml). The contents are signed by a Cisco private key to guarantee the authenticity and integrity at every release.

Note: The following instructions use Notepad as the text editor and HyperTerminal as the terminal emulation program. Another text editor and terminal emulation program can be used.

Step 1: Locate and open the crypto key file.

On PC-A, locate the crypto key file named realm-cisco.pub.key.txt and open it using Notepad or another text editor. The contents should look similar to the following:

```
crypto key pubkey-chain rsa
 named-key realm-cisco.pub signature
  key-string
   30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
   00C19E93 A8AF124A D6CC7A24 5097ª975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
   17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
   B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
   5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
   FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
   50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7ª0AF99E AD768C36
   006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
   2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782ª5 CF31CB6E B4B094D3
   F3020301 0001
  quit
```

Step 2: Copy the contents of the text file.

From the Notepad menu bar, select **Edit > Select All**.

a. Select **Edit > Copy** (or press Ctrl+C).

Step 3: Apply the contents of the text file to the router.

At the R1 privileged EXEC prompt, enter global config mode using the **config t** command.

With the cursor at the R1(config)# prompt, paste the text file contents from HyperTerminal by right-clicking and selecting **Paste to Host** from the context menu. Alternatively, you can select **Edit > Paste to Host** from the HyperTerminal menu bar.

Exit global config mode and issue the **show run** command to confirm that the crypto key is configured.

Task 4. Configure IPS

Step 1: Create an IPS rule.

a. On R1, create an IPS rule name using the **ip ips name** *name* command in global configuration mode. Name the IPS rule iosips. This will be used later on an interface to enable IPS.

```
R1(config)#ip ips name iosips
```

b. You can specify an optional extended or standard access control list (ACL) to filter the traffic that will be scanned by this rule name. All traffic that is permitted by the ACL is subject to inspection by the IPS. Traffic that is denied by the ACL is not inspected by the IPS.

c. To see the options available for specifying an ACL with the rule name, use the **ip ips name** command and the CLI help function (**?**).

```
R1(config)#ip ips name ips list ?
  <1-199>  Numbered access list
  WORD     Named access list
```

Step 2: Configure the IPS Signature storage location in router flash memory.

The IPS files will be stored in the ipsdir directory that was created in Task 2, Step 2. Configure the location using the **ip ips config location** command.

```
R1(config)#ip ips config location flash:ipsdir
```

Step 3: Enable IPS SDEE event notification.

The Cisco Security Device Event Exchange (SDEE) server is a Simple Object Access Protocol (SOAP) based, intrusion detection system (IDS) alert format and transport protocol specification. SDEE replaces Cisco RDEP.

To use SDEE, the HTTP server must be enabled with the **ip http server** command. If the HTTP server is not enabled, the router cannot respond to the SDEE clients because it cannot see the requests. SDEE notification is disabled by default and must be explicitly enabled.

Note: SDM Monitor uses HTTP and SDEE to capture IPS events.

To enable SDEE, use the following command.

```
R1(config)#ip ips notify sdee
```

Step 4: Enable IPS syslog support.

IOS IPS also supports the use of syslog to send event notification. SDEE and syslog can be used independently or enabled at the same time to send IOS IPS event notification. Syslog notification is enabled by default.

a. If logging console is enabled, you see IPS syslog messages. Enable syslog if it is not enabled.

```
R1(config)#ip ips notify log
```

Use the **show clock** command to verify the current time and date for the router. Use the **clock set** command from privileged EXEC mode to reset the clock if necessary. The following is an example of how to set the clock.

```
R1#clock set 01:20:00 6 january 2009
```

b. Verify that the timestamp service for logging is enabled on the router using the **show run** command. Enable the timestamp service if it is not enabled.

```
R1(config)#service timestamps log datetime msec
```

c. To send log messages to the syslog server on PC-A, use the following command:

```
R1(config)#logging 192.168.1.3
```

To see the type and level of logging enabled on R1, use the **show logging** command.

```
R1#show logging
```

Note: Verify that you have connectivity between R1 and PC-A by pinging from PC-A to the R1 Fa0/1 interface IP address 192.168.1.1. If it is not successful, troubleshoot as necessary before continuing.

The next step describes how to download one of the freeware syslog servers if one is not available on PC-A.

Step 5: (Optional) Download and start the syslog server.

If a syslog server is not currently available on PC-A, you can download the latest version of Kiwi from http://www.kiwisyslog.com or Tftpd32 from http://tftpd32.jounin.net/. If the syslog server is available on the PC, go to Step 6.

Note: This lab uses the Tftpd32 syslog server.

Start the syslog server software on PC-A if you want to send log messages to it.

Step 6: Configure IOS IPS to use one of the pre-defined signature categories.

IOS IPS with Cisco 5.x format signatures operates with signature categories, just like Cisco IPS appliances do. All signatures are pre-grouped into categories, and the categories are hierarchical. This helps classify signatures for easy grouping and tuning.

Warning: The "all" signature category contains *all* signatures in a signature release. Because IOS IPS cannot compile and use all the signatures contained in a signature release at one time, do not unretire the "all" category. Otherwise, the router will run out of memory.

Note: When configuring IOS IPS, it is required to first retire all the signatures in the "all" category and then unretire selected signature categories.

In the following example, all signatures in the "all" category are retired, and then the "ios_ips basic" category is unretired.

```
R1(config)#ip ips signature-category
R1(config-ips-category)#category all
R1(config-ips-category-action)#retired true
R1(config-ips-category-action)#exit
R1(config-ips-category)#category ios_ips basic
R1(config-ips-category-action)#retired false
R1(config-ips-category-action)#exit
R1(config-ips-category)#exit
Do you want to accept these changes? [confirm] <Enter>

Jan  6 01:32:37.983: Applying Category configuration to signatures ...
```

Step 7: Apply the IPS rule to an interface.

Apply the IPS rule to an interface with the **ip ips** *name direction* command in interface configuration mode. Apply the rule you just created inbound on the S0/0/0 interface. After you enable IPS, some log messages will be sent to the console line indicating that the IPS engines are being initialized.

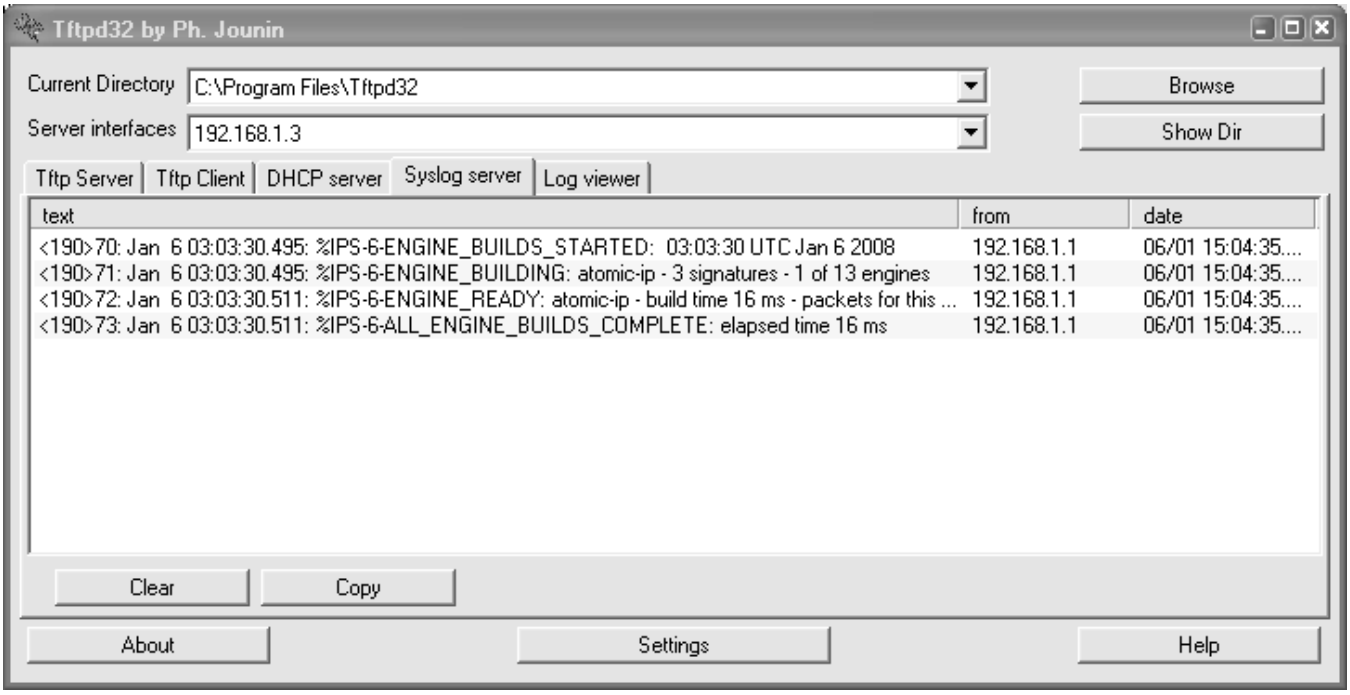
Note: The direction **in** means that IPS inspects only traffic going into the interface. Similarly, **out** means only traffic going out the interface. To enable IPS to inspect both in and out traffic, enter the IPS rule name for in and out separately on the same interface.

```
R1(config)#interface serial0/0/0
R1(config-if)#ip ips iosips in

Jan  6 03:03:30.495: %IPS-6-ENGINE_BUILDS_STARTED:  03:03:30 UTC Jan 6
2008
Jan  6 03:03:30.495: %IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1
of 13 engines
```

```
Jan  6 03:03:30.511: %IPS-6-ENGINE_READY: atomic-ip - build time 16 ms -
packets for this engine will be scanned
Jan  6 03:03:30.511: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 16 ms
```

The message also displays on the syslog server if it is enabled. The Tftpd32 syslog server is shown here.



Although the R1 Fa0/1 interface is an internal interface, it might be desirable to configure it with IPS to respond to internal attacks. Apply the IPS rule to the R1 Fa0/1 interface in the inbound direction.

```
R1(config)#interface fa0/1
R1(config-if)#ip ips iosips in
```

Step 8: Save the running configuration.

Enter privileged EXEC mode using the **enable** command and provide the enable password cisco12345.

```
R1#copy run start
```

Task 5. Load the IOS IPS Signature Package to the Router

The most common way to load the signature package to the router is to use TFTP. Refer to Step 4 for alternative methods for loading the IOS IPS Signature package. The alternative methods include the use of FTP and a USB flash drive.

Step 1: (Optional) Download the TFTP server.

The Tftpd32 freeware TFTP server is used in this task. Many other free TFTP servers are also available. If a TFTP server is not currently available on PC-A, you can download the latest version of Tftpd32 from http://tftpd32.jounin.net/. If it is already installed, go to Step 2.

Note: This lab uses the Tftpd32 TFTP server. This software also includes a syslog server, which runs simultaneously with the TFTP server.

Step 2: Start the TFTP server on PC-A and verify the IPS file directory.

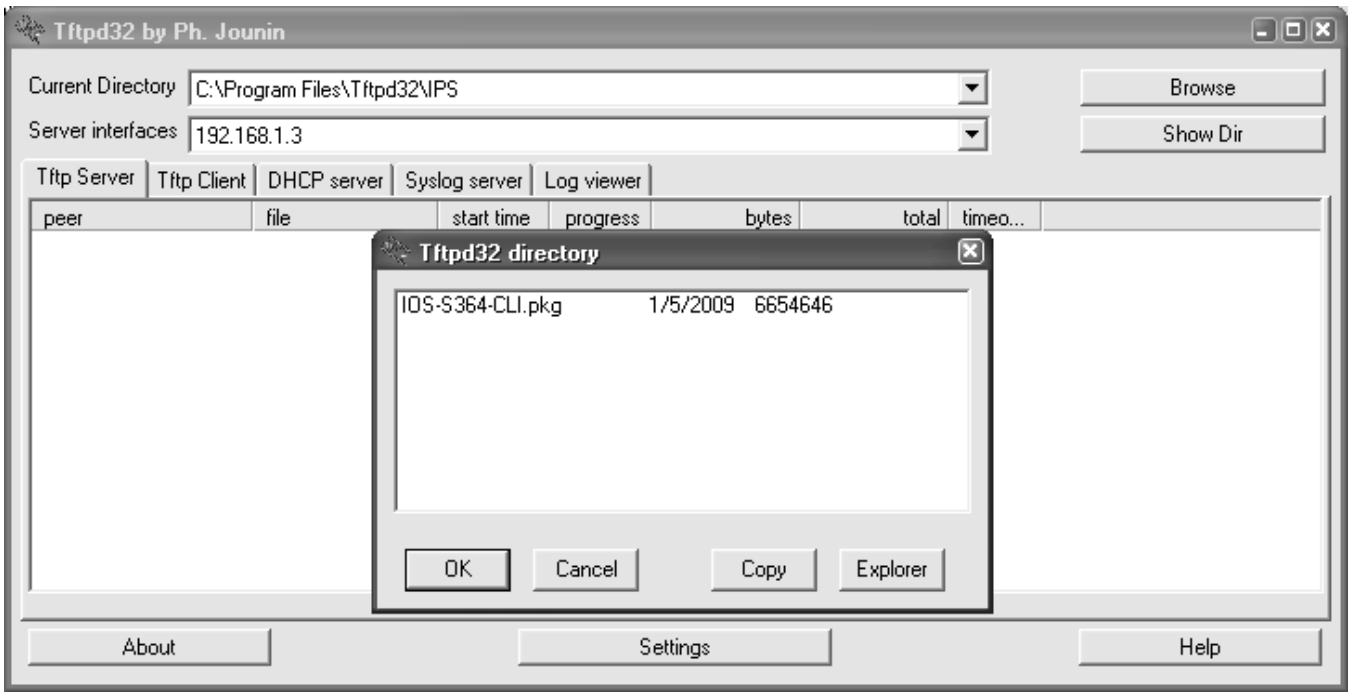
a. Verify connectivity between R1 and PC-A, the TFTP server, using the **ping** command.

b. Verify that the PC has the IPS Signature package file in a directory on the TFTP server. This file is typically named IOS-S*xxx*-CLI.pkg, where *xxx* is the signature file version.

Note: If this file is not present, contact your instructor before continuing.

c. Start Tftpd32 or another TFTP server and set the default directory to the one with the IPS Signature package in it. The Tftpd32 screen is shown here with the C:\Program Files\Tftpd32\IPS directory contents displayed. Take note of the filename for use in the next step.

d. What is the name of the signature file? _____



Step 3: Copy the signature package from the TFTP server to the router.

If you do not have a TFTP server available and are using a router with a USB port, you can go to Step 5 and use the procedure described there.

a. Use the **copy tftp** command to retrieve the signature file. Be sure to use the **idconf** keyword at the end of the **copy** command.

Note: Immediately after the signature package is loaded to the router, signature compiling begins. You can see the messages on the router with logging level 6 or above enabled.

```
R1#copy tftp://192.168.1.3/IOS-S364-CLI.pkg idconf

Loading IOS-S364-CLI.pkg from 192.168.1.3 (via FastEthernet0/1):
!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 6654646 bytes]
```

```
Jan  6 03:18:36.799: %IPS-6-ENGINE_BUILDS_STARTED:  03:18:36 UTC Jan 6
2008
Jan  6 03:18:36.799: %IPS-6-ENGINE_BUILDING: multi-string - 8
signatures - 1 of 13 engines
Jan  6 03:18:36.811: %IPS-6-ENGINE_READY: multi-string - build time 12
ms - packets for this engine will be scanned
Jan  6 03:18:36.831: %IPS-6-ENGINE_BUILDING: service-http - 629
signatures - 2 of 13 engines
Jan  6 03:18:46.755: %IPS-6-ENGINE_READY: service-http - build time
9924 ms - packets for this engine will be scanned
<Output omitted>
```

b. Use the **`dir flash`** command to see the contents of the ipsdir directory created earlier. There should be six files as shown here.

```
R1#dir flash:ipsdir
Directory of flash:/ipsdir/

16  -rw-   230621  Jan 6 2008 03:19:42 +00:00  R1-sigdef-default.xml
15  -rw-      255  Jan 6 2008 01:35:26 +00:00  R1-sigdef-delta.xml
14  -rw-     6632  Jan 6 2008 03:17:48 +00:00  R1-sigdef-typedef.xml
13  -rw-    28282  Jan 6 2008 03:17:52 +00:00  R1-sigdef-category.xml
10  -rw-      304  Jan 6 2008 01:35:28 +00:00  R1-seap-delta.xml
18  -rw-      491  Jan 6 2008 01:35:28 +00:00  R1-seap-typedef.xml
```

Step 4: Verify that the signature package is properly compiled.

a. Use the **`show ip ips signature count`** command to see the counts for the signature package compiled.

```
R1#show ip ips signature count

Cisco SDF release version S364.0
Trend SDF release version V0.0

Signature Micro-Engine: multi-string: Total Signatures 11
      multi-string enabled signatures: 9
      multi-string retired signatures: 11

Signature Micro-Engine: service-http: Total Signatures 662
      service-http enabled signatures: 163
      service-http retired signatures: 565
      service-http compiled signatures: 97
      service-http obsoleted signatures: 1

Signature Micro-Engine: string-tcp: Total Signatures 1148
      string-tcp enabled signatures: 622
      string-tcp retired signatures: 1031
      string-tcp compiled signatures: 117
      string-tcp obsoleted signatures: 21

<Output Omitted>

Total Signatures: 2435
   Total Enabled Signatures: 1063
   Total Retired Signatures: 2097
   Total Compiled Signatures: 338
   Total Obsoleted Signatures: 25
```

Note: If you see an error message during signature compilation, such as "%IPS-3-INVALID_DIGITAL_SIGNATURE: Invalid Digital Signature found (key not found)," it means the public crypto key is invalid. Refer to Task 3, Configuring the IOS IPS Crypto Key, to reconfigure the public crypto key.

b. Use the **show ip ips all** command to see an IPS configuration status summary. To which interfaces and in which direction is the iosips rule applied? _____

```
R1#show ip ips all

IPS Signature File Configuration Status
    Configured Config Locations: flash:ipsdir/
    Last signature default load time: 18:47:52 UTC Jan 6 2009
    Last signature delta load time: 20:11:35 UTC Jan 6 2009
    Last event action (SEAP) load time: -none-

    General SEAP Config:
    Global Deny Timeout: 3600 seconds
    Global Overrides Status: Enabled
    Global Filters Status: Enabled

IPS Auto Update is not currently configured

IPS Syslog and SDEE Notification Status
    Event notification through syslog is enabled
    Event notification through SDEE is enabled

IPS Signature Status
    Total Active Signatures: 339
    Total Inactive Signatures: 2096

IPS Packet Scanning and Interface Status
    IPS Rule Configuration
      IPS name iosips
    IPS fail closed is disabled
    IPS deny-action ips-interface is false
    Interface Configuration
      Interface Serial0/0/0
        Inbound IPS rule is iosips
        Outgoing IPS rule is not set
      Interface FastEthernet0/1
              Inbound IPS rule is iosips
              Outgoing IPS rule is not set

IPS Category CLI Configuration:
    Category all:
        Retire: True
    Category ios_ips basic:
        Retire: False
```

Step 5: (Optional) Alternative methods of copying the signature package to the router.

If you used TFTP to copy the file and do not intend to use one of these alternative methods, read through the procedures described here to become familiar with them. If you use one of these methods instead of TFTP, return to Step 4 to verify that the signature package loaded properly.

FTP method: Although the TFTP method is generally adequate, the signature file is rather large and FTP provides a more positive method of copying the file. You can use an FTP server to copy the signature file to the router with this command:

```
copy ftp://<ftp_user:password@Server_IP_address>/<signature_package> idconf
```

In the following example, the user admin must be defined on the FTP server with a password of cisco.

```
R1#copy ftp://admin:cisco@192.168.1.3/IOS-S364-CLI.pkg idconf
Loading IOS-S364-CLI.pkg !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 7608873/4096 bytes]
```

USB method: If there is no access to a FTP or TFTP server, you can use a USB flash drive to load the signature package to the router.

a. Copy the signature package onto the USB drive.

b. Connect the USB drive to one of the USB ports on the router.

c. Use the **show file systems** command to see the name of the USB drive. In the following output, a 4GB USB drive is connected to the USB port on the router as file system usbflash0:.

```
R1#show file systems
File Systems:

       Size(b)       Free(b)      Type  Flags  Prefixes
             -             -    opaque     rw   archive:
             -             -    opaque     rw   system:
             -             -    opaque     rw   tmpsys:
             -             -    opaque     rw   null:
             -             -   network     rw   tftp:
        196600        185972     nvram     rw   nvram:
*     64012288      14811136      disk     rw   flash:#
             -             -    opaque     wo   syslog:
             -             -    opaque     rw   xmodem:
             -             -    opaque     rw   ymodem:
             -             -   network     rw   rcp:
             -             -   network     rw   pram:
             -             -   network     rw   http:
             -             -   network     rw   ftp:
             -             -   network     rw   scp:
             -             -    opaque     ro   tar:
             -             -   network     rw   https:
             -             -    opaque     ro   cns:
    4001378304    3807461376  usbflash     rw   usbflash0:
```

d. Verify the contents of the flash drive using the **dir** command.

```
R1#dir usbflash0:
Directory of usbflash0:/
90  -rw-  6654646  Jan 5 2009 14:49:34 +00:00  IOS-S364-CLI.pkg
91  -rw-      805  Jan 5 2009 14:49:34 +00:00  realm-cisco.pub.key.txt
```

e. Use the **copy** command with the **idconf** keyword to copy the signature package to the router.

```
R1#copy usbflash0:IOS-S364-CLI.pkg idconf
```

The USB copy process can take 60 seconds or more, and no progress indicator is displayed. When the copy process is completed, numerous engine building messages display. These must finish before the command prompt returns.

Task 6. Test the IPS Rule and Modify a Signature

You can work with signatures in many ways. They can be retired and unretired, enabled and disabled, and their characteristics and actions can be changed. In this task, you first test the default behavior of IOS IPS by pinging it from the outside.

Step 1: Ping from R2 to the R1 serial 0/0/0 interface.

From the CLI on R2, ping R1 S0/0/0 at IP address 10.1.1.1. The pings are successful because the ICMP Echo Request signature 2004:0 is retired.

Step 2: Ping from R2 to PC-A.

From the CLI on R2, ping PC-A at IP address 192.168.1.3. These pings are also successful because of the retired signature. This is the default behavior of the IPS Signatures.

```
R2#ping 192.168.1.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Step 3: Modify the signature.

You can use Cisco IOS CLI to change signature status and actions for one signature or a group of signatures based on signature categories.

The following example shows how to un-retire the echo request signature, enable it, change the signature action to alert, and drop and reset for signature 2004 with a subsig ID of 0.

```
R1(config)#ip ips signature-definition
R1(config-sigdef)#signature 2004 0
R1(config-sigdef-sig)#status
R1(config-sigdef-sig-status)#retired false
R1(config-sigdef-sig-status)#enabled true
R1(config-sigdef-sig-status)#engine
R1(config-sigdef-sig-engine)#event-action produce-alert
R1(config-sigdef-sig-engine)#event-action deny-packet-inline
R1(config-sigdef-sig-engine)#event-action reset-tcp-connection
R1(config-sigdef-sig-engine)#exit
R1(config-sigdef-sig)#exit
R1(config-sigdef)#exit
Do you want to accept these changes? [confirm] <Enter>

*Jan  6 19:36:56.459: %IPS-6-ENGINE_BUILDS_STARTED:  19:36:56 UTC Jan 6 2009
*Jan  6 19:36:56.891: %IPS-6-ENGINE_BUILDING: atomic-ip - 306 signatures - 1
of 13 engines
*Jan  6 19:36:57.599: %IPS-6-ENGINE_READY: atomic-ip - build time 704 ms -
packets for this engine will be scanned
*Jan  6 19:36:57.979: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 1520 ms
```

Step 4: Ping from R2 to R1 serial 0/0/0 interface.

a. Start the syslog server.

b. From the CLI on R2 ping R1 S0/0/0 at IP address 10.1.1.1. Where the pings successful? Why or why not? _____

Step 5: Ping from R2 to PC-A.

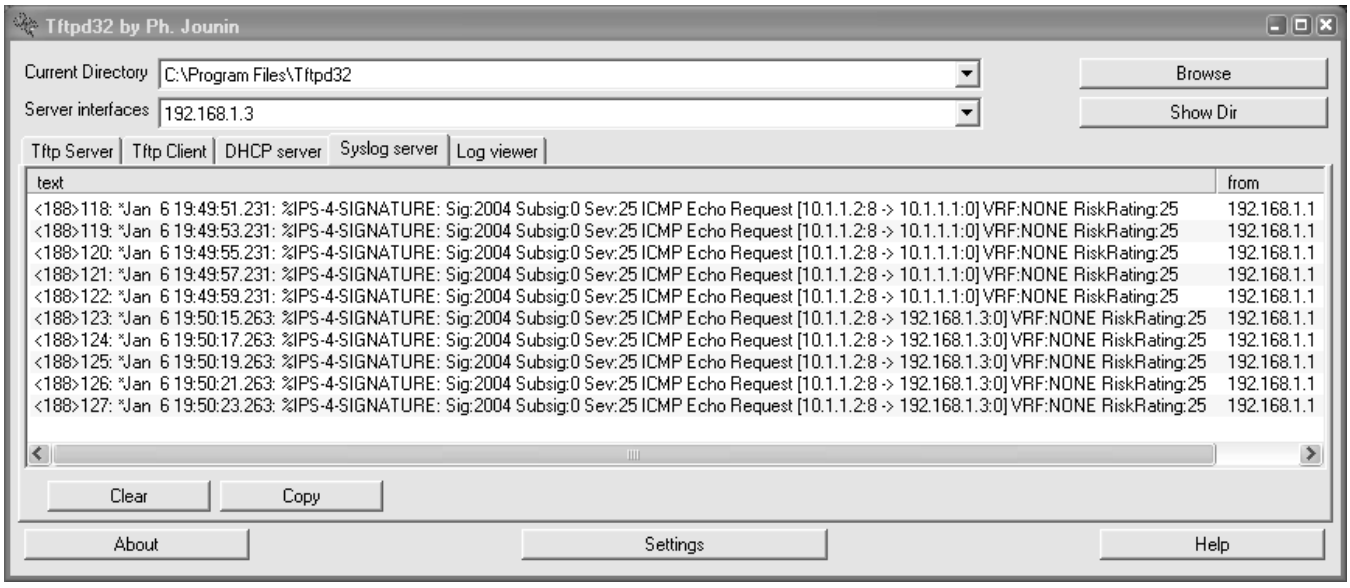
a. From the CLI on R2, ping R1 S0/0/0 at IP address 192.168.1.3. Were the pings successful?

_____

```
R2#ping 192.168.1.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

b. Notice the IPS messages from R1 on the syslog server screen below. How many messages were generated from the R2 pings to R1 and PC-A? _____



Note: The ICMP echo request IPS risk rating (severity level) is relatively low at 25. Risk rating can range from 0 to 100.

Task 7. (Optional) Test IPS with SuperScan

SuperScan is a freeware scanning tool that runs with Windows XP. It can detect open TCP and UDP ports on a target host. If the SuperScan program is available on PC-A or can be downloaded, you can perform this task.

SuperScan will test the IPS capabilities on R1. You will run the scanning program from PC-A and attempt to scan open ports on router R2. The IPS rule iosips, which is set on R1 F0/1 inbound, should intercept the scanning attempts and send messages to the R1 console and syslog server.

Step 1: Download the SuperScan program.

a. If SuperScan is not on PC-A, download the SuperScan 4.0 tool from the Scanning Tools group at http://www.foundstone.com.

b. Unzip the file into a folder. The SuperScan4.exe file is executable and installation is not required.

Step 2: Run SuperScan and set scanning options.

a. Start the SuperScan program on PC-A.

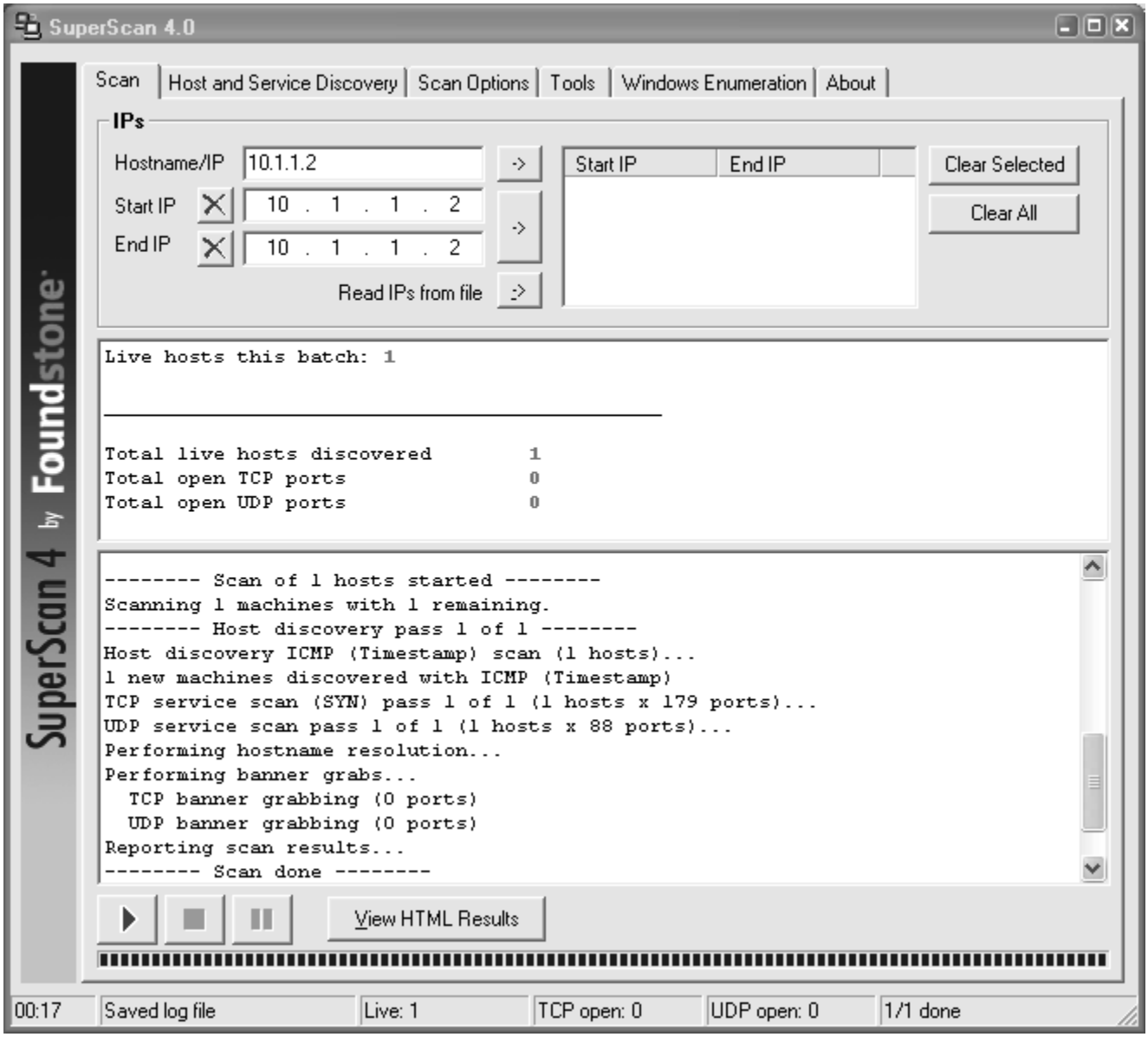
b. Click the **Host and Service Discovery** tab. Check the **Timestamp Request** check box, and uncheck the **Echo Request** check box.

c. Scroll the UDP and TCP port selection lists and notice the range of ports that will be scanned.

d. Click the **Scan** tab and enter the IP address of R2 S0/0/0 (10.1.1.2) in the **Hostname/IP** field.

> **Note:** You can also specify an address range, such as 10.1.1.1 to 10.1.1.254, by entering an address in the **Start IP** and **End IP** fields. The program scans all hosts with addresses in the range specified.

e. To start the scan, click the button with the blue arrow at the bottom left of the screen. Results of the scan are shown in the SuperScan window.



f. How many open TCP and UDP ports did SuperScan find on R2? Why do you think this is?

_____

g. Exit SuperScan.

Step 3: Observe the Syslog messages on R1.

You should see syslog entries on the R1 console and on the syslog server if it is enabled. The descriptions should include phrases such as “Invalid DHCP Packet” and “DNS Version Request.”

```
R1#
*Jan  6 19:43:35.611: %IPS-4-SIGNATURE: Sig:6054 Subsig:0 Sev:50 DNS
Version Request [192.168.1.3:1076 -> 10.1.1.2:53] VRF:NONE
RiskRating:50
*Jan  6 19:43:35.851: %IPS-4-SIGNATURE: Sig:4619 Subsig:0 Sev:75
Invalid DHCP Packet [192.168.1.3:1096 -> 10.1.1.2:67] VRF:NONE
RiskRating:75
```

a. What is the IPS risk rating or severity level (Sev:) of the DNS version request, signature 6054? _____

b. What is the IPS risk rating or severity level (Sev:) of the Invalid DHCP Packet, signature 4619? _____

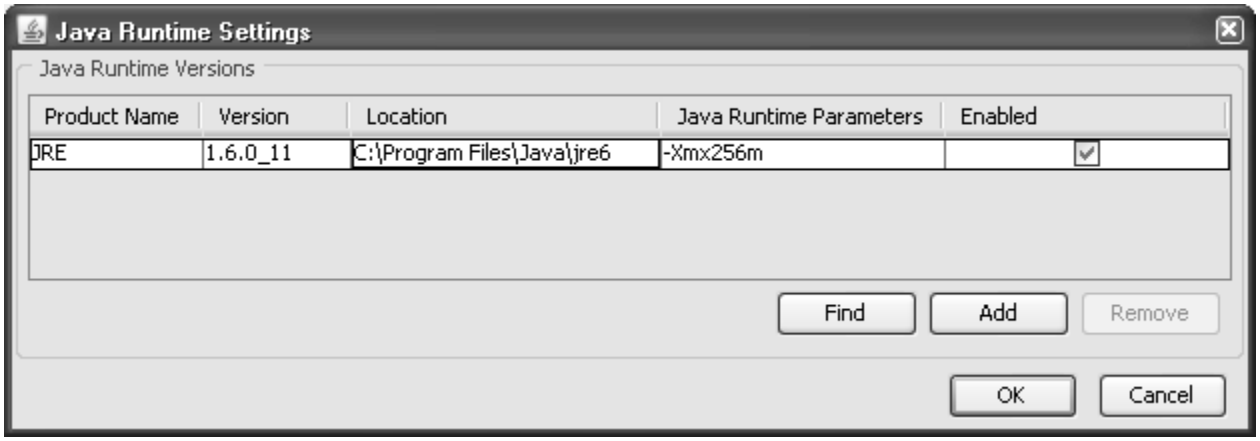
c. Which signature is considered by IPS to be more of a threat? _____

Part 3. Configuring IPS using SDM

In Part 3 of this lab, you configure IOS IPS on R3 using SDM.

Note: To support SDM configuration of IPS, PC-C should be running Java JRE version 6 or newer to set the Java heap to 256MB. This is done using the runtime parameter –Xmx256m. The latest JRE for Windows XP can be downloaded from Sun Microsystems at http://www.sun.com/.

The PC must have at least 512MB of RAM. From the PC Start Menu, click **Settings > Control Panel > Java** to open the Java Control Panel window. From the Java Control Panel window, click the **Java** tab and click the **View** button to enter or change the Java Applet Runtime Settings. The following screenshot shows setting the heap size to 256MB using the Runtime Parameter –Xmx256m.



Task 1. Verify Access to the R3 LAN from R2

In this task, you verify that, without IPS configured, external router R2 can access the R3 S0/0/1 interface and PC-C on the R3 internal LAN.

Step 1: Ping from R2 to R3.

a. From R2, ping the R3 interface S0/0/1 at IP address 10.2.2.1.

```
R2#ping 10.2.2.1
```

b. Were the results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Step 2: Ping from R2 to PC-C on the R3 LAN.

a. From R2, ping PC-C on the R3 LAN at IP address 192.168.3.3.

```
R2#ping 192.168.3.3
```

b. Were the results successful? _____

c. If the pings are not successful, troubleshoot the basic device configurations before continuing.

Step 3: Display the R3 running config prior to starting SDM.

a. Issue the **show run** command to review the current basic configuration on R3.

b. Verify the R3 basic configuration as performed in Part 1 of the lab. Are there any security commands related to IPS? _____

Task 2. Prepare the Router for SDM and IPS

Step 1: Configure the enable secret password and HTTP router access prior to starting SDM.

a. From the CLI, configure the enable secret password for use with SDM on R3.

```
R3(config)#enable secret cisco12345
```

b. Enable the HTTP server on R3.

```
R3(config)#ip http server
```

Step 2: Verify or create the IPS directory in router flash.

a. From the R3 CLI, display the content of flash memory using the **show flash** command and check for the ipsdir directory.

```
R3#show flash
```

b. If this directory is not listed, create it by entering the command **mkdir ipsdir** in privileged EXEC mode.

```
R3#mkdir ipsdir
Create directory filename [ipsdir]?
Created dir flash:ipsdir
```

c. From the R3 CLI, verify that the directory is present using the **dir flash:ipsdir** command.

```
R3#dir flash:ipsdir

Directory of flash:/ipsdir/

No files in directory
```

Note: The directory exists, but there are currently no files in it.

Task 3. Prepare the TFTP Server

Step 1: Download the TFTP server.

The Tftp32 freeware TFTP server is used in this task. Many other free TFTP servers are also available. If a TFTP server is not currently available on PC-C, you can download the latest version of Tftpd32 from http://tftpd32.jounin.net/. If it is already installed, go to Step 2.

This lab uses the Tftpd32 TFTP server. This software also includes a syslog server that runs simultaneously with the TFTP server.

Step 2: Start the TFTP server on PC-A and verify the IPS file directory.

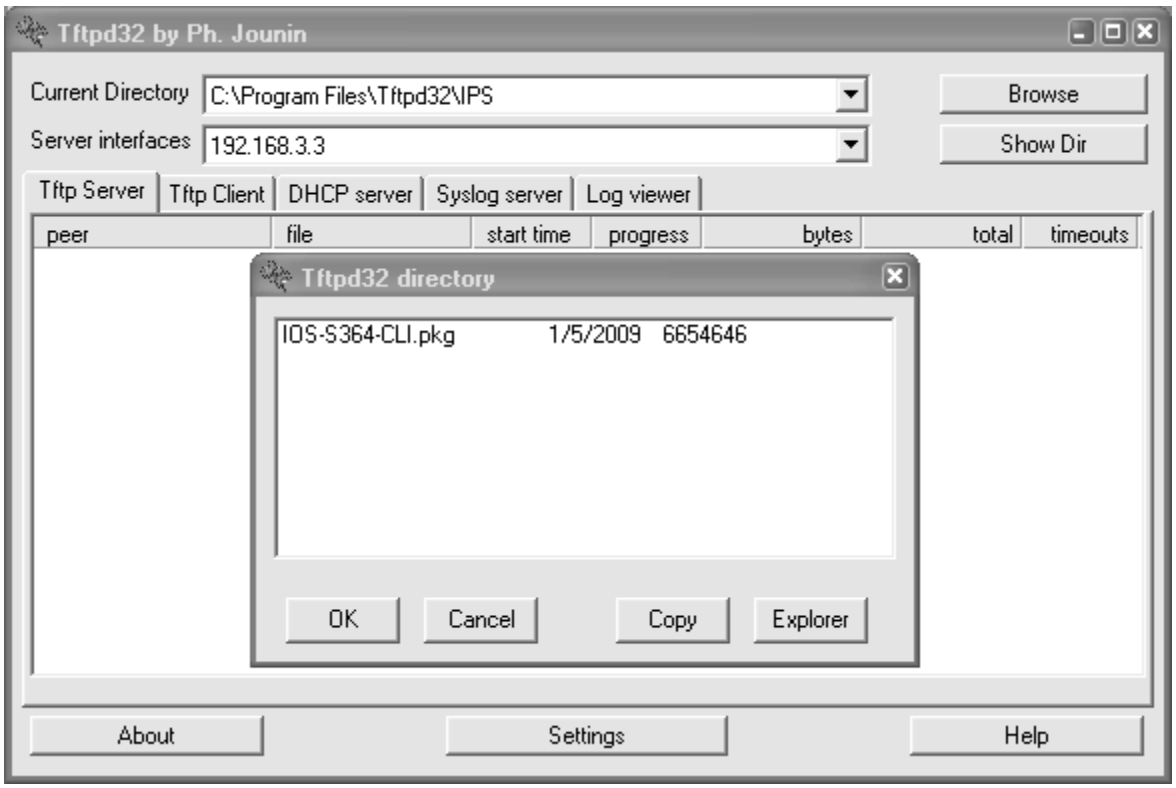
Verify connectivity between R3 and PC-C, the TFTP server, using the **`ping`** command.

a. Verify that the PC has the IPS Signature package file in a directory on the TFTP server. This file is typically named IOS-S*xxx*-CLI.pkg, where *xxx* is the signature file version.

Note: If this file is not present, contact your instructor before continuing.

b. Start Tftpd32 or another TFTP server and set the default directory to the one with the IPS Signature package. The Tftpd32 screen is shown here with the C:\Program Files\Tftpd32\IPS directory contents displayed. Take note of the filename for use in the next step.

c. What is the name of the signature file? _____



Task 4. Configure IPS Using SDM

Step 1: Access SDM and set command delivery preferences.

a. Run the SDM application or open a browser on PC-C and start SDM by entering the R3 IP address 192.168.3.1 in the address field.

b. Log in with no username and the enable secret password cisco12345.

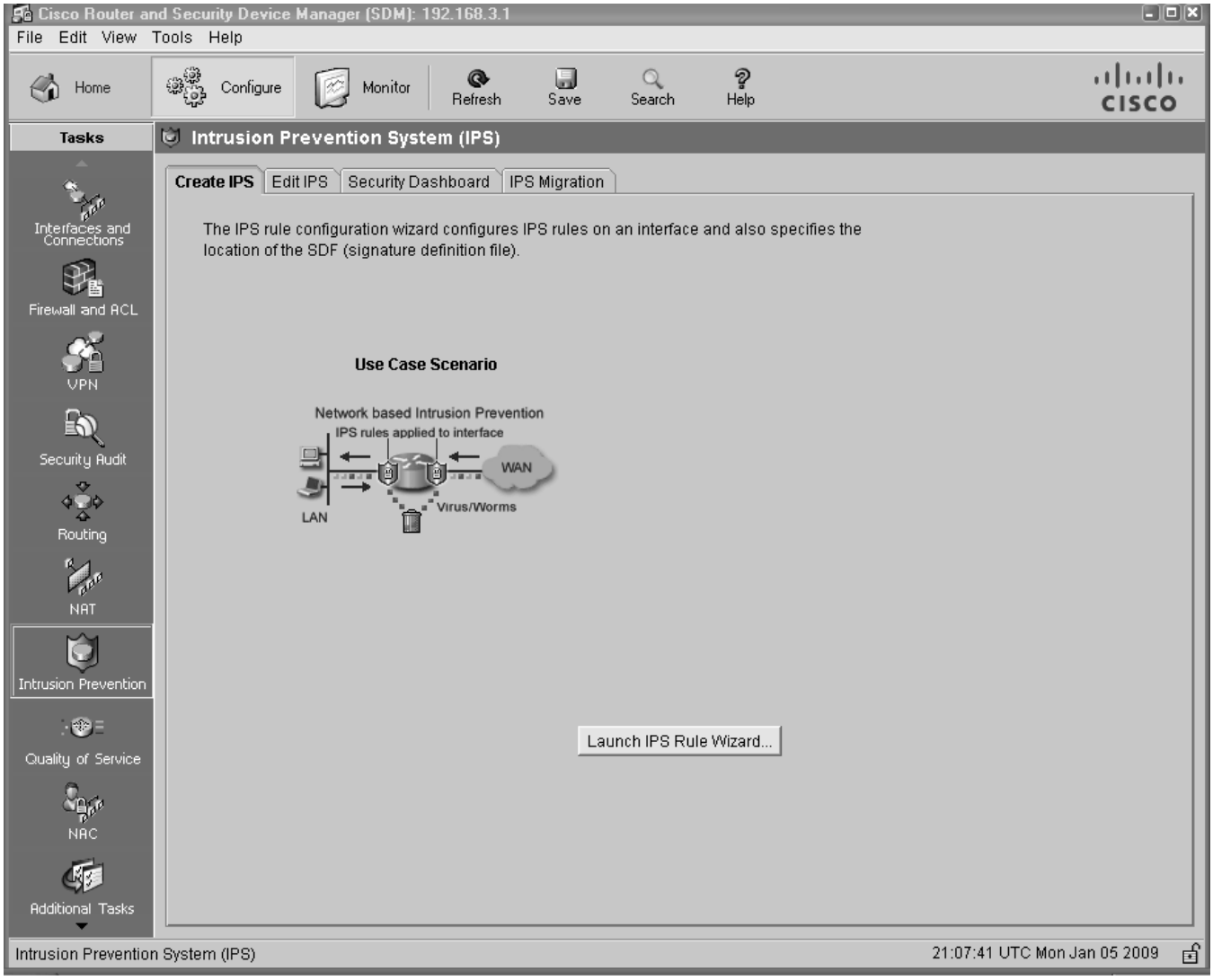
Note: If you are using Java version 1.6 or later, the Java console displays by default when SDM is run. If the Java console displays, you can close it. You can also start the Java plug-in application and select **Advanced > Java Console > Do not start console**. The Java console will not appear again unless you change the setting.

c. In the **Authentication Required** and **IOS IPS Login** dialog boxes, enter cisco12345 in the **Password** field and click **OK**.

d. Configure SDM to allow you to preview the commands before sending them to the router. Select **Edit** > **Preferences.** In the User Preferences window, check the **Preview commands before delivering to router** check box and click **OK**.

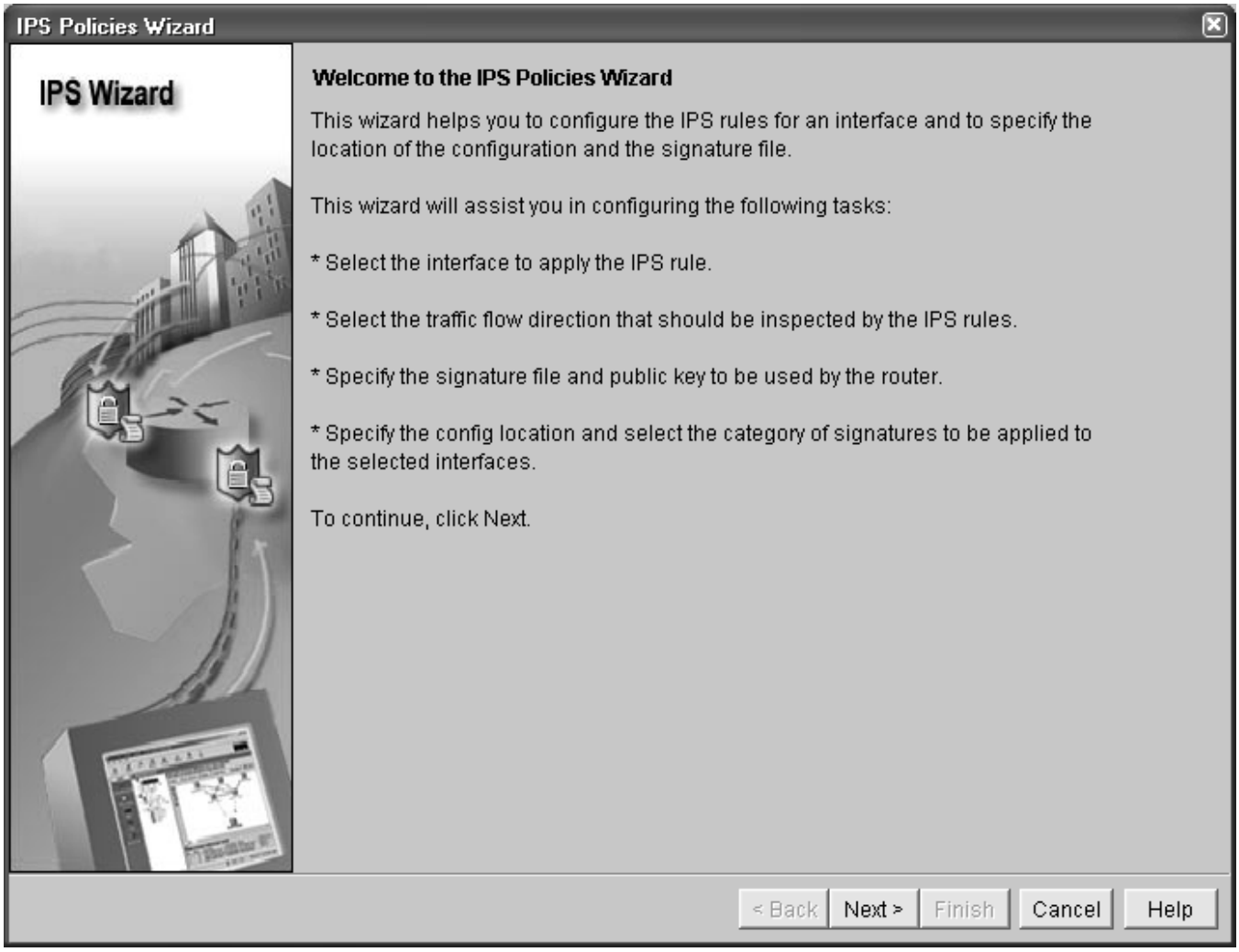
Step 2: Use the SDM IPS Wizard to configure Cisco IOS IPS.

a. Click the **Configure** button at the top of the SDM screen and then select **Intrusion Prevention > Create IPS**.



b. Click the **Launch IPS Rule Wizard** button to open the Welcome to the IPS Policies Wizard window.

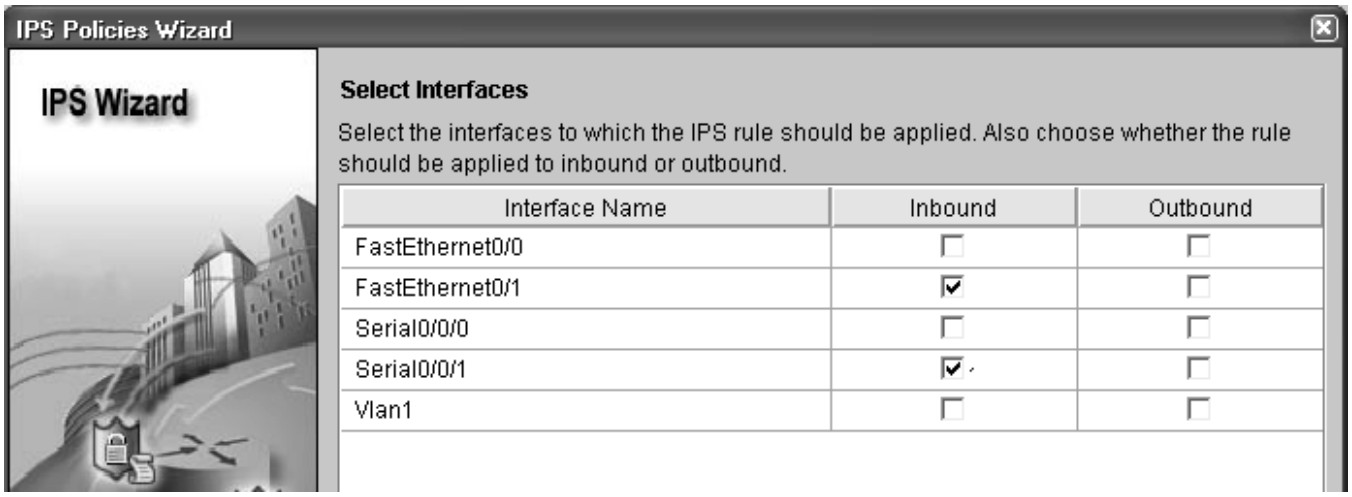
c. Read the information on the IPS Policies Wizard screen to become familiar with what the wizard does. Click **Next.**



Note: SDEE dialog boxes might appear. Read the information and click **OK** for each dialog box.

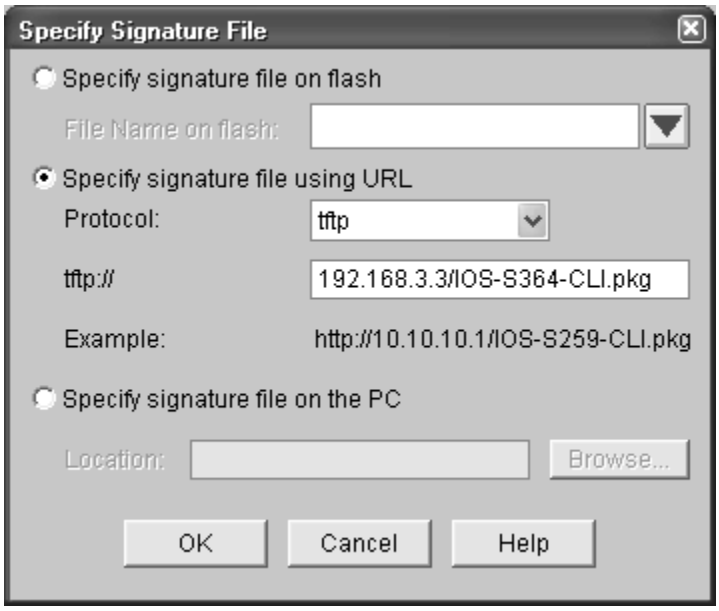
d**.** In the Select Interfaces window, check the **Inbound** check box for FastEthernet0/1 and Serial0/0/1. Click **Next.**

> **Note:** Selecting inbound on both interfaces allows IPS to monitor attacks on the router from the internal and external network.



e. In the Signature File and Public Key window, click the ellipsis (**…**) button next to **Specify the Signature File You Want to Use with IOS IPS** to open the Specify Signature File window. Confirm that the **Specify Signature File using URL** option is chosen.

f. For Protocol, select **tftp** from the drop-down menu. Enter the IP address of the PC-C TFTP server and the filename. For example, 192.168.3.3/IOS-S364-CLI.pkg.



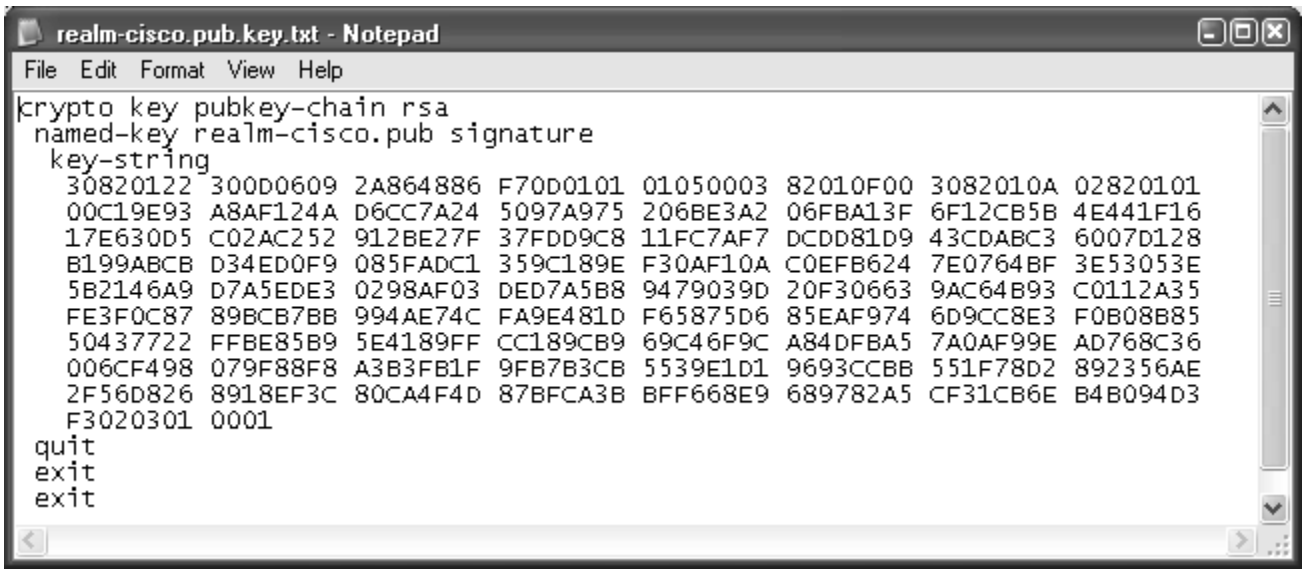
g. What other options can be specified as a source for the Signature File?

_____

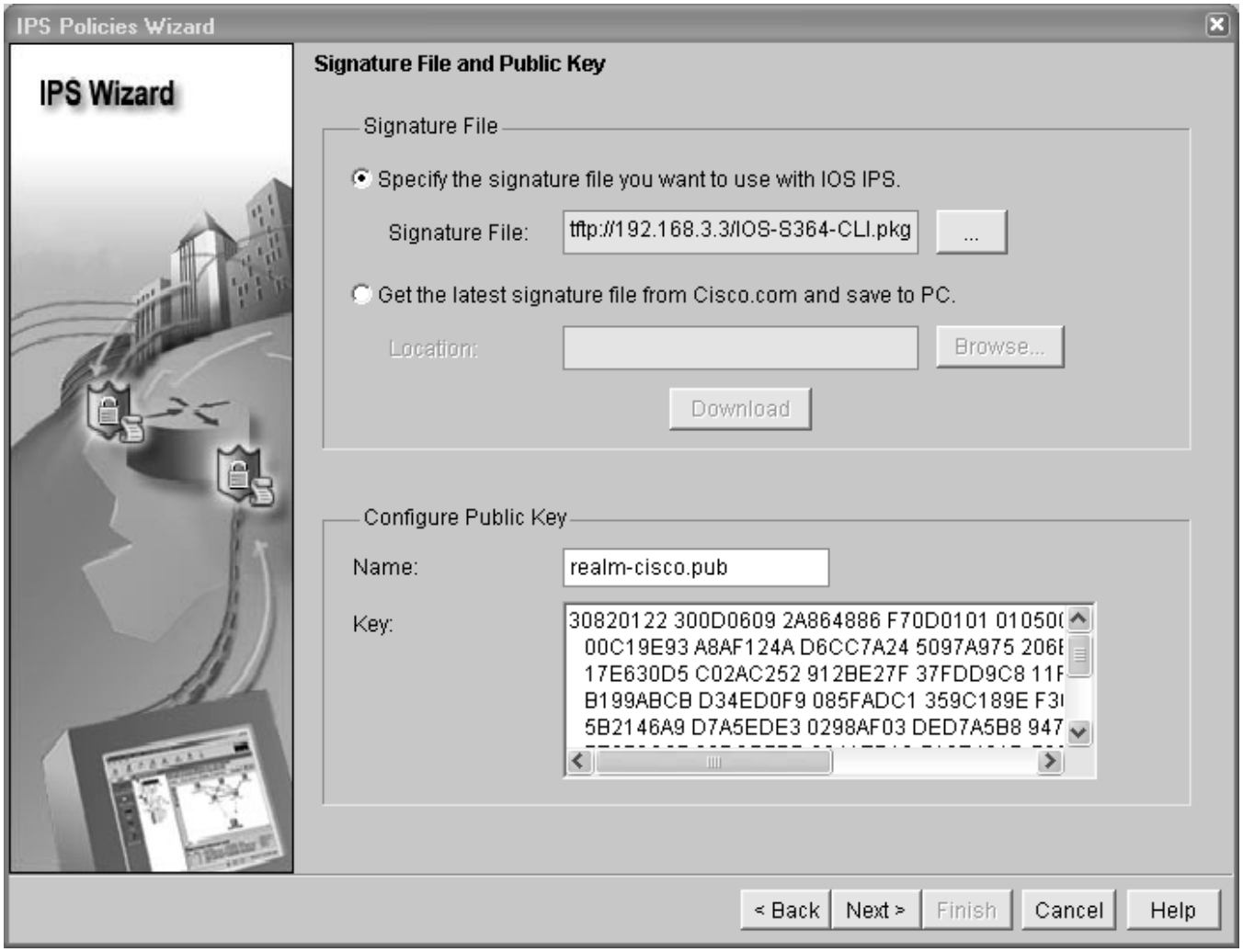
h. Click **OK** to return to the Signature File and Public Key window. In the Configure Public Key section of the Signature File and Public Key window, enter realm-cisco.pub in the **Name** field.

Each change to the signature configuration is saved in a delta file. This file must be digitally signed with a public key. You can obtain a key from Cisco.com and paste the information in the Name and Key fields. In this lab, you will copy and paste the key from a text file on PC-C.

i. Open the realm-cisco-pub-key.txt file located on the PC-C desktop. The following is an example from the realm-cisco-pub-key.txt file.



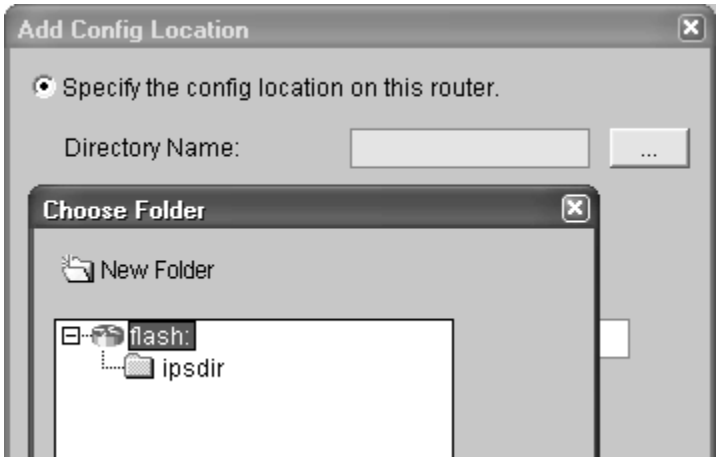
j. Copy the text between the phrase **key-string** and the word **quit** into the **Key** field in the Configure Public Key section. The Signature File and Public Key window should look similar to the following when the entries are completed.



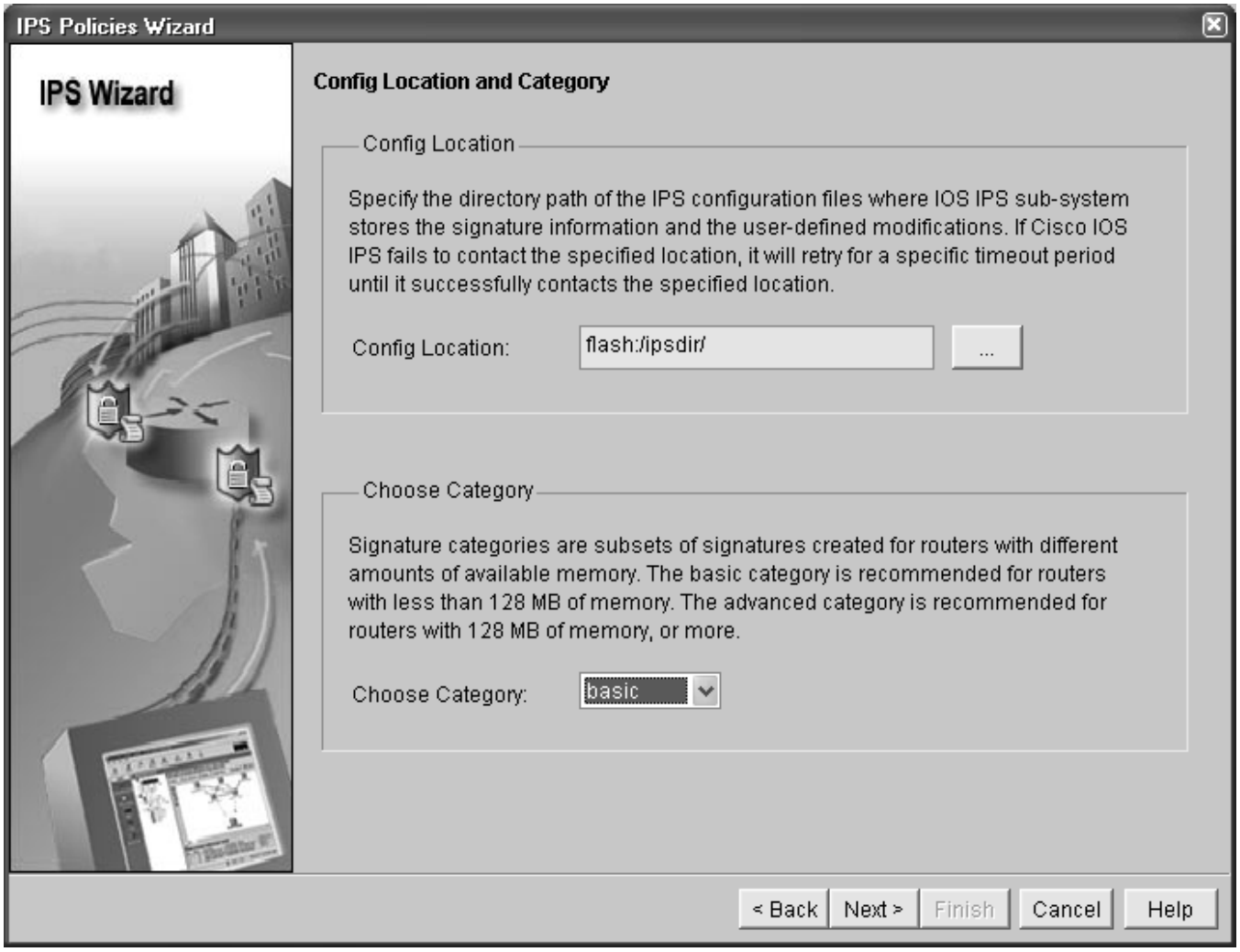
k. Click **Next** to display the Config Location and Category window. This is used to specify where to store the signature information. This file is used by the Cisco IOS IPS for detecting attacks from coming into the FastEthernet0/1 or Serial0/0/1 interfaces.

l. In the Config Location and Category window in the Config Location section, click the ellipsis (**...**) button next to **Config Location** to add the location.

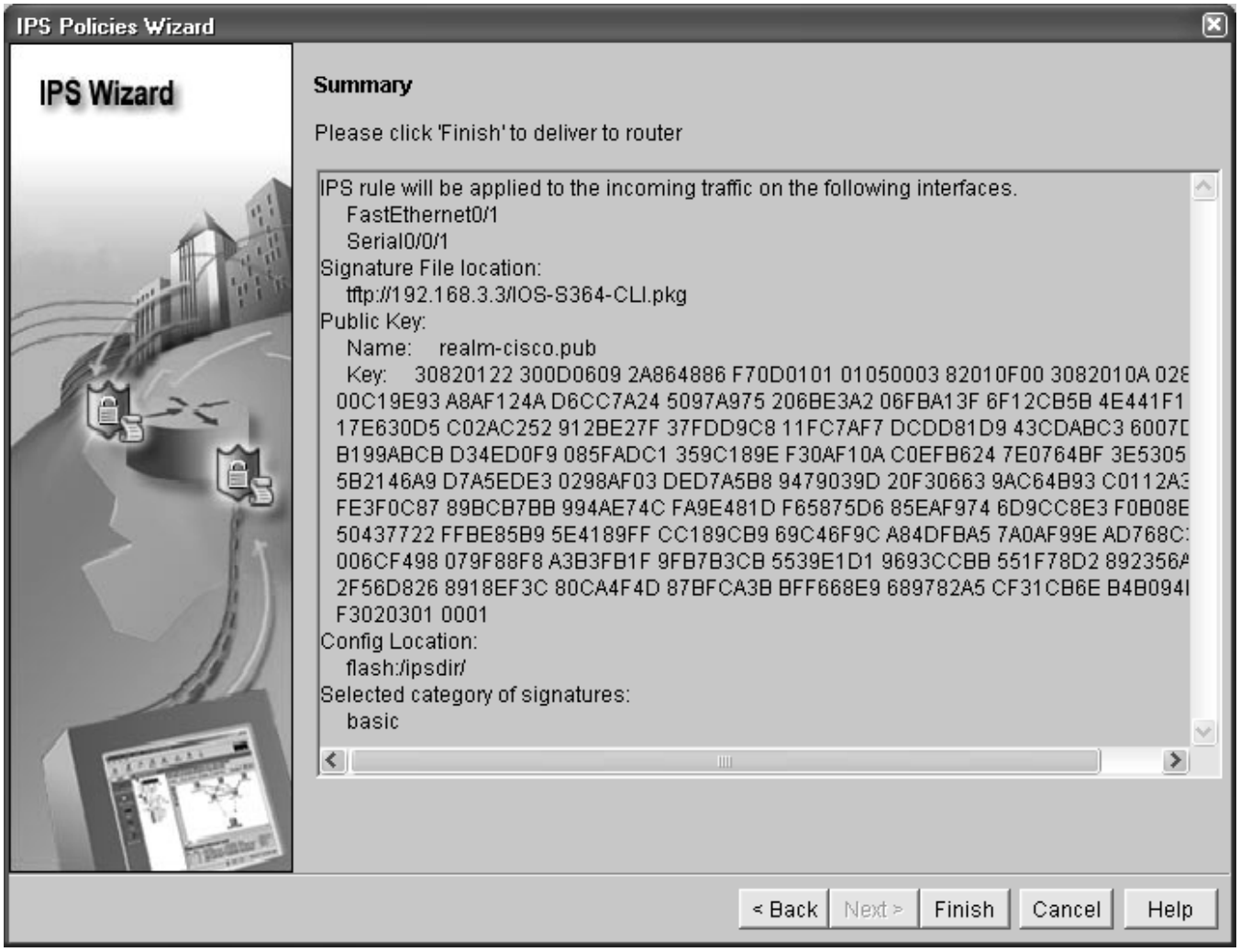
m. Verify that **Specify the config location on this router** is selected. Click the ellipsis (**...**) button. Click the plus sign (+) next to flash. Choose **ipsdir** and then click **OK**.



n. Because router memory and resource constraints might prevent using all the available signatures, there are two categories of signatures: basic and advanced. In the **Choose Category** field of the Config Location and Category window, choose **basic**. The Config Location and Category window should look similar to the following when the entries are completed.



o. Click **Next** in the Cisco SDM IPS Policies Wizard window. The Summary window appears. Examine the IPS configuration information shown.

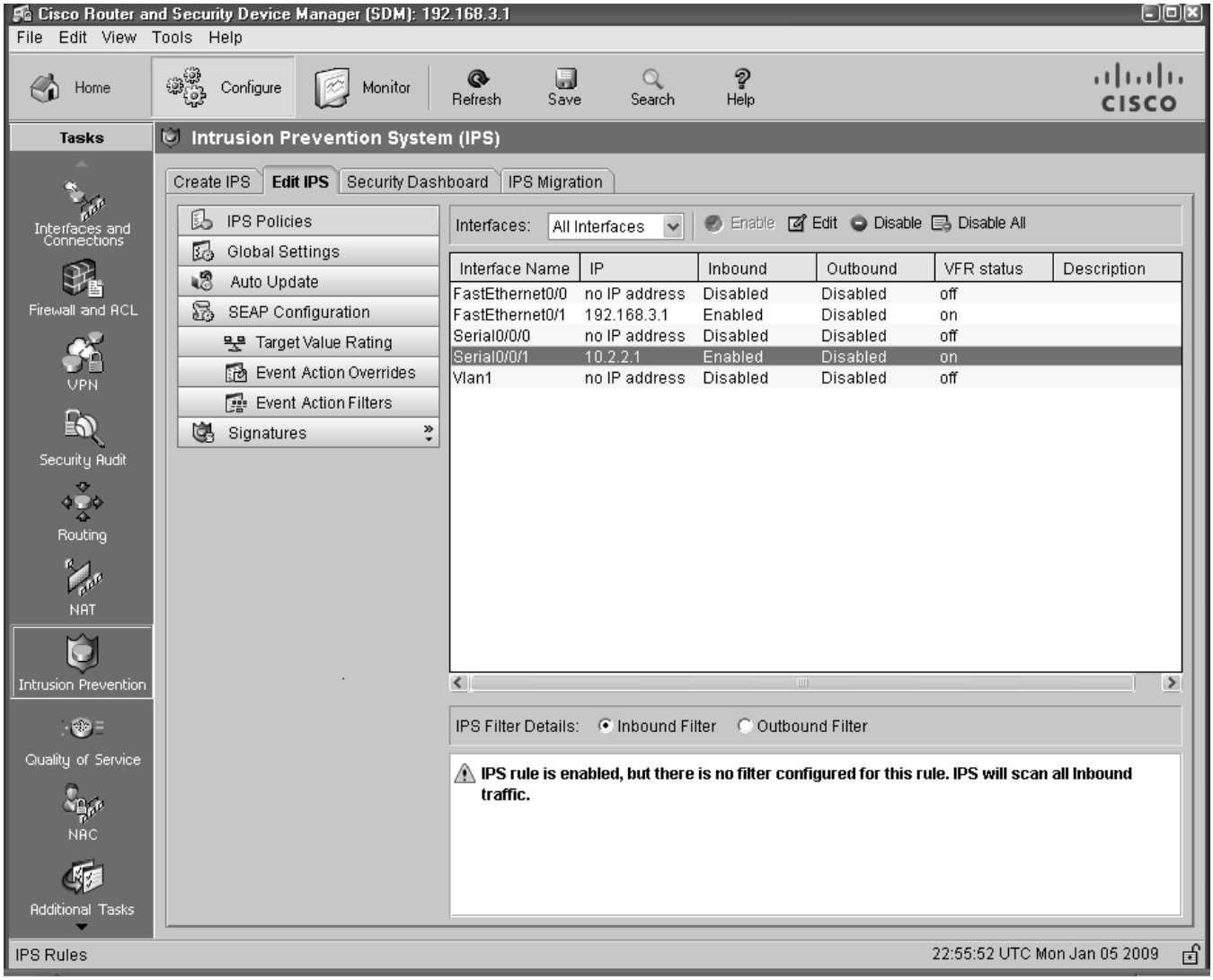


p. Click **Finish** in the IPS Policies Wizard window and review the commands that will be delivered to the router.

q. Click **Deliver**. How many commands were delivered to the router? _____

r. When the Commands Deliver Status window is ready, click **OK**. The IOS IPS Configuration Status window opens stating that it can take several minutes for the signatures to be configured.

s. When the signature configuration process has completed, you return to the IPS window with the Edit IPS tab selected. Your screen should look similar to the following.



t. Select interface Serial0/0/1 from the list. What information is displayed at the bottom of the screen?

_____

Task 5. Modify Signature Settings

Step 1: Verify connectivity.

From PC-C, ping R3. The pings should be successful.

Step 2: Configure the IPS application to drop ping (echo request) traffic.

a. From SDM, click **Configure** and select **Intrusion Prevention > Edit IPS > Signatures**. How many total signatures are there? _____

Are all of them enabled? _____

b. In the **View By** drop-down list, choose **Sig ID**.

c. In the **Sig ID** field, enter 2004, and then click **Go**. What is Sig ID 2004?

_____

d. Do you know why the pings from PC-C in Step 1 were successful?

_____

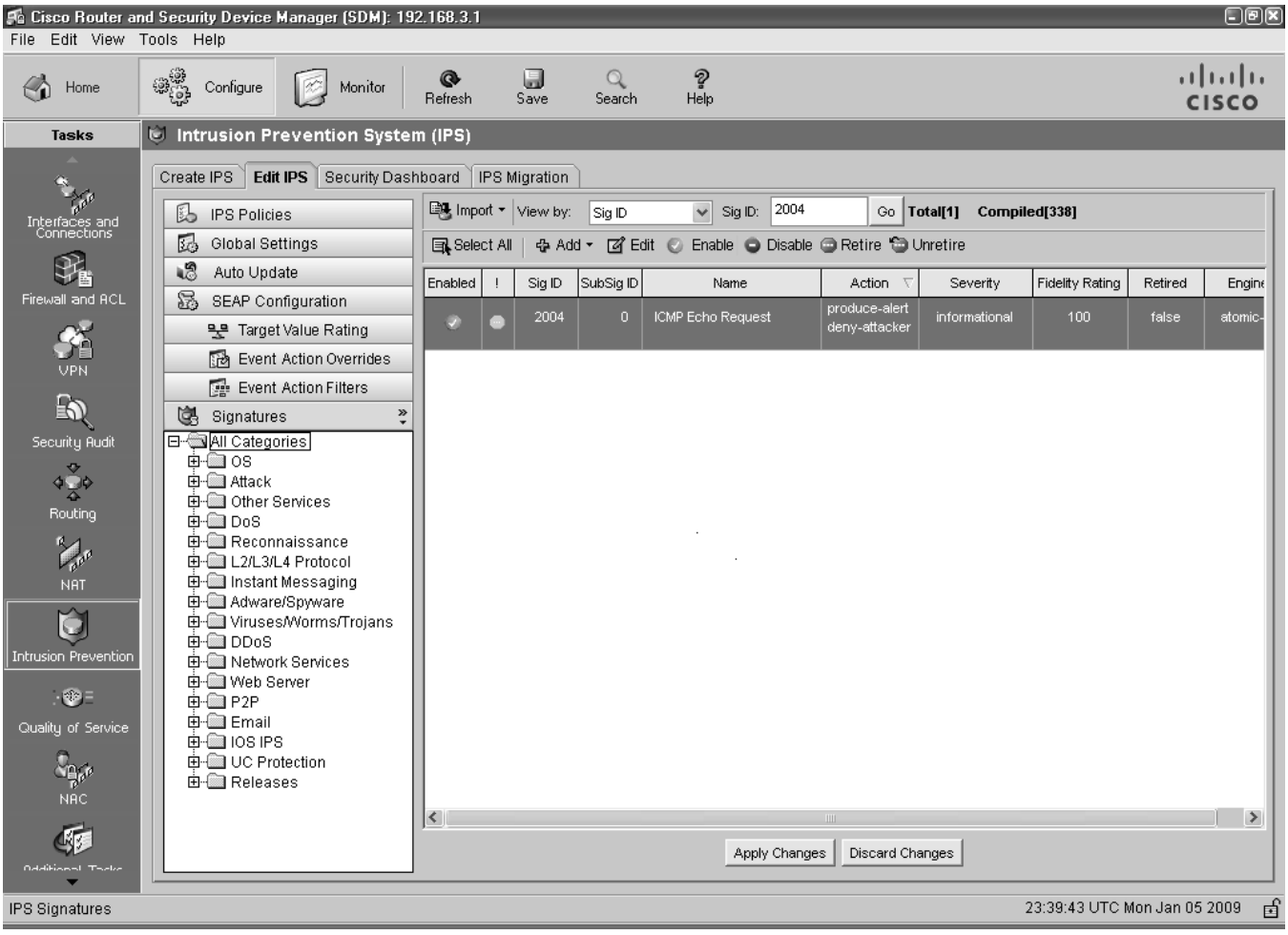
e. Select signature **2004**, click the **Unretire** button**,** and then click the **Enable** button.

f. Right-click the signature and choose **Actions** from the context menu.

g. Choose **Deny Packet Inline** and leave the **Produce Alert** check box checked. Click **OK**.

h. Click **Apply Changes**. Your screen should look similar to the following.

Note: It may take some time for the changes to take effect.



i**.** Return to PC-C and ping R3 again. Were the pings successful this time?

_____

Task 6. Configure IPS Global Settings

In this task, you enable the syslog and SDEE global settings using the Cisco SDM GUI.

a. From SDM, click **Configure** and select **Intrusion Prevention > Edit IPS > Global Settings**.

b. Verify that the syslog and SDEE options are enabled.

Note: Even if the Syslog and SDEE options are already enabled, click the **Edit** button and explore the options available in the Edit Global Settings dialog box. Examine the options to learn whether Cisco IOS IPS has set the default to fail opened or to fail closed.

Task 7. Verify IPS Functionality with SDM Monitor and Ping

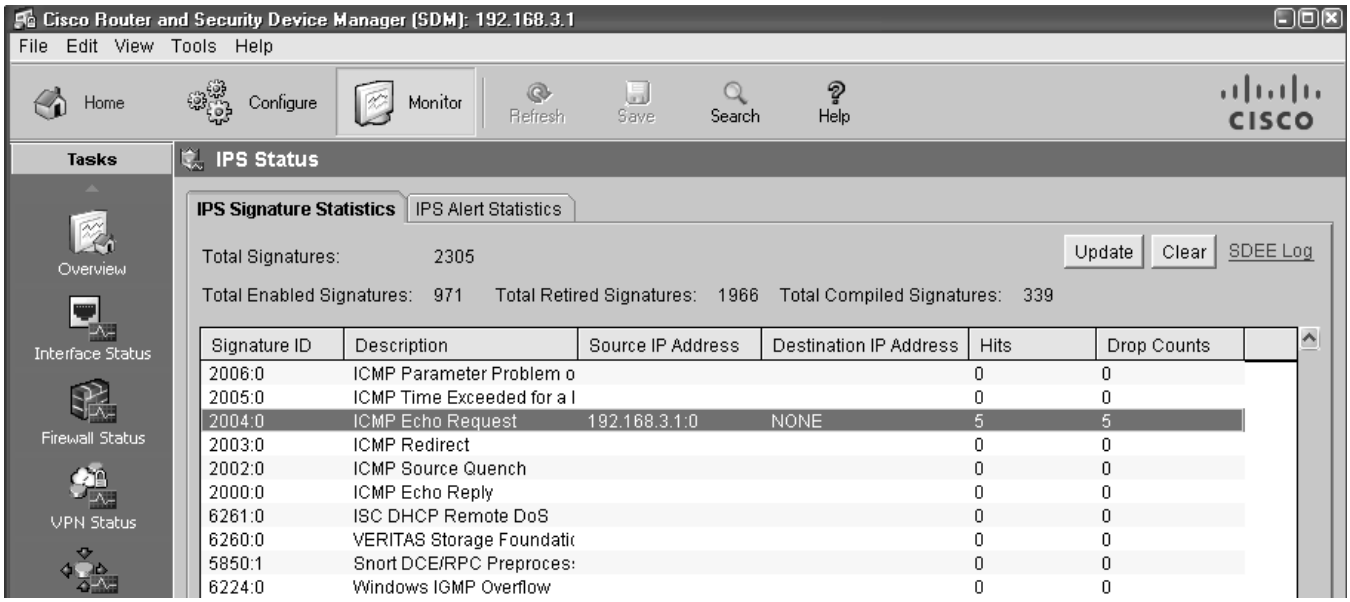
In this task, you demonstrate how the Cisco IOS IPS protects against an external attacker using ping.

a. From the R2 CLI, ping the R3 Fa0/1 interface at 192.168.3.1. Were the pings successful?

_____

b. From SDM, click the **Monitor** button and select **IPS Status**. The IPS Signature Statistics tab is selected by default. Wait for the screen to populate.

c. Scroll to near the bottom to locate the signature ID 2004 ICMP echo request. You should see an entry similar to the one below indicating that IPS identified the ping attempt from R2. Notice that there are five hits and five drops for signature ID 2004, detected on Fa0/1 IP address 192.168.3.1.

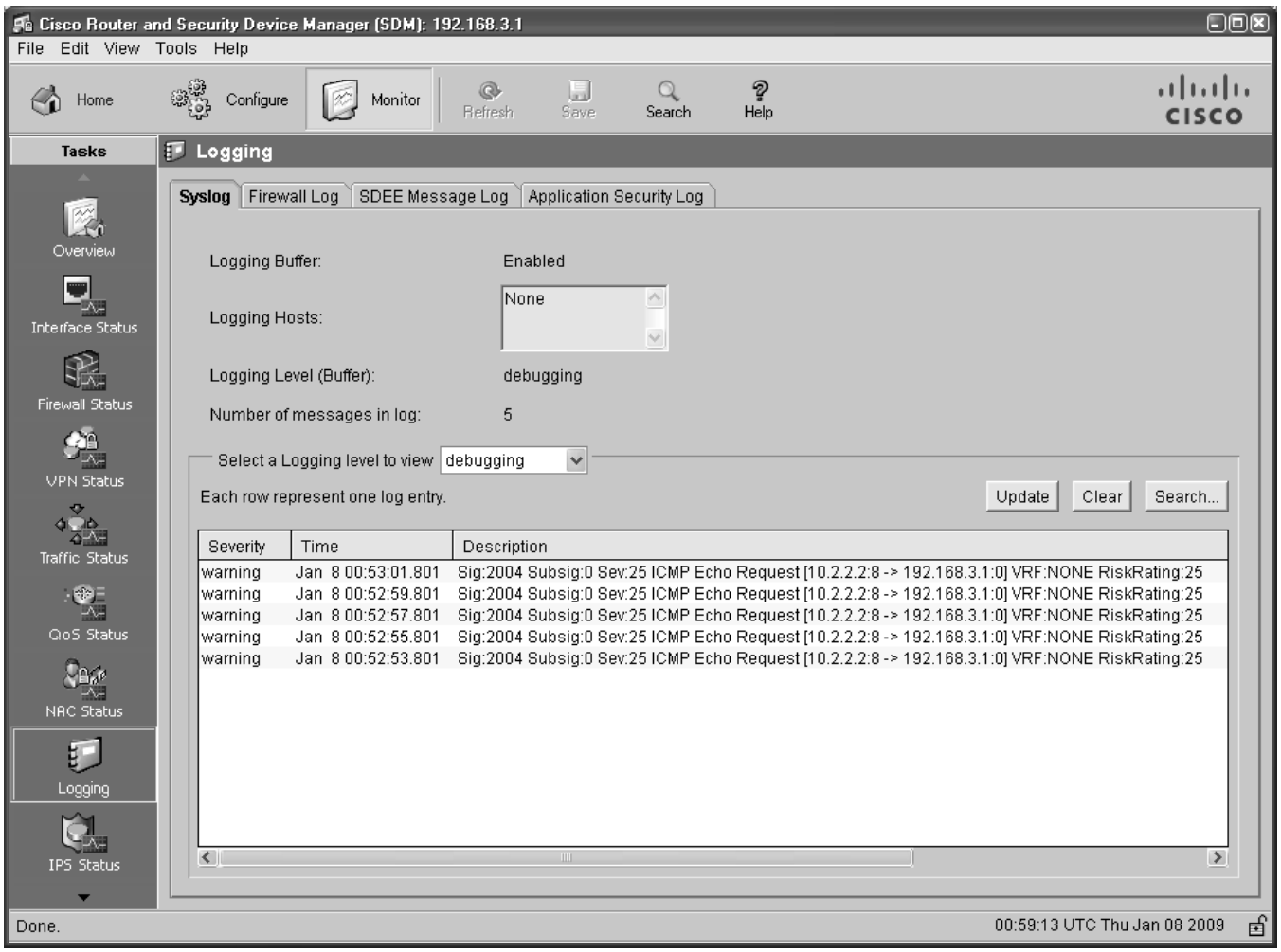


d. From SDM, Click the **Monitor** button and select **Logging**.

e. A number of Syslog message are displayed. Click the **Clear** button to clear the log.

f. From the R2 CLI, ping the R3 Fa0/1 interface at 192.168.3.1 again.

g. Click the **Update** button. You will see that the Cisco IOS IPS logged the ping attempts from R2.



Task 8. (Optional) Verify IPS Functionality with SDM Monitor and SuperScan

In this task, you demonstrate how the Cisco IOS IPS protects against an internal attacker using SuperScan. SuperScan is a freeware scanning tool that runs with Windows XP that can detect open TCP and UDP ports on a target host. You can perform this task if the SuperScan program is available on PC-C or if it can be downloaded.

SuperScan will test the IPS capabilities on R3. You will run the scanning program from PC-C and attempt to scan open ports on router R2. The IPS rule iosips, which is set on R3 Fa0/1 inbound, should intercept the scanning attempts and send messages to the R3 console and SDM syslog.

Step 1: Download the SuperScan program.

a. If SuperScan is not on PC-C, download the SuperScan 4.0 tool from the Scanning Tools group at http://www.foundstone.com.

b. Unzip the file into a folder. The SuperScan4.exe file is executable and installation is not required.

Step 2: Run SuperScan and set scanning options.

a. Start SuperScan on PC-C. Click the **Host and Service Discovery** tab. Check the **Timestamp Request** check box, and uncheck the **Echo Request** check box. Scroll the UDP and TCP port selection lists and notice the range of ports that will be scanned.

b. Click the **Scan** tab and enter the IP address of R2 S0/0/1 (10.2.2.2) in the **Hostname/IP** field.

> **Note:** You can also specify an address range, such as 10.2.2.1 to 10.2.2.254, by entering an address in the **Start IP** and **End IP** fields. The program will scan all hosts with addresses in the range specified.

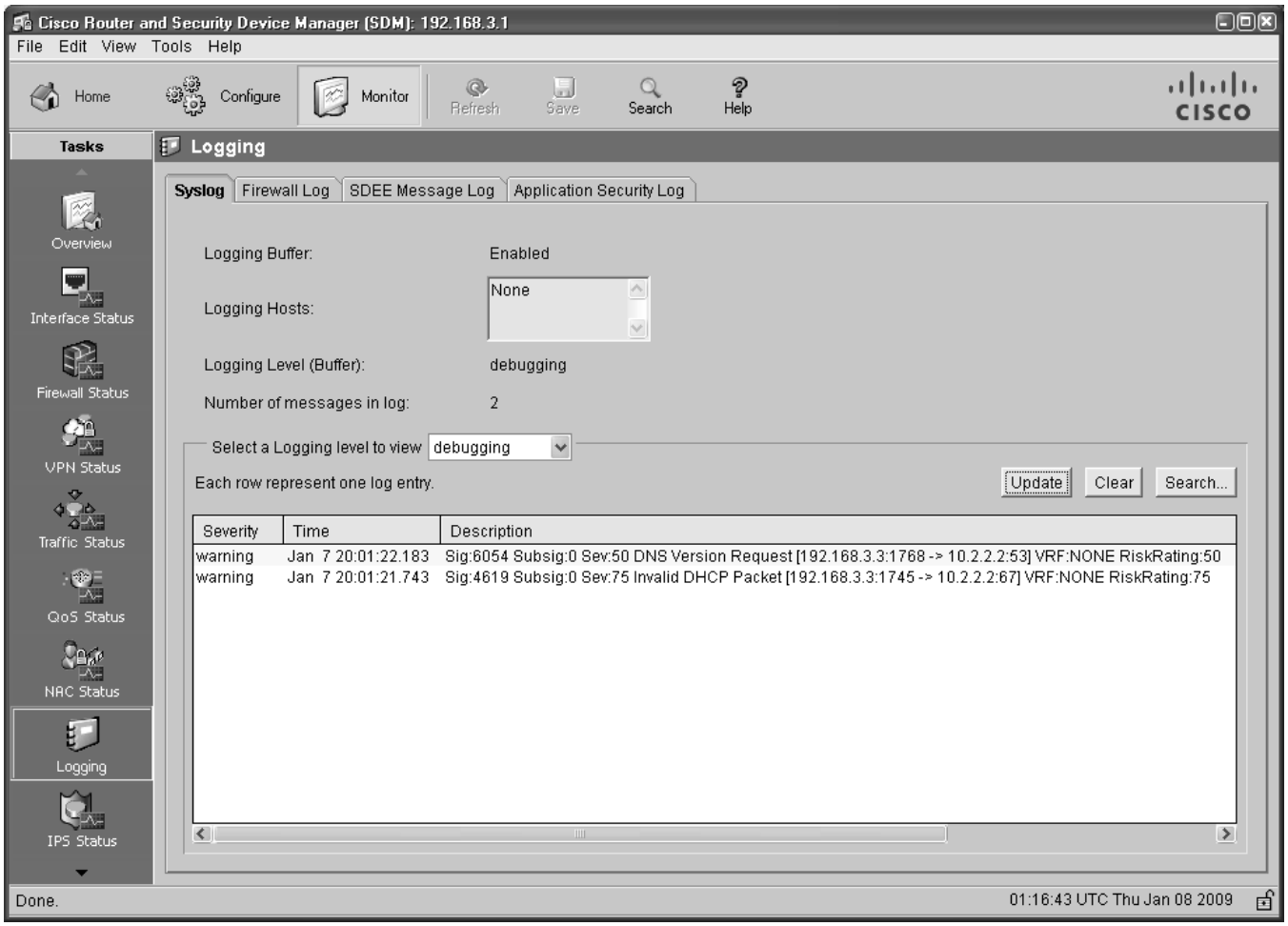
c. Click the button with the blue arrow in the lower left corner of the screen to start the scan.

Step 3: Check the results with SDM logging.

a. From Cisco SDM, choose **Monitor > Logging**.

b. Click the **Update** button. You will see that the Cisco IOS IPS has been logging the port scans generated by SuperScan.

c. You should see syslog messages on R3 and entries in the SDM Monitor Log with descriptions that include one of these phrases: “Invalid DHCP Packet” or “DNS Version Request.”



d. Close the SuperScan window.

Task 9. Compare the Results for Different IPS Configuration Methods

a. On R1, display the running configuration after IPS was configured with IOS CLI commands. Note the commands related to IPS.

_____
_____
_____
_____
_____

b. On R3, from the menu bar, select **View** > **Show Running Config** to display the running configuration after IPS was configured with the SDM GUI. Note the commands related to IPS.

_____
_____
_____
_____
_____

c. What differences are there between the CLI-based running configuration and the SDM-based running configuration?

_____
_____
_____
_____
_____

Task 10. Reflection

a. What are some advantages and disadvantages to using CLI or SDM to configure IPS?

_____
_____
_____
_____
_____

b. With version 5.x signature files, if changes are made to a signature, are they visible in the router running configuration?

_____
_____
_____
_____
_____

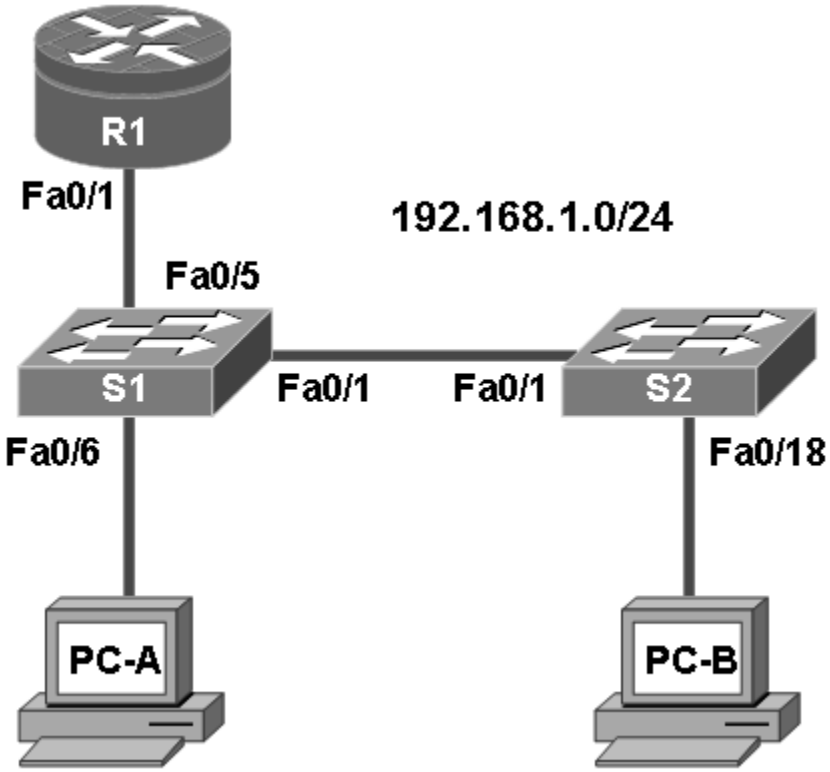
Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1700	Fast Ethernet 0 (FA0)	Fast Ethernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2600	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
2800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Chapter 6: Lab A: Securing Layer 2 Switches

Topology



IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	Fa0/1	192.168.1.1	255.255.255.0	N/A	S1 FA0/5
S1	VLAN 1	192.168.1.2	255.255.255.0	N/A	N/A
S2	VLAN 1	192.168.1.3	255.255.255.0	N/A	N/A
PC-A	NIC	192.168.1.10	255.255.255.0	192.168.1.1	S1 FA0/6
PC-B	NIC	192.168.1.11	255.255.255.0	192.168.1.1	S2 FA0/18

Objectives

Part 1: Configure Basic Switch Settings

- Build the topology.
- Configure the host name, IP address, and access passwords.

Part 2: Configure SSH Access to the Switches

- Configure SSH access on the switch.

- Configure an SSH client to access the switch.
- Verify the configuration.

Part 3: Secure Trunks and Access Ports

- Configure trunk port mode.
- Change the native VLAN for trunk ports.
- Verify trunk configuration.
- Enable storm control for broadcasts.
- Configure access ports.
- Enable PortFast and BPDU guard.
- Verify BPDU guard.
- Enable root guard.
- Configure port security.
- Verify port security.
- Disable unused ports.

Part 4: Configure SPAN and Monitor Traffic

- Configure Switched Port Analyzer (SPAN).
- Monitor port activity using Wireshark.
- Analyze a sourced attack.

Background

The Layer 2 (Data Link) infrastructure consists mainly of interconnected Ethernet switches. Most end-user devices, such as computers, printers, IP phones and other hosts, connect to the network via Layer 2 access switches. As a result, they can present a network security risk. Similar to routers, switches are subject to attack from malicious internal users. The switch Cisco IOS software provides many security features that are specific to switch functions and protocols.

In this lab, you configure SSH access and Layer 2 security for switches S1 and S2. You also configure various switch protection measures, including access port security, switch storm control, and Spanning Tree Protocol (STP) features such as BPDU guard and root guard. Lastly, you use Cisco SPAN to monitor traffic to specific ports on the switch.

Note: The router commands and output in this lab are from a Cisco 1841 with Cisco IOS Release 12.4(20)T (Advanced IP image). The switch commands and output are from a Cisco WS-C2960-24TT-L with Cisco IOS Release 12.2(46)SE (C2960-LANBASEK9-M image). Other routers, switches, and IOS versions may be used. See the Router Interface Summary table at the end of the lab to determine which interface identifiers to use based on the equipment in the lab. Depending on the router or switch model and IOS version, the commands available and output produced might vary from what is shown in this lab.

Note: Make sure that the router and the switches have been erased and have no startup configurations.

Required Resources

- One router (Cisco 1841 with Cisco IOS Release 12.4(20)T1 or comparable)

- Two switches (Cisco 2960 or comparable with cryptography IOS image for SSH support – Release 12.2(46)SE or comparable)
- PC-A (Windows XP or Vista with a PuTTY SSH client and Wireshark)
- PC-B (Windows XP or Vista with a PuTTY SSH client and SuperScan)
- Ethernet cables as shown in the topology
- Rollover cables to configure the switches via the console

Part 1. Basic Device Configuration

In Part 1 of this lab, you set up the network topology and configure basic settings such as the host names, IP addresses, and device access passwords.

Note: Perform all tasks on router R1 and switches S1 and S2. The procedure for S1 is shown here as an example.

Step 1: Cable the network as shown in the topology.

Attach the devices shown in the topology diagram and cable as necessary.

Step 2: Configure basic settings for the router and each switch.

a. Configure host names as shown in the topology.

b. Configure interface IP addresses as shown in the IP Addressing Table. The configuration of the VLAN 1 management interface on switch S1 is shown here.

```
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.1.2 255.255.255.0
S1(config-if)#no shutdown
```

c. Configure the enable secret and console passwords.

```
S1(config)#enable secret cisco12345
S1(config)#line console 0
S1(config-line)#password ciscoconpass
S1(config-line)#exec-timeout 5 0
S1(config-line)#login
S1(config-line)#logging synchronous
```

Note: Do not configure the switch vty access at this time. The vty lines are configured on the switches in Part 2 for SSH access.

d. Configure the vty lines and password on R1.

```
R1(config)#line vty 0 4
R1(config-line)#password ciscovtypass
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
```

e. To prevent the router or switch from attempting to translate incorrectly entered commands, disable DNS lookup. Router R1 is shown here as an example.

```
R1(config)#no ip domain-lookup
```

f. HTTP access to the switch is enabled by default. To prevent HTTP access, disable the HTTP server and HTTP secure server.

```
S1(config)#no ip http server
S1(config)#no ip http secure-server
```

Note: The switch must have a cryptography IOS image to support the **ip http secure-server** command. HTTP access to the router is disabled by default.

Step 3: Configure PC host IP settings.

Configure a static IP address, subnet mask, and default gateway for PC-A and PC-B as shown in the IP Addressing Table.

Step 4: Verify basic network connectivity.

a. Ping from PC-A and PC-B to the R1 Fa0/1 interface at IP address 192.168.1.1. Were the results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

b. Ping from PC-A to PC-B. Were the results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Step 5: Save the basic configurations for the router and both switches.

Save the running configuration to the startup configuration from the privileged EXEC prompt.

```
S1#copy running-config startup-config
```

Part 2. SSH Configuration

In Part 2 of this lab, you configure switches S1 and S2 to support SSH connections and install SSH client software on the PCs.

Note: A switch IOS image that supports encryption is required to configure SSH. Otherwise, you cannot specify SSH as an input protocol for the vty lines and the **crypto** commands are not available.

Task 1. Configure the SSH Server on Switch S1 and S2 Using the CLI

In this task, use the CLI to configure the switch to be managed securely using SSH instead of Telnet. Secure Shell (SSH) is a network protocol that establishes a secure terminal emulation connection to a switch or other networking device. SSH encrypts all information that passes over the network link and provides authentication of the remote computer. SSH is rapidly replacing Telnet as the remote login tool of choice for network professionals.

Note: For a switch to support SSH, it must be configured with local authentication, AAA services or username. In this task, you configure an SSH username and local authentication on S1 and S2. S1 is shown here as an example.

Step 1: Configure a domain name.

Enter global configuration mode and set the domain name.

```
S1#conf t
S1(config)#ip domain-name ccnasecurity.com
```

Step 2: Configure a privileged user for login from the SSH client.

Use the **username** command to create the user ID with the highest possible privilege level and a secret password.

```
S1(config)#username admin privilege 15 secret cisco12345
```

Exit to the initial switch login screen, and log in with this username. What was the switch prompt after you entered the password? _____

Step 3: Configure the incoming vty lines.

a. Configure vty access on lines 0 through 4. Specify a privilege level of 15 so that a user with the highest privilege level (15) will default to privileged EXEC mode when accessing the vty lines. Other users will default to user EXEC mode. Specify the use of local user accounts for mandatory login and validation, and accept only SSH connections.

```
S1(config)#line vty 0 4
S1(config-line)#privilege level 15
S1(config-line)#exec-timeout 5 0
S1(config-line)#login local
S1(config-line)#transport input ssh
S1(config-line)#exit
```

b. Disable login for switch vty lines 5 through 15.

```
S1(config)#line vty 5 15
S1(config-line)#no login
```

Step 4: Generate the RSA encryption key pair for the router.

The switch uses the RSA key pair for authentication and encryption of transmitted SSH data.

Configure the RSA keys with 1024 for the number of modulus bits. The default is 512, and the range is from 360 to 2048.

```
S1(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: S1.ccnasecurity.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

S1(config)#
00:15:36: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Note: The details of encryption methods are covered in Chapter 7.

Step 5: Verify the SSH configuration.

Use the **show ip ssh** command to see the current settings.

```
S1#show ip ssh
```

Fill in the following information based on the output of the **show ip ssh** command.

SSH version enabled: _____
Authentication timeout: _____
Authentication retries: _____

Step 6: Configure SSH timeouts and authentication parameters.

The default SSH timeouts and authentication parameters can be altered to be more restrictive using the following commands.

```
S1(config)#ip ssh time-out 90
S1(config)#ip ssh authentication-retries 2
```

Step 7: Save the running-config to the startup-config.

```
S1#copy running-config startup-config
```

Task 2. Configure the SSH Client

TeraTerm and PuTTY are two terminal emulation programs that can support SSHv2 client connections. This lab uses PuTTY.

Step 1: (Optional) Download and install an SSH client on PC-A and PC-B.

If the SSH client is not already installed, download either TeraTerm or PuTTY.

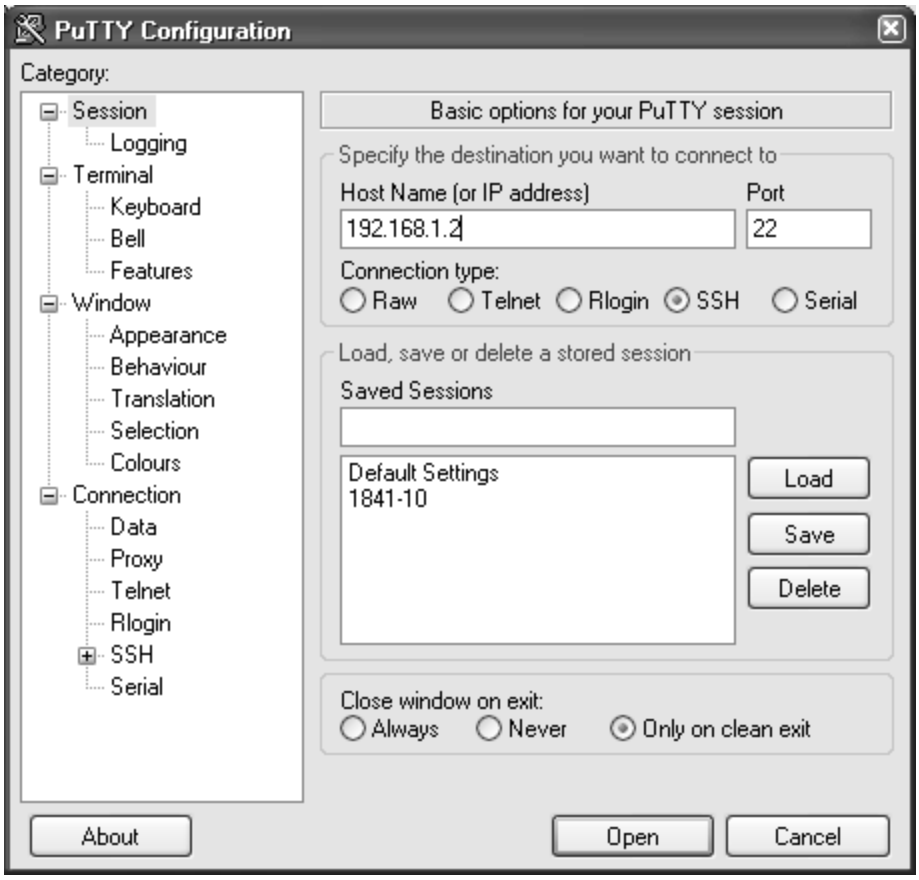
Note: The procedure described here is for PuTTY and pertains to PC-A.

Step 2: Verify SSH connectivity to S1 from PC-A.

a. Launch PuTTY by double-clicking the putty.exe icon.

b. Input the S1 IP address 192.168.1.2 in the **Host Name or IP address** field.

c. Verify that the **SSH** radio button is selected. PuTTY defaults to SSH version 2.



d. Click **Open**.

e. In the PuTTY Security Alert window, click **Yes**.

f. Enter the **admin** username and password **cisco12345** in the PuTTY window.

g. At the S1 privileged EXEC prompt, enter the **show users** command.

```
S1#show users
```

What users are connected to switch S1 at this time?

_____

h. Close the PuTTy SSH session window with the **exit** or **quit** command.

i. Try to open a Telnet session to switch S1 from PC-A. Were you able to open the Telnet session? Why or why not? _____

Step 3: Save the configuration.

Save the running configuration to the startup configuration from the privileged EXEC prompt.

```
R1#copy running-config startup-config
```

Part 3. Secure Trunks and Access Ports

In Part 3 of this lab, you configure trunk ports, change the native VLAN for trunk ports, verify trunk configuration, and enable storm control for broadcasts on the trunk ports.

Securing trunk ports can help stop VLAN hopping attacks. The best way to prevent a basic VLAN hopping attack is to turn off trunking on all ports except the ones that specifically require trunking. On the required trunking ports, disable DTP (auto trunking) negotiations and manually enable trunking. If no trunking is required on an interface, configure the port as an access port. This disables trunking on the interface.

Note: Tasks should be performed on switches S1 or S2 as indicated.

Task 1. Secure Trunk Ports

Step 1: Configure switch S1 as the root switch.

For the purposes of this lab, assume that switch S2 is currently the root bridge and that switch S1 is preferred as the root switch. To force S1 to become the new root bridge, you configure a new priority for it.

a. From the console on S1, enter privileged EXEC mode and then global configuration mode.

The default priority for switches S1 and S2 is 32769 (32768 + 1 with System ID Extension). Set S1 priority to 0 so that it becomes the root switch.

```
S1(config)#spanning-tree vlan 1 priority 0
S1(config)#exit
```

b. Issue the **show spanning-tree** command to verify that S1 is the root bridge and to see the ports in use and their status.

```
S1#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    1
              Address     001d.4635.0c80
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    1      (priority 0 sys-id-ext 1)
              Address     001d.4635.0c80
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/5            Desg FWD 19        128.5    P2p
Fa0/6            Desg FWD 19        128.6    P2p
```

c. What is the S1 priority? _____

d. What ports are in use and what is their status? _____

Step 2: Configure trunk ports on S1 and S2.

a. Configure port Fa0/1 on S1 as a trunk port.

```
S1(config)#interface FastEthernet 0/1
S1(config-if)#switchport mode trunk
```

b. Configure port Fa0/1 on S2 as a trunk port.

```
S2(config)#interface FastEthernet 0/1
S2(config-if)#switchport mode trunk
```

c. Verify that S1 port Fa0/1 is in trunking mode with the **show interfaces trunk** command.

```
S1#show interfaces trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1
```

Step 3: Change the native VLAN for the trunk ports on S1 and S2.

Changing the native VLAN for trunk ports to an unused VLAN helps prevent VLAN hopping attacks.

a. From the output of the **show interfaces trunk** in the previous step, what is the current native VLAN for the S1 Fa0/1 trunk interface? _____

b. Set the native VLAN on the S1 Fa0/1 trunk interface to an unused VLAN 99.

```
S1(config)#interface Fa0/1
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#end
```

The following message should be displayed after a brief period of time.

```
02:16:28: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered
on FastEthernet0/1 (99), with S2 FastEthernet0/1 (1).
```

What does the message mean? _____

c. Set the native VLAN on the S2 Fa0/1 trunk interface to VLAN 99.

```
S2(config)#interface Fa0/1
S2(config-if)#switchport trunk native vlan 99
S2(config-if)#end
```

Step 4: Prevent the use of DTP on S1 and S2.

Setting the trunk port to not negotiate also helps to mitigate VLAN hopping by turning off the generation of DTP frames.

```
S1(config)#interface Fa0/1
S1(config-if)#switchport nonegotiate

S2(config)#interface Fa0/1
S2(config-if)#switchport nonegotiate
```

Step 5: Verify the trunking configuration on port Fa0/1.

```
S1#show interface fa0/1 trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1

S1#show interface fa0/1 switchport

Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (Inactive)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Step 6: Enable storm control for broadcasts.

Enable storm control for broadcasts on the trunk port with a 50 percent rising suppression level using the **storm-control broadcast** command.

```
S1(config)#interface FastEthernet 0/1
S1(config-if)#storm-control broadcast level 50

S2(config)#interface FastEthernet 0/1
S2(config-if)#storm-control broadcast level 50
```

Step 7: Verify your configuration with the show run command.

Use the **show run** command to display the running configuration, beginning with the first line that has the text string “0/1” in it.

```
S1#show run | beg 0/1
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
 switchport nonegotiate
 storm-control broadcast level 50.00

<Output omitted>
```

Task 2. Secure Access Ports

By manipulating the STP root bridge parameters, network attackers hope to spoof their system, or a rogue switch that they add to the network, as the root bridge in the topology. If a port that is configured with PortFast receives a BPDU, STP can put the port into the blocking state by using a feature called BPDU guard.

Step 1: Disable trunking on S1 access ports.

On S1, configure Fa0/5, the port to which R1 is connected, as access mode only.

```
S1(config)#interface FastEthernet 0/5
S1(config-if)#switchport mode access
```

On S1, configure Fa0/6, the port to which PC-A is connected, as access mode only.

```
S1(config)#interface FastEthernet 0/6
S1(config-if)#switchport mode access
```

On S2, configure Fa0/18, the port to which PC-B is connected, as access mode only.

```
S2(config)#interface FastEthernet 0/18
S2(config-if)#switchport mode access
```

Task 3. Protect Against STP Attacks

The topology has only two switches and no redundant paths, but STP is still active. In this step, you enable some switch security features that can help reduce the possibility of an attacker manipulating switches via STP-related methods.

Step 1: Enable PortFast on S1 and S2 access ports.

PortFast is configured on access ports that connect to a single workstation or server to enable them to become active more quickly.

a. Enable PortFast on the S1 Fa0/5 access port.

```
S1(config)#interface FastEthernet 0/5
S1(config-if)#spanning-tree portfast
```

The following Cisco IOS warning message is displayed:

```
%Warning: portfast should only be enabled on ports connected to a
single host. Connecting hubs, concentrators, switches, bridges, etc...
to this interface when portfast is enabled, can cause temporary
bridging loops. Use with CAUTION

%Portfast has been configured on FastEthernet0/5 but will only
 have effect when the interface is in a non-trunking mode.
```

b. Enable PortFast on the S1 Fa0/6 access port.

```
S1(config)#interface FastEthernet 0/6
S1(config-if)#spanning-tree portfast
```

c. Enable PortFast on the S2 Fa0/18 access ports

```
S2(config)#interface FastEthernet 0/18
S2(config-if)#spanning-tree portfast
```

Step 2: Enable BPDU guard on the S1 and S2 access ports.

BPDU guard is a feature that can help prevent rogue switches and spoofing on access ports.

a. Enable BPDU guard on the switch ports previously configured as access only.

```
S1(config)#interface FastEthernet 0/5
S1(config-if)#spanning-tree bpduguard enable

S1(config)#interface FastEthernet 0/6
S1(config-if)#spanning-tree bpduguard enable

S2(config)#interface FastEthernet 0/18
S2(config-if)#spanning-tree bpduguard enable
```

b. PortFast and BPDU guard can also be enabled globally with the **spanning-tree portfast default** and **spanning-tree portfast bpduguard** commands in global configuration mode.

Note: BPDU guard can be enabled on all access ports that have PortFast enabled. These ports should never receive a BPDU. BPDU guard is best deployed on user-facing ports to prevent rogue switch network extensions by an attacker. If a port enabled with BPDU guard receives a BPDU, it is disabled and must be manually re-enabled. An err-disable timeout can be configured on the port so that it can recover automatically after a specified time period.

c. Verify that BPDU guard is configured by using the **show spanning-tree interface fa0/5 detail** command on switch S1.

```
S1#show spanning-tree interface fa0/5 detail

Port 5 (FastEthernet0/5) of VLAN0001 is designated forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.5.
   Designated root has priority 1, address 001d.4635.0c80
   Designated bridge has priority 1, address 001d.4635.0c80
   Designated port id is 128.5, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
```

```
The port is in the portfast mode
Link type is point-to-point by default
Bpdu guard is enabled
BPDU: sent 3349, received 0
```

Step 3: (Optional) Enable root guard.

Root guard is another option in helping to prevent rogue switches and spoofing. Root guard can be enabled on all ports on a switch that are not root ports. It is normally enabled only on ports connecting to edge switches where a superior BPDU should never be received. Each switch should have only one root port, which is the best path to the root switch.

The following command configures root guard on S2 interface Gi0/1. Normally, this is done if another switch is attached to this port. Root guard is best deployed on ports that connect to switches that should not be the root bridge.

```
S2(config)#interface gigabitEthernet 0/1
S2(config-if)#spanning-tree guard root
```

a. Issue the **show run** command to verify that root guard is configured.

```
S2#sh run | beg Gig
interface GigabitEthernet0/1
 spanning-tree guard root
```

Note: The S2 Gi0/1 port is not currently up, so it is not participating in STP. Otherwise, you could use the **show spanning-tree interface Gi0/1 detail** command.

b. If a port that is enabled with BPDU guard receives a superior BPDU, it goes into a root-inconsistent state. Use the **show spanning-tree inconsistentports** command to determine if there are any ports currently receiving superior BPDUs that should not be.

```
S2#show spanning-tree inconsistentports

Name                 Interface              Inconsistency
-------------------- ---------------------- ------------------
Number of inconsistent ports (segments) in the system : 0
```

Note: Root guard allows a connected switch to participate in STP as long as the device does not try to become the root. If root guard blocks the port, subsequent recovery is automatic. If the superior BPDUs stop, the port returns to the forwarding state.

Task 4. Configure Port Security and Disable Unused Ports

Switches can also be subject to CAM table overflow, MAC spoofing attacks, and unauthorized connections to switch ports. In this task, you configure port security to limit the number of MAC addresses that can be learned on a switch port and disable the port if that number is exceeded.

Step 1: Record the R1 Fa0/0 MAC address.

a. From the router R1 CLI, use the **show interface** command and record the MAC address of the interface.

```
R1#show interface fa0/1

FastEthernet0/1 is up, line protocol is up
  Hardware is Gt96k FE, address is 001b.5325.256f (bia 001b.5325.256f)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
```

```
   reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s, 100BaseTX/FX
```

b. What is the MAC address of the R1 Fa0/1 interface? _____

Step 2: Configure basic port security.

This procedure should be performed on all access ports that are in use. Switch S1 port Fa0/5 is shown here as an example.

Note: A switch port must be configured as an access port to enable port security.

a. From the switch S1 CLI, enter interface configuration mode for the port that connects to the router (Fast Ethernet 0/5).

```
S1(config)#interface FastEthernet 0/5
```

b. Shut down the switch port.

```
S1(config-if)#shutdown
```

c. Enable port security on the port.

```
S1(config-if)#switchport port-security
```

Note: Entering just the **switchport port-security** command sets the maximum MAC addresses to 1 and the violation action to shutdown. The **switchport port-security maximum** and **switchport port-security violation** commands can be used to change the default behavior.

d. Configure a static entry for the MAC address of R1 Fa0/1/ interface recorded in Step 1.

```
S1(config-if)#switchport port-security mac-address xxxx.xxxx.xxxx
```

(*xxxx.xxxx.xxxx* is the actual MAC address of the router Fast Ethernet 0/1 interface.)

Note: Optionally, you can use the **switchport port-security mac-address sticky** command to add all the secure MAC addresses that are dynamically learned on a port (up to the maximum set) to the switch running configuration.

e. Bring up the switch port.

```
S1(config-if)#no shutdown
```

Step 3: Verify port security on S1 Fa0/5.

On S1, issue the **show port-security** command to verify that port security has been configured on S1 Fa0/5.

```
S1#show port-security interface f0/5
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
```

```
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 001b.5325.256f:1
Security Violation Count   : 0
```

What is the status of the Fa0/5 port? _____

What is the Last Source Address and VLAN? _____

From the router R1 CLI, ping PC-A to verify connectivity. This also ensures that the R1 Fa0/1 MAC address is learned by the switch.

```
R1#ping 192.168.1.10
```

You will now violate security by changing the MAC address on the router interface. Enter interface configuration mode for the Fast Ethernet 0/1 interface and shut it down.

```
R1(config)#interface FastEthernet 0/1
R1(config-if)#shutdown
```

Configure a MAC address for the interface on the interface, using aaaa.bbbb.cccc as the address.

```
R1(config-if)#mac-address aaaa.bbbb.cccc
```

Enable the Fast Ethernet 0/1 interface.

```
R1(config-if)#no shutdown
R1(config-if)#end
```

From the router R1 CLI, ping PC-A. Was the ping successful? Why or why not?

_____

On switch S1 console, observe the messages when port Fa0/5 detects the violating MAC address.

```
*Jan 14 01:34:39.750: %PM-4-ERR_DISABLE: psecure-violation error
detected on Fa0/5, putting Fa0/5 in err-disable state
*Jan 14 01:34:39.750: %PORT_SECURITY-2-PSECURE_VIOLATION: Security
violation occurred, caused by MAC address aaaa.bbbb.cccc on port
FastEthernet0/5.
*Jan 14 01:34:40.756: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/5, changed state to down
*Mar  1 01:34:41.755: %LINK-3-UPDOWN: Interface FastEthernet0/5,
changed state to down
```

On the switch, use the various **show port-security** commands to verify that port security has been violated.

```
S1#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
      Fa0/5            1           1                1         Shutdown
```

```
S1#show port-security interface fastethernet0/5
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
```

```
Last Source Address:Vlan   : aaaa.bbbb.cccc:1
Security Violation Count   : 1

S1#show port-security address
          Secure Mac Address Table
```

Vlan	Mac Address	Type	Ports	Remaining Age (mins)
1	001b.5325.256f	SecureConfigured	Fa0/5	-

On the router, shut down the Fast Ethernet 0/1 interface, remove the hard-coded MAC address from the router, and re-enable the Fast Ethernet 0/1 interface.

```
R1(config)#interface FastEthernet 0/1
R1(config-if)#shutdown
R1(config-if)#no mac-address aaaa.bbbb.cccc
R1(config-if)#no shutdown
```

Note: This will restore the original FastEthernet interface MAC address.

From R1, try to ping the PC-A again at 192.168.1.10. Was the ping successful? Why or why not?

_____

Step 4: Clear the S1 Fa0/5 error disabled status.

a. From the S1 console, clear the error and re-enable the port using the following commands. This will change the port status from Secure-shutdown to Secure-up.

```
S1(config)#interface FastEthernet 0/5
S1(config-if)#shutdown
S1(config-if)#no shutdown
```

Note: This assumes the device/interface with the violating MAC address has been removed and replaced with the one originally configured.

b. From R1, ping PC-A again. You should be successful this time.

```
R1#ping 192.168.1.10
```

Step 5: Remove basic port security on S1 Fa0/5.

a. From the S1 console, remove port security on Fa0/5. This procedure can also be used to re-enable the port but port security commands will need to be reconfigured.

```
S1(config)#interface FastEthernet 0/5
S1(config-if)#shutdown
S1(config-if)#no switchport port-security
S1(config-if)#no switchport port-security mac-address 001b.5325.256f
S1(config-if)#no shutdown
```

b. You can also use the following commands to reset the interface to its default settings.

```
S1(config)#interface FastEthernet 0/5
S1(config-if)#shutdown
S1(config-if)#exit
S1(config)#default interface fastethernet 0/5
S1(config)#interface FastEthernet 0/5
S1(config-if)#no shutdown
```

Note: This **default interface** command also requires you to reconfigure the port as an access port in order to re-enable the security commands.

Step 6: (Optional) Configure port security for VoIP.

The following example shows a typical port security configuration for a voice port. Two MAC addresses are allowed, and they are to be learned dynamically. One MAC address is for the IP phone, and the other IP address is for the PC connected to the IP phone. Violations of this policy result in the port being shut down. The aging timeout for the learned MAC addresses is set to two hours.

This example is shown for switch S2 port Fa0/18.

```
S2(config)#interface Fa0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 2
S2(config-if)#switchport port-security violation shutdown
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#switchport port-security aging time 120
```

Step 7: Disable unused ports on S1 and S2.

As a further security measure, disable any ports not being used on the switch.

a. Ports Fa0/1, Fa0/5, and Fa0/6 are used on switch S1. The remaining Fast Ethernet ports and the two Gigabit Ethernet ports will be shutdown.

```
S1(config)#interface range Fa0/2 – 4
S1(config-if-range)#shutdown
S1(config-if-range)#interface range Fa0/7 – 24
S1(config-if-range)#shutdown
S1(config-if-range)#interface range gigabitethernet0/1 – 2
S1(config-if-range)#shutdown
```

b. Ports Fa0/18 and Gi0/1 are used on switch S2. The remaining Fast Ethernet ports and the Gigabit Ethernet ports will be shutdown.

```
S2(config)#interface range Fa0/2 - 17
S2(config-if-range)#shutdown
S2(config-if-range)#interface range Fa0/19 - 24
S2(config-if-range)#shutdown
S2(config-if-range)#exit
S2(config)#interface gigabitethernet0/2
S2(config-if)#shutdown
```

Step 8: (Optional) Move active ports to a VLAN other than the default VLAN 1

As a further security measure, you can move all active end user and router ports to a VLAN other than the default VLAN 1 on both switches.

a. Configure a new VLAN for users on each switch using the following commands:

```
S1(config)#vlan 20
S1(config-vlan)#name Users

S2(config)#vlan 20
S2(config-vlan)#name Users
```

b. Add the current active access (non-trunk) ports to the new VLAN.

```
S1(config)#interface range fa0/5 - 6
S1(config-if)#switchport access vlan 20

S2(config)#interface fa0/18
S2(config-if)#switchport access vlan 20
```

Note: This will prevent communication between end user hosts and the management VLAN IP address of the switch, which is currently VLAN 1. The switch can still be accessed and configured using the console connection.

If you need to provide Telnet or SSH access to the switch, a specific port can be designated as the management port and added to VLAN 1 with a specific management workstation attached. A more elaborate solution is to create a new VLAN for switch management (or use the existing native trunk VLAN 99) and configure a separate subnet for the management and user VLANs. Enable trunking with subinterfaces on R1 to route between the management and user VLAN subnets.

Part 4. Configure SPAN and Monitor Traffic

Note: There are two tasks in this part of the lab, Task 1: Option 1 is to be performed using hands-on equipment. Task 2: Option 2 is modified to be compatible with the NETLAB+ system but can also be performed using hands-on equipment.

Cisco IOS provides a feature that can be used to monitor network attacks called Switched Port Analyzer (SPAN). Cisco IOS supports local SPAN and remote SPAN (RSPAN). With local SPAN, the source VLANs, source switch ports, and the destination switch ports are on the same physical switch.

In this part of the lab, you configure a local SPAN to copy traffic from one port where a host is connected to another port where a monitoring station is connected. The monitoring station will run the Wireshark packet sniffer application to analyze traffic.

Note: SPAN allows you to select and copy traffic from one or more source switch ports or source VLANs onto one or more destination ports.

Task 1. Option 1: Configure a SPAN Session Using Hands-on Equipment.

Note: Option 1 assumes you have physical access to the devices shown in the topology for this lab. NETLAB+ users accessing lab equipment remotely should proceed to Task 2: Option 2.

Step 1: Configure a SPAN session on S1 with a source and destination

a. Set the SPAN source interface using the **monitor session** command in global configuration mode. The following configures a SPAN source port on FastEthernet 0/5 for ingress and egress traffic. Traffic copied on the source port can be ingress only, egress only or both. Switch S1 port Fa0/5 is connected to router R1, so traffic to (ingress) and from (egress) switch port Fa0/5 to R1 will be monitored.

```
S1(config)#monitor session 1 source interface fa0/5 both
```

Note: You can specify to monitor tx (transmit) or rx (receive) traffic. The keyword **both** includes tx and rx. The source can be a single interface, a range of interfaces, a single VLAN, or a range of VLANs.

b. Set the SPAN destination interface.

```
S1(config)#monitor session 1 destination interface fa0/6
```

All traffic from S1 Fa0/5, where R1 is connected, will be copied to the SPAN destination port Fa0/6, where PC-A with Wireshark is connected.

Note: The destination can be an interface or a range of interfaces.

Step 2: Verify the setup of the SPAN session on S1.

Confirm the SPAN session setup.

```
S1#show monitor session 1

Session 1
---------------------------------
Type                   : Local Session
Source Ports           :
    Both               : Fa0/5
Destination Ports      : Fa0/6
    Encapsulation      : Native

          Ingress      : Disabled
```

Step 3: (Optional) Download and install Wireshark on PC-A.

a. Wireshark is a network protocol analyzer (also called a packet sniffer) that runs with Windows XP and Vista. If Wireshark is not currently available on PC-A, you can download the latest version from http://www.wireshark.org/download.html. This lab uses Wireshark version 1.0.5. The initial Wireshark installation screen is shown here.

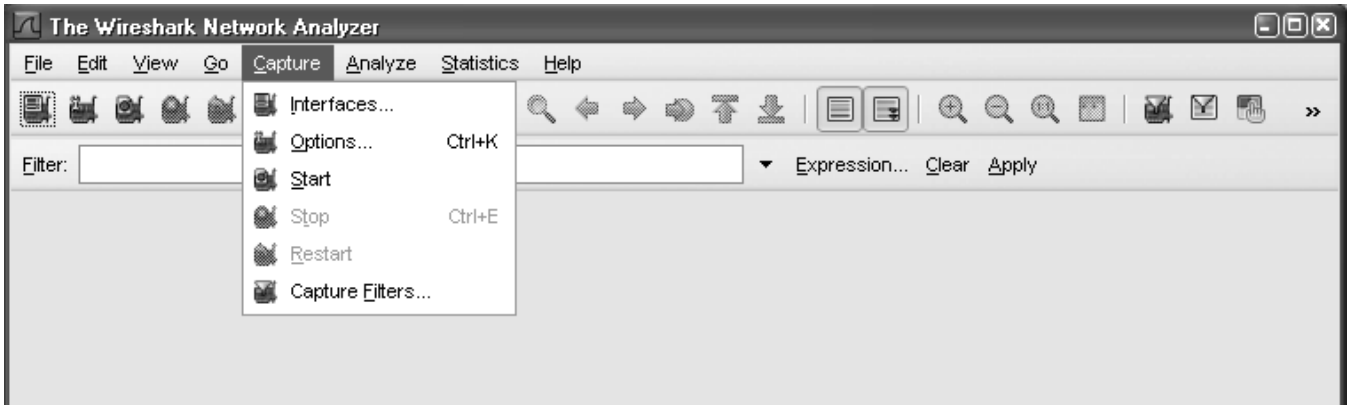
b. Click **I Agree** to the License agreement and accept the defaults by clicking **Next** when prompted.

Note: On the Install WinPcap screen, select the install WinPcap options and select **Start WinPcap service** option if you want to have other users besides those with administrative privileges run Wireshark.

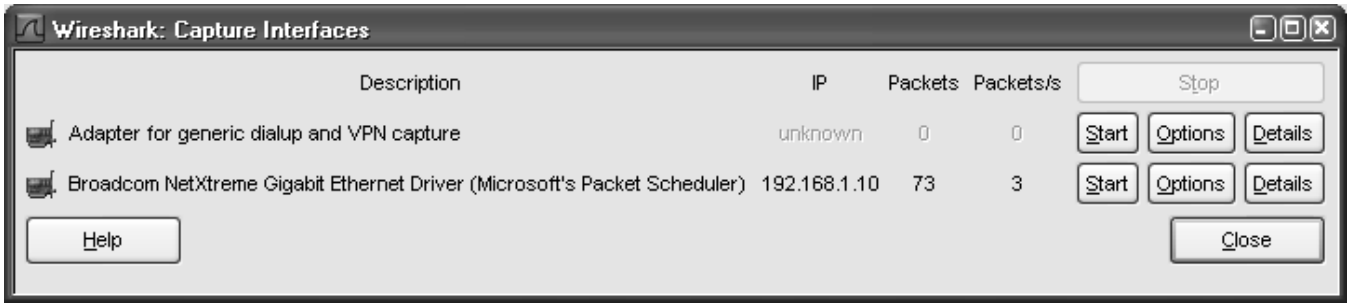
Step 4: Monitor switch S1 port Fa0/5 ping activity using Wireshark on PC-A.

a. If Wireshark is available, start the application.

b. From the main menu, select **Capture > Interfaces**.



c. Click the **Start** button for the local area network interface adapter with IP address 192.168.1.10.

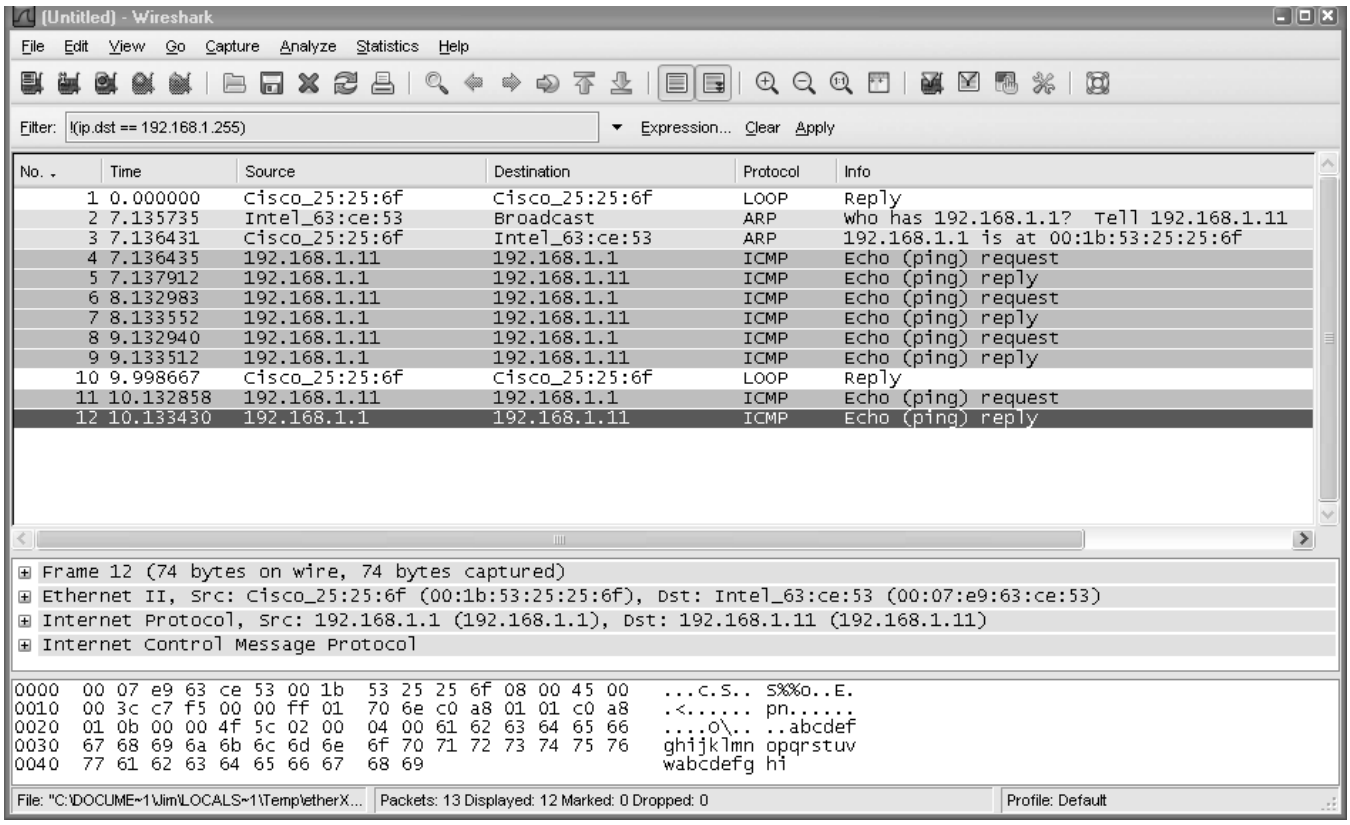


d. Generate some traffic from PC-B (192.168.1.11) to R1 interface Fa0/1 (192.168.1.1) using **ping**. This traffic will go from S2 port Fa0/18 to S2 port Fa0/1 across the trunk link to S1 port Fa0/1 and then exit interface Fa0/5 on S1 to reach R1.

```
PC-B:\>ping 192.168.1.1
```

e. Observe the results in Wireshark on PC-A. Notice the initial ARP request broadcast from PC-B (Intel NIC) to determine the MAC address of the R1 Fa0/1 interface with IP address 192.168.1.1 and the ARP reply from the R1 Cisco Ethernet interface. After the ARP request, the pings (echo request and replies) can be seen going from PC-B to R1 and from R1 to PC-B through the switch.

Note: Your screen should look similar to the one below. Some additional packets might be captured in addition to the pings, such as the R1 Fa0/1 LOOP reply.



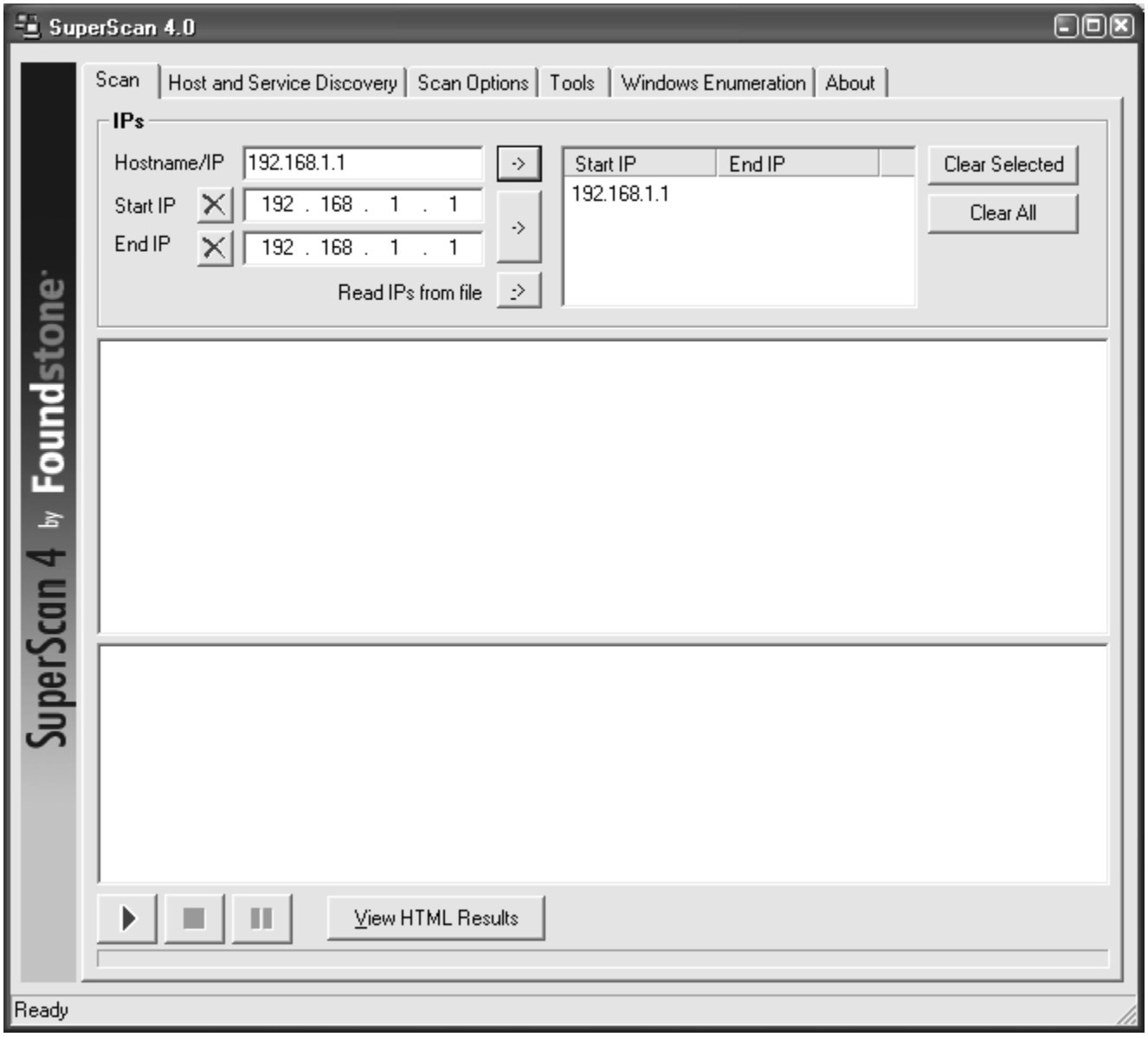
Step 5: Monitor switch S1 port Fa0/5 SuperScan activity using Wireshark on PC-A.

a. If SuperScan is not on PC-B, download the SuperScan 4.0 tool from the Scanning Tools group at http://www.foundstone.com. Unzip the file into a folder. The SuperScan4.exe file is executable and installation is not required.

b. Start the SuperScan program on PC-B. Click the **Host and Service Discovery** tab. Check the **Timestamp Request** check box, and uncheck the **Echo Request** check box. Scroll through the UDP and TCP port selection lists and notice the range of ports that will be scanned.

c. In the SuperScan program, click the **Scan** tab and enter the IP address R1 FA0/1 (192.168.1.1) in the **Hostname/IP** field.

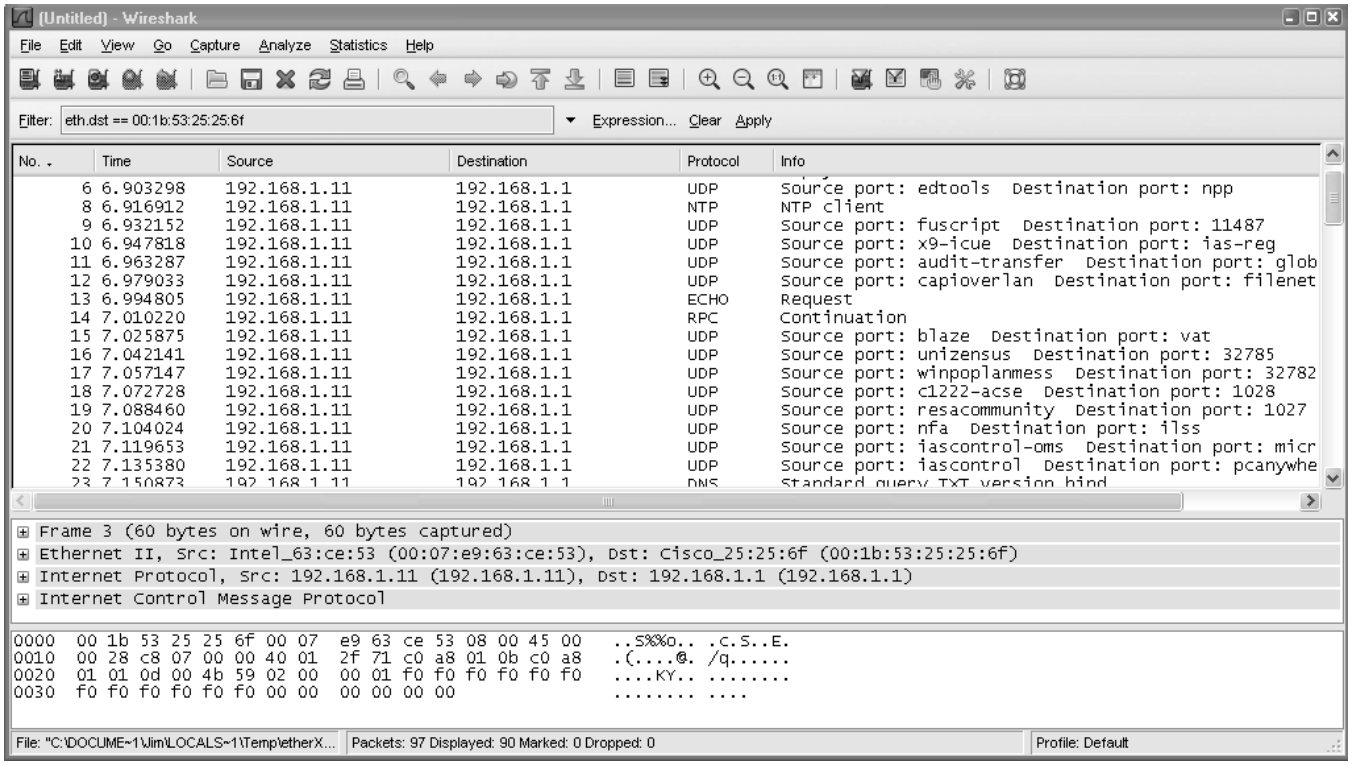
d. Click the right arrow to populate the **Start IP** and **End IP** fields.



e. Clear the previous capture in Wireshark and start a new capture by clicking **Capture > Start**. When prompted, click the **Continue without saving** button.

f. In the SuperScan program, click the blue arrow button in the lower left to start the scan.

g. Observe the results in the Wireshark window on PC-A. Notice the number and types of ports tried by the simulated SuperScan attack from PC-B (192.168.1.11) to R1 Fa0/1 (192.168.1.1). Your screen should look similar to the following:

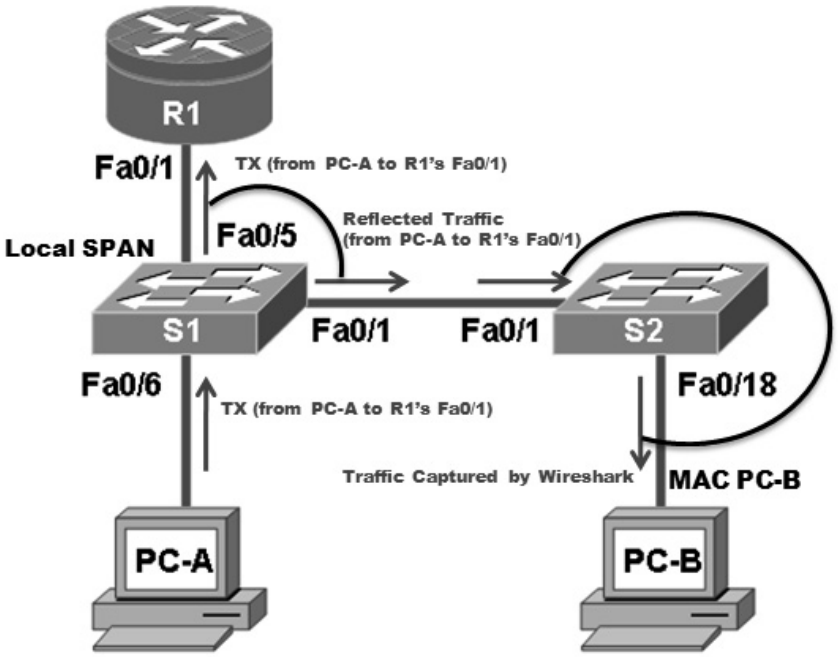


Task 2. Option 2: Configure a SPAN Session Using NETLAB+ Remote Equipment.

Note: This portion of the lab has been rewritten to enhance compatibility with the NETLAB+ system.

On switch S1, you will configure a local SPAN to reflect the traffic exiting Port Fa0/5, in this case, the traffic from PC-A to R1's Fa0/1. This traffic should be received by switch S2, and forwarded to PC-B, where Wireshark is capturing the packets. Refer to the following diagram which illustrates the SPAN traffic flow.

Note: To perform this Task, Wireshark should be installed on PC-B.



Note: Switch S2 is acting as a regular switch, forwarding frames based on destination MAC addresses and switch ports. The traffic entering S2 through Port Fa0/1 utilizes the R1's MAC address as destination for the Ethernet frame, therefore in order to forward those packets to PC-B, the R1's MAC address must be the same as PC-B. To accomplish this, R1's Fa0/1 MAC address is modified using the IOS CLI to simulate PC-B's MAC address. This requirement is specific to the NETLAB+ environment.

Step 1: Configure a SPAN session on S1 with Source and Destination:

a. Return the Fa0/1 on S1 and S2 to its default configuration. This link S1 Fa0/1 to S2 Fa0/1 is going to be used to carry the traffic being monitored.

```
S1(config)#default interface fastethernet 0/1
S2(config)#default interface fastethernet 0/1
```

b. Write down the MAC address for PC-B

PC-B's MAC Address: _____

PC-B's MAC Address in this example is 000c-299a-e61a

c. Configure the PC-B's MAC address on R1's Fa0/1.

```
R1(config)#interface fa0/1
R1(config-if)#mac-address 000c.299a.e61a
```

d. Set the SPAN Source Interface using the monitor session command in global configuration mode. The following configures a SPAN source port on fastethernet0/5 for egress traffic. Traffic copied on the source port can be ingress only, egress only or both. In this case, the egress traffic is the only one analyzed. On Switch S1 port Fa0/5 is connected to router R1 so traffic to the switch port Fa0/5 to R1 will be monitored.

```
S1(config)#monitor session 1 source interface fa0/5 tx
```

Note: The source can be a single interface, a range of interfaces, a single VLAN, or range of VLANs.

e. Set the SPAN destination interface.

```
S1(config)#monitor session 1 destination interface fa0/1
```

All egress traffic from S1 Fa0/5, where R1 is connected, will be copied to the SPAN destination port Fa0/1, where PC-B with WireShark is connected.

Note: The destination can be an interface or a range of interfaces.

Step 2: Verify the setup of the SPAN session on S1.

Confirm the SPAN session setup using the **show monitor session 1** command.

```
S1#show monitor session 1

Session 1
---------
Type                   : Local Session
Source Ports           :
    TX Only            : Fa0/5
Destination Ports      : Fa0/1
    Encapsulation      : Native

          Ingress      : Disabled
```

Step 3: (Optional) Download and install Wireshark on PC-B

WireShark is a network protocol analyzer (also called a packet sniffer) that runs with Windows XP and Vista. If WireShark is not currently available on PC-B, you may download the latest version from http://www.wireshark.org/download.html and install it as described in Part 4, Task 1, Step 3.

Step 4: Monitor Switch S1 port Fa0/5 ping activity using Wireshark on PC-B

a. If WireShark is available, start the application.

b. From the main menu, select **Capture > Interfaces**.

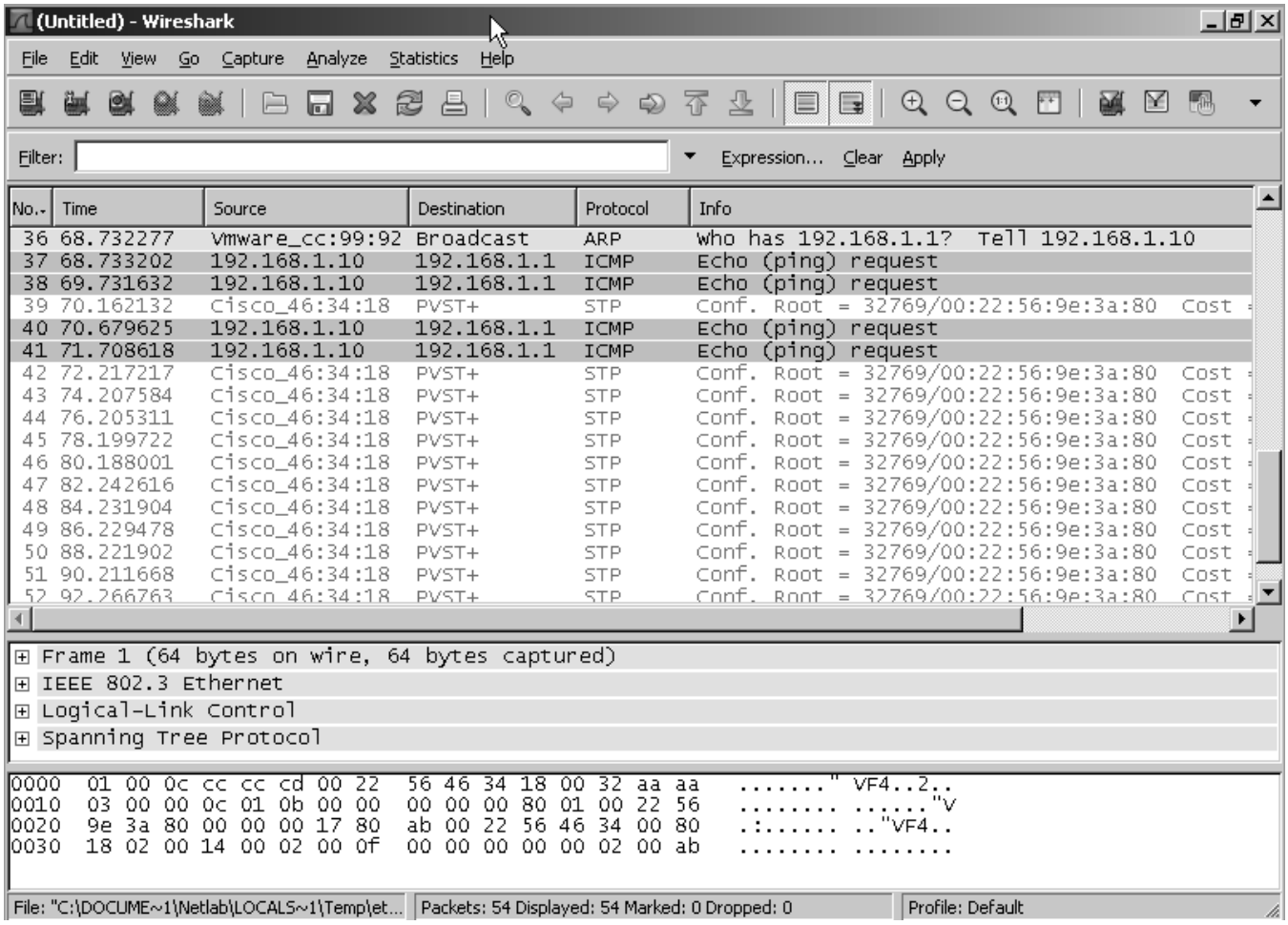
c. Click the **Start** button for the Local area network interface adapter.

d. Generate some traffic from PC-A (192.168.1.10) to R1 interface Fa0/1 (192.168.1.1) using ping. This traffic will go from S1 port Fa0/6 to S1 port Fa0/5. In addition, the traffic going from PC-A to R1 interface Fa0/1 is forwarded across the link between S1 and S2, and then S2 will forward this traffic to PC-B, where Wireshark is capturing the packets. Before pinging, delete the ARP table on PC-A, so an ARP request would be generated. Note that the SPAN session is configured only on S1, and S2 is operating as a normal switch.

```
C:\>arp –d *
C:\>ping 192.168.1.1
```

e. Observe the results in WireShark on PC-B. Notice the initial ARP request broadcast from PC-A to determine the MAC address of the R1 Fa0/1 interface with IP address 192.168.1.1 and the ARP reply from the R1 Cisco Ethernet interface. After the ARP request the pings (echo requests) can be seen going from PC-A to R1 through the switch.

Note: Your screen should look similar to the one below. There may be some addition packets captured, in addition to the pings, such as the R1 Fa0/1 LOOP Reply and Spanning Tree Packets.



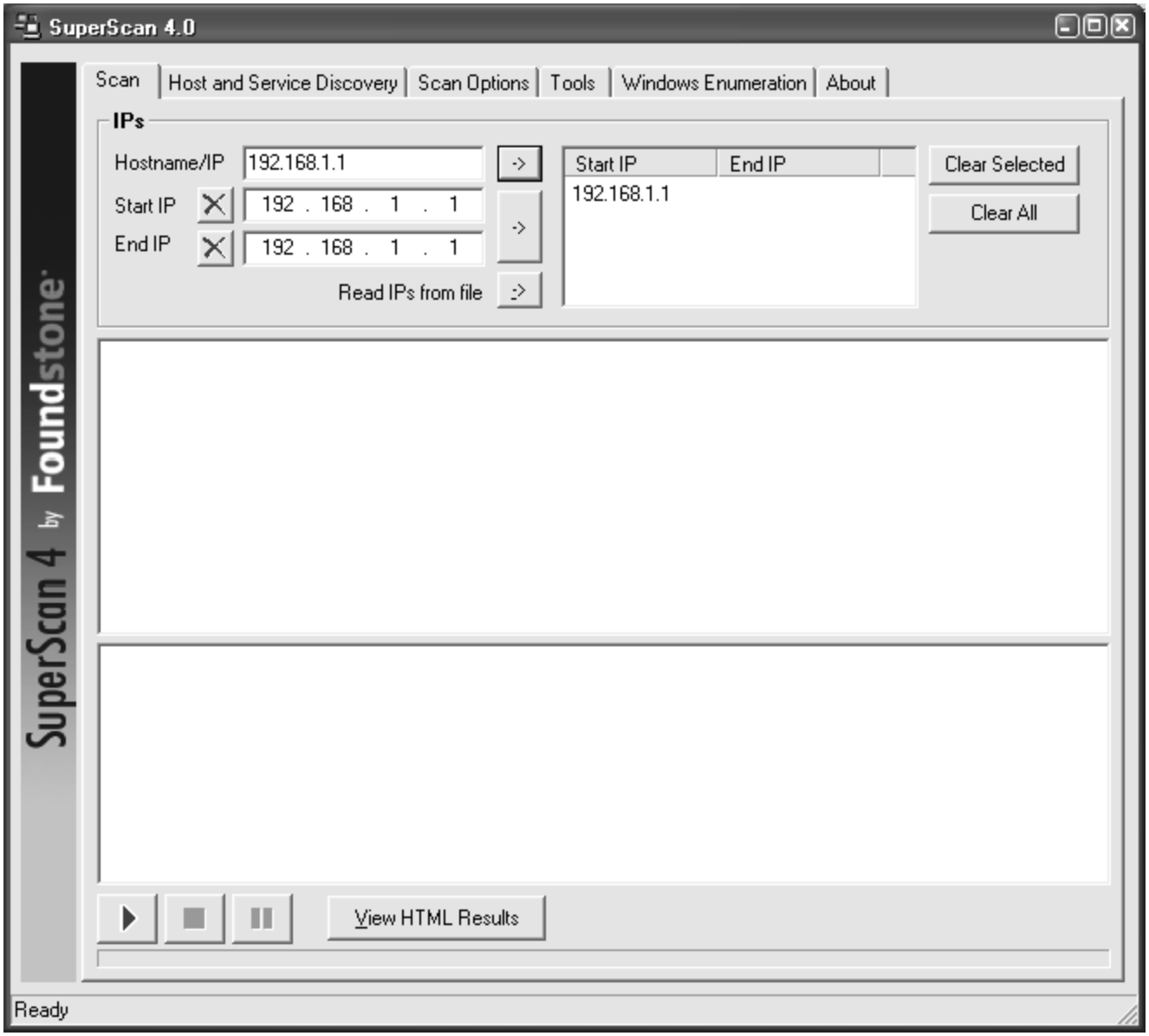
Step 5: Monitor Switch S1 port Fa0/5 SuperScan activity using Wireshark on PC-B

a. If SuperScan is not on PC-A, download the SuperScan 4.0 tool from the Scanning Tools group at http://www.foundstone.com. Unzip the file into a folder. The SuperScan4.exe file is executable and installation is not required.

b. Start the SuperScan program on PC-A. Click the **Host and Service Discovery** tab. Check the **Timestamp Request** check box and uncheck the **Echo Request** check box. Scroll the UDP and TCP port selection lists and notice the range of ports that will be scanned.

c. In the SuperScan program click the **Scan** tab and enter the IP address of R1 FA0/1 (192.168.1.1) in the **Hostname/IP** field.

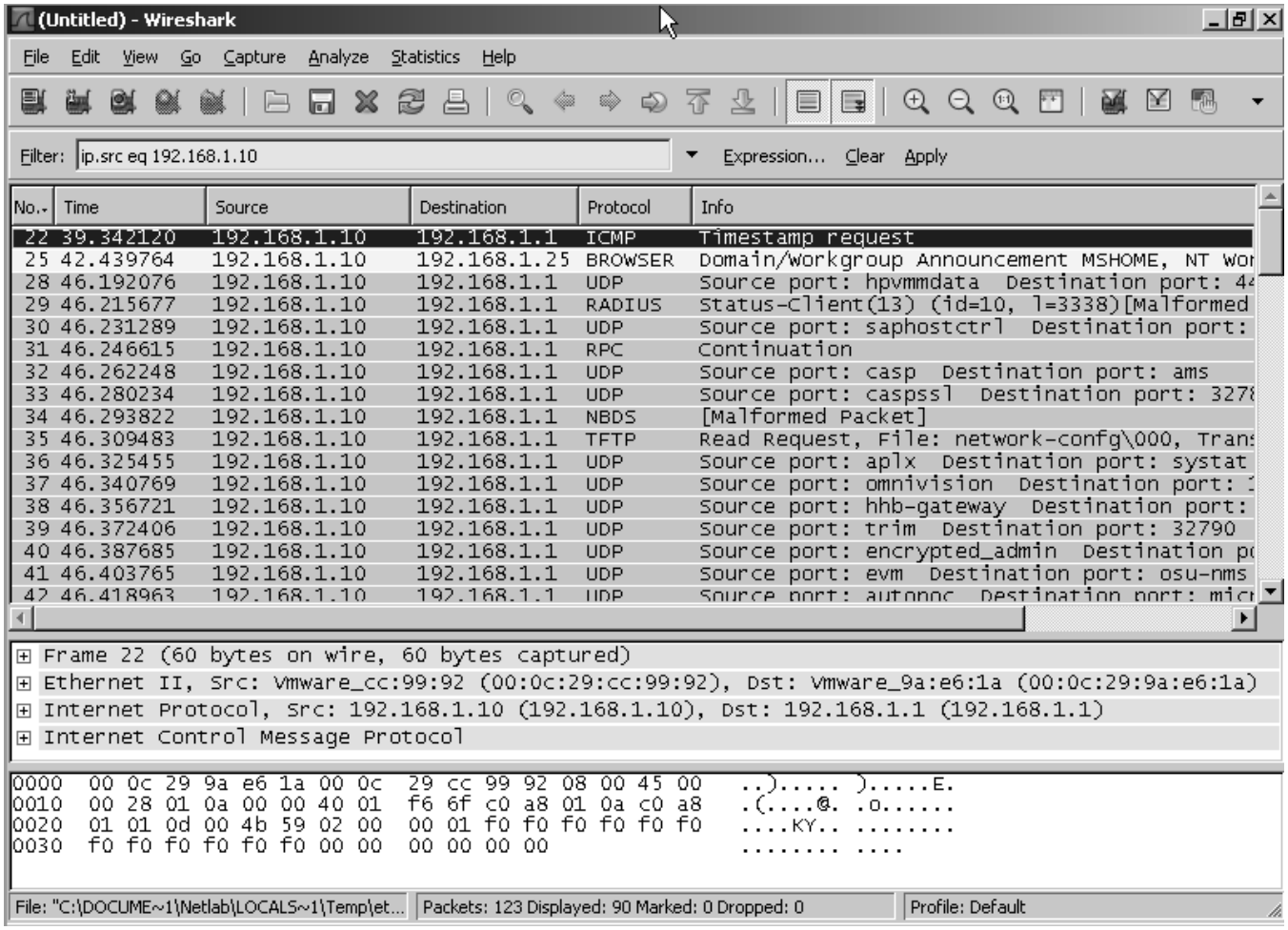
d. Click the right facing arrow to populate the Start and End IP fields.



e. Clear the previous capture in WireShark and start a new capture by clicking **Capture > Start** and when prompted click the **Continue without saving** button.

f. In the SuperScan program click the button which is in the lower left of the screen, with the blue arrow on it, to start the scan.

g. Observe the results on the WireShark window on PC-B. Notice the number and types of ports tried by the simulated SuperScan attack from PC-A (192.168.1.11) to R1 Fa0/1 (192.168.1.1). Your screen should look similar the following:



Step 6: Reflection.

a. Why should port security be enabled on switch access ports?

_____

_____

b. Why should port security be enabled on switch trunk ports?

_____

_____

c. Why should unused ports on a switch be disabled?

_____

_____

Router Interface Summary Table

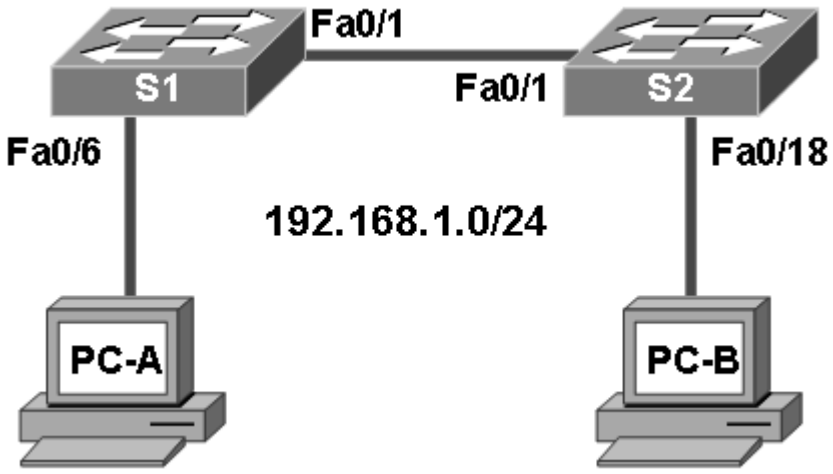
Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1700	Fast Ethernet 0 (FA0)	Fast Ethernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)

Router Interface Summary				
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2600	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
2800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Chapter 7: Lab A: Exploring Encryption Methods

Topology



Objectives

Part 1: (Optional) Build the Network and Configure the PCs

- Connect the PCs and configure IP addresses.

Part 2: Decipher a Pre-encrypted Message Using the Vigenere Cipher

- Given an encrypted message, a cipher key, and the Vigenere cipher square, decipher the message.

Part 3: Create a Vigenere Cipher Encrypted Message and Decrypt It

- Work with a lab partner and agree on a secret password.
- Create a secret message using the Vigenere cipher and the key.
- Exchange messages and decipher them using the pre-shared key.
- Use an interactive Vigenere decoding tool to verify decryption.

Part 4: Use Steganography to Embed a Secret Message in a Graphic7

- Create a secret message and save it as a .txt file.
- Use S-Tools to embed the secret text message into a .bmp graphic.
- Send the graphic to a lab partner to reveal the embedded message.

Background

The Cisco IOS password encryption service uses a Cisco-proprietary algorithm that is based on the Vigenere cipher. Vigenere is an example of a common type of cipher mechanism called polyalphabetic substitution. Although not a strong encryption technique, Vigenere serves to illustrate a commonly used encryption and decryption process.

Note: Students can work in teams of two for this lab.

Required Resources

- 2 switches (Cisco 2960 or comparable)
- PC-A (Windows XP or Vista)
- PC-B (Windows XP or Vista)
- Ethernet cables as necessary

Part 1. (Optional) Build the Network and Configure the PCs

In Part 1 of this lab, you connect the PCs and configure IP addresses. This is not required to perform the lab, unless you want to copy files between PCs.

Step 1: Cable the network as shown in the topology.

Attach the devices shown in the topology diagram, and cable as necessary.

Note: The switches in the topology can be omitted and the PCs connected directly together using a crossover cable, if desired. This is only necessary if the files used in the lab are to be exchanged by copying them from one PC to the other, If files are to be exchanged using removable media, such as a flash drive or floppy disk, no cabling is required.

Step 2: Configure PC host IP settings.

Configure a static IP address and subnet mask for PC-A and PC-B as shown below. A default gateway is not required because the PCs are on the same local network.

- PC-A IP address: 192.168.1.1, Subnet mask 255.255.255.0
- PC-B IP address: 192.168.1.2, Subnet mask 255.255.255.0

Step 3: Verify connectivity between PC-A and PC-B.

Ping from PC-A to PC-B.

Are the ping results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Part 2. Decipher a Pre-encrypted Message Using the Vigenere Cipher

In Part 2 of this lab, you analyze an encrypted message and decrypt it using a cipher key and the Vigenere cipher square.

Step 1: Review the encrypted message.

The following message has been encrypted using the Vigenere cipher.

VECIHXEJZXMA

Can you tell what the message says? _____

Step 2: Review the cipher keyword.

The cipher keyword **TCPIP** was used to encrypt the message. The same keyword will be used to decrypt or decipher the message.

Step 3: Review the structure of the Vigenere square.

A standard Vigenere square or table is used with the keyword to decipher the message.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Step 4: Decrypt the message using the keyword and Vigenere square.

a. Use the table below to help you decrypt the message. Start by entering the letters of the encrypted message in the second row of cells, from left to right.

b. Enter the keyword TCPIP in the top row, repeating the letters until there is a keyword letter for each letter of the encrypted message, even if the keyword letters at the end do not represent the complete keyword.

c. Refer to the Vigenere square or table shown in Step 3 and find the horizontal row that starts with the first letter of the keyword (the letter T). Scan across that row and locate the first letter of the encrypted message in the row (the letter V). The letter at the top of the column where the encrypted message letter appears is the first letter of the decrypted message (the letter C).

d. Continue this process until you have decrypted the entire message and enter it in the following table.

Cipher Keyword												
Encrypted Message												
Decrypted Message												

Part 3. Create a Vigenere Cipher Encrypted Message and Decrypt It

In Part 3 of this lab, you work with a lab partner and agree on a secret password, referred to as the pre-shared key. Each lab partner creates a secret message using the Vigenere cipher and the key. Partners exchange messages and decipher them using their pre-shared key.

Note: If you do not have a partner, you can perform the steps by yourself.

Step 1: Determine the cipher keyword.

With your partner, establish a cipher keyword and enter it here. _____

Step 2: Create a plain text message and encrypt it (both partners).

Create a plain text (decrypted) message to be encrypted by your partner. _____

You can use the following table to help you encrypt the message. You can enter the unencrypted message and cipher keyword here, but do not let your partner see it.

In the Vigenere table, locate the row that starts with the first letter of the cipher keyword. Next locate the first letter to be encrypted at the top of the column in the table. The point (cell) at which the table row (key letter) and column (message letter) intersect is the first letter of the encrypted message. Continue this process until you have encrypted the entire message.

Note: This table is limited to messages of 12 characters. You can create longer messages if desired. Message encryption and decryption is not case sensitive.

Cipher Keyword												
Encrypted Message												
Decrypted Message												

Step 3: Decrypt the message from your partner.

You can use the following table to help you decrypt your partner's encrypted message. Enter the encrypted message from your partner and the cipher keyword.

Use the same procedure described in Part 2, Step 4.

Note: This table is limited to messages of 12 characters. You can create longer messages if desired.

Cipher Keyword												
Encrypted Message												
Decrypted Message												

Step 4: Use an interactive decryption tool to confirm decryption.

A search for "vigenere decode" on the Internet shows that various cipher encryption and decryption tools are available. Many of these are interactive.

One interactive tool is located at http://sharkysoft.com/misc/vigenere/. Go to this URL. Enter the encrypted message from your partner in the top part of the screen and the cipher key in the middle. Click the **Decode** button to see the clear text version of the message. You can also use this tool to encrypt messages.

The following example shows using Sharky's Vigenere Cipher tool for decoding the encrypted message from Part 1 of the lab.

Part 4. Use Steganography to Embed a Secret Message in a Graphic

In Part 4 of this lab, you create a secret message for your partner, embed it into a graphic file, and then give it to your partner to retrieve it. You embed the message in a graphic file using S-Tools. S-Tools is a steganography tool that hides files in BMP, GIF, and WAV files. You start by opening S-Tools and then drag graphics and sounds into the blank window. To hide files, you drag them into open graphics or sound windows. Data is compressed before being encrypted and then hidden.

Note: The following steps should be performed by both partners, one at PC-A and the other at PC-B. If you do not have a partner, you can perform the steps by yourself.

Step 1: (Optional) Download and install S-Tools.

If the S-Tools application is not installed on the PC, download it from http://www.spychecker.com/program/stools.html or another site and unzip the files to a folder.

Step 2: Create a secret message text file (both partners).

On PC-A or PC-B, open the Windows Notepad application and create a message.

a. Save the message in a folder on the desktop and name it **secret.txt.**

b. Close the Notepad application.

Step 3: Create a simple .bmp graphics file.

Open the Windows Paint application and create a simple graphic. For example, you can write your first name using the pencil tool or text tool and apply some color using the spray can or fill tool.

a. Save the graphic as a .bmp file in a folder on the desktop and name it **graphic.bmp**.

b. Close the Paint application.

Step 4: Create a secret password using the Vigenere cipher.

Choose a passphrase to be encrypted using the Vigenere cipher and record it here. _____ Do not share the passphrase with your partner. This passphrase will be used later to protect the text file when it is embedded in the graphics file.

Choose a cipher keyword to be used when encrypting and decrypting the passphrase and record it here. _____

Encrypt the passphrase using the cipher keyword and the procedure described in Part 3, Step 2. Record the encrypted passphrase here. _____

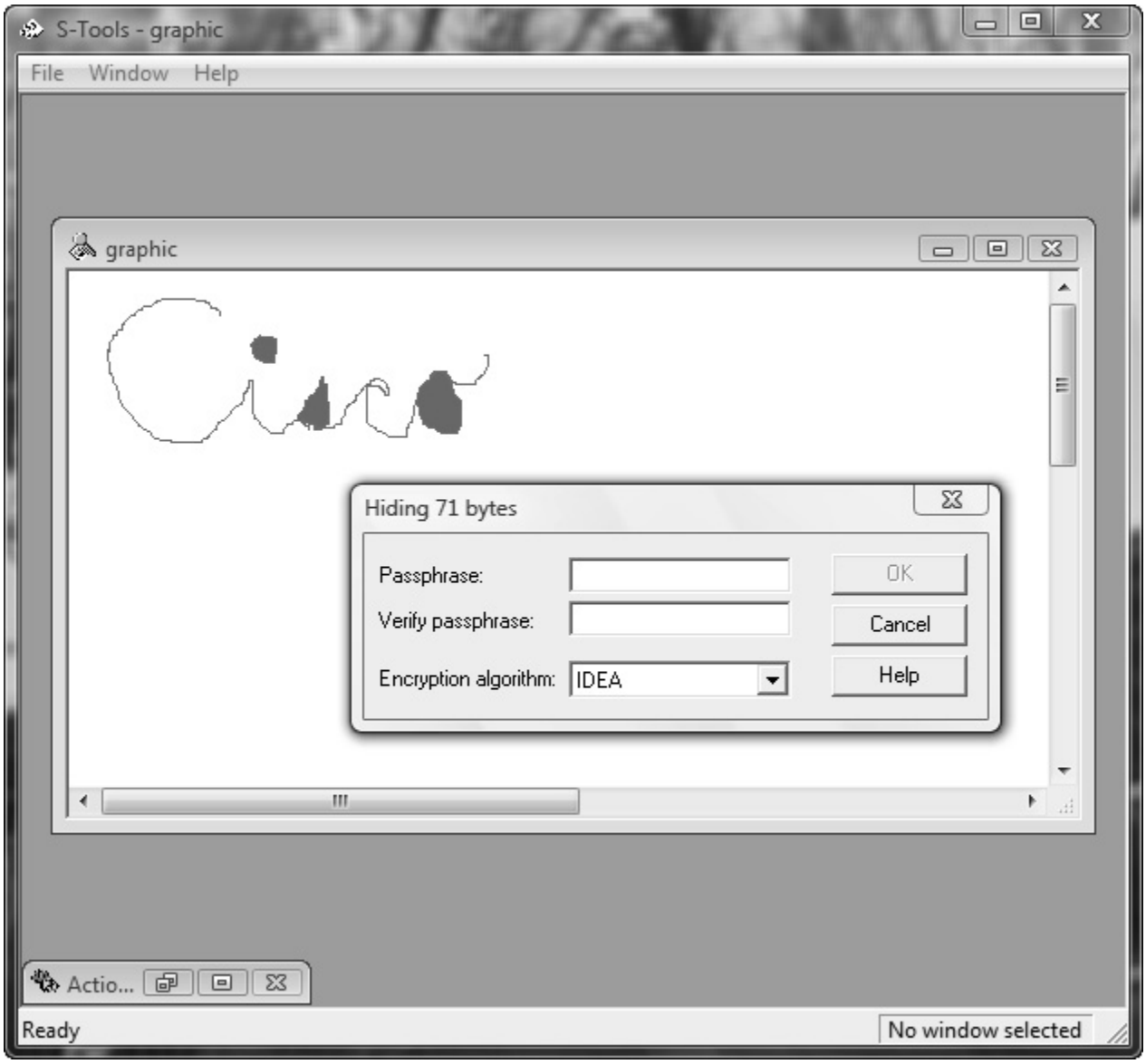
Step 5: Embed the message into a graphic image file.

Open the S-Tools.exe application.

a. Locate the file named **graphic.bmp,** which you saved previously. Determine its size by right-clicking the file and selecting **Properties**. Record the file size, for example 2,359,350 bytes. _____

b. Drag the **graphic.bmp** file into the S-Tools window.

c. Drag the file **secret.txt**, which you created in Step 2, and place it inside the **graphic.bmp** window. The image should still be displayed. A dialog box is displayed showing the number of bytes being hidden. You can enter a passphrase and select the encryption algorithm to be used. The default algorithm is IDEA.



Step 6: Use the unencrypted passphrase to protect the embedded text file.

a. Enter the unencrypted passphrase from Step 4 in the **Passphrase** and **Verify passphrase** fields.

b. Choose **Triple DES** from the **Encryption Algorithm** field and click **OK**. This creates a second image with the name “hidden data”.

c. Right-click the hidden data graphic image and choose **Save As** from the menu. Name the file **graphic2** and save it as a bmp file.

d. Close the S-Tools application.

Step 7: Provide the graphic2.bmp file to your partner.

Provide a copy of your **graphic2.bmp** file to your partner. You can do this by sharing folders (if PCs were cabled together and IP addresses were assigned in Part 1 of the lab). You can also copy the file onto a removable drive (flash drive or floppy disk), or send it as an email attachment if you are performing the lab remotely.

Provide your partner with the Vigenere-encrypted passphrase from Step 4 and the cipher keyword that you used to create it.

Step 8: Decrypt the Vigenere password from your partner.

Decrypt your partner's passphrase using the procedure described in Part 1, Step 4. This is done so that you can use it with S-Tools to reveal the hidden message embedded in your partner's graphic.

Step 9: Reveal the embedded message from your partner.

Open the S-Tools application.

a. Locate the **graphic2.bmp** file from your partner, and determine how large it is using the same method as in Step 5. Record the file size here. _____

b. Has the file size changed? _____

c. Drag the file into the S-Tools window. The image should be displayed. Can you tell that there is a secret message embedded in the graphic image? _____

d. Right-click the image and choose **Reveal** from the menu.

e. Enter the Vigenere passphrase decrypted in Step 8 into the **Passphrase** field.

f. Choose **Triple DES** from the **Encryption Algorithm** field and click **OK**. This displays a revealed archive.

g. Right-click the hidden message file and choose **Save As** from the menu. Name the file **secret2.txt**.

h. Close the S-Tools application.

i. Open the **secret2.txt** file from your partner to reveal the hidden message and write it here.
_____

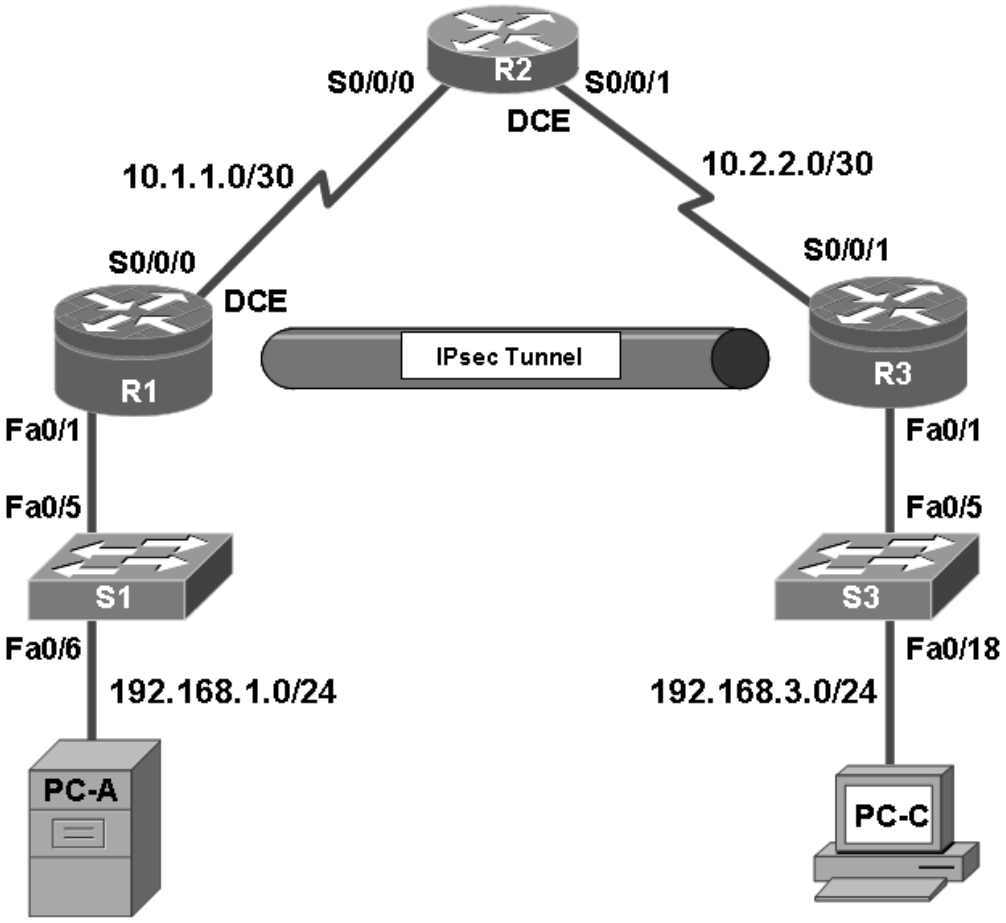
Step 10: Reflection

Could the Vigenere cipher be used to decode messages in the field without a computer?
_____

Do an Internet search for Vigenere cipher cracking tools. Is the Vigenere cipher considered a strong encryption system that is difficult to crack? _____

Chapter 8: Lab A: Configuring a Site-to-Site VPN Using Cisco IOS and SDM

Topology



IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	FA0/1	192.168.1.1	255.255.255.0	N/A	S1 FA0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	FA0/1	192.168.3.1	255.255.255.0	N/A	S3 FA0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 FA0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 FA0/18

Objectives

Part 1: Basic Router Configuration

- Configure host names, interface IP addresses, and access passwords.
- Configure the EIGRP dynamic routing protocol.

Part 2: Configure a Site-to-Site VPN Using Cisco IOS

- Configure IPsec VPN settings on R1 and R3
- Verify site-to-site IPsec VPN configuration
- Test IPsec VPN operation

Part 3: Configure a Site-to-Site VPN Using SDM

- Configure IPsec VPN settings on R1
- Create a mirror configuration for R3
- Apply the mirror configuration to R3
- Verify the configuration
- Test the VPN configuration using SDM

Background

VPNs can provide a secure method of transmitting data over a public network, such as the Internet. VPN connections can help reduce the costs associated with leased lines. Site-to-Site VPNs typically provide a secure (IPsec or other) tunnel between a branch office and a central office. Another common implementation that uses VPN technology is remote access to a corporate office from a telecommuter location such as a small office or home office.

In this lab, you build a multi-router network and configure the routers and hosts. You use Cisco IOS and SDM to configure a site-to-site IPsec VPN and test it. The IPsec VPN tunnel is from router R1 to router R3 via R2. R2 acts as a pass-through and has no knowledge of the VPN. IPsec provides secure transmission of sensitive information over unprotected networks such as the Internet. IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec devices (peers), such as Cisco routers.

Note: The router commands and output in this lab are from a Cisco 1841 with Cisco IOS Release 12.4(20)T (Advanced IP image). Other routers and Cisco IOS versions can be used. See the Router Interface Summary table at the end of the lab to determine which interface identifiers to use based on the equipment in the lab. Depending on the router model and Cisco IOS version, the commands available and output produced might vary from what is shown in this lab.

Note: Make sure that the routers and the switches have been erased and have no startup configurations.

Required Resources

- 3 routers with SDM 2.5 installed (Cisco 1841 with Cisco IOS Release 12.4(20)T1 or comparable)
- 2 switches (Cisco 2960 or comparable)
- PC-A (Windows XP or Vista)
- PC-C (Windows XP or Vista)

- Serial and Ethernet cables as shown in the topology
- Rollover cables to configure the routers via the console

Part 1. Basic Router Configuration

In Part 1 of this lab, you set up the network topology and configure basic settings, such as the interface IP addresses, dynamic routing, device access, and passwords.

Note: All tasks should be performed on routers R1, R2, and R3. The procedure for R1 is shown here as an example.

Step 1: Cable the network as shown in the topology.

Attach the devices shown in the topology diagram, and cable as necessary.

Step 2: Configure basic settings for each router.

a. Configure host names as shown in the topology.

b. Configure the interface IP addresses as shown in the IP addressing table.

c. Configure a clock rate for the serial router interfaces with a DCE serial cable attached.

```
R1(config)#interface S0/0/0
R1(config-if)#clock rate 64000
```

Step 3: Disable DNS lookup.

To prevent the router from attempting to translate incorrectly entered commands, disable DNS lookup.

```
R1(config)#no ip domain-lookup
```

Step 4: Configure the EIGRP routing protocol on R1, R2, and R3.

a. On R1, use the following commands.

```
R1(config)#router eigrp 101
R1(config-router)#network 192.168.1.0 0.0.0.255
R1(config-router)#network 10.1.1.0 0.0.0.3
R1(config-router)#no auto-summary
```

b. On R2, use the following commands.

```
R2(config)#router eigrp 101
R2(config-router)#network 10.1.1.0 0.0.0.3
R2(config-router)#network 10.2.2.0 0.0.0.3
R2(config-router)#no auto-summary
```

c. On R3, use the following commands.

```
R3(config)#router eigrp 101
R3(config-router)#network 192.168.3.0 0.0.0.255
R3(config-router)#network 10.2.2.0 0.0.0.3
R3(config-router)#no auto-summary
```

Step 5: Configure PC host IP settings.

a. Configure a static IP address, subnet mask, and default gateway for PC-A, as shown in the IP addressing table.

b. Configure a static IP address, subnet mask, and default gateway for PC-C, as shown in the IP addressing table.

Step 6: Verify basic network connectivity.

a. Ping from R1 to the R3 Fa0/1 interface at IP address 192.168.3.1.

Were the results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

b. Ping from PC-A on the R1 LAN to PC-C on the R3 LAN.

Were the results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Note: If you can ping from PC-A to PC-C, you have demonstrated that the EIGRP routing protocol is configured and functioning correctly. If you cannot ping but the device interfaces are up and IP addresses are correct, use the **show run** and **show ip route** commands to help identify routing protocol-related problems.

Step 7: Configure a minimum password length.

Note: Passwords in this lab are set to a minimum of 10 characters but are relatively simple for the benefit of performing the lab. More complex passwords are recommended in a production network.

Use the **security passwords** command to set a minimum password length of 10 characters.

```
R1(config)#security passwords min-length 10
```

Step 8: Configure the basic console and vty lines.

a. Configure a console password and enable login for router R1. For additional security, the **exec-timeout** command causes the line to log out after 5 minutes of inactivity. The **logging synchronous** command prevents console messages from interrupting command entry.

Note: To avoid repetitive logins during this lab, the **exec-timeout** can be set to 0 0, which prevents it from expiring. However, this is not considered a good security practice.

```
R1(config)#line console 0
R1(config-line)#password ciscoconpass
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
R1(config-line)#logging synchronous
```

b. Configure the password on the vty lines for router R1.

```
R1(config)#line vty 0 4
R1(config-line)#password ciscovtypass
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
```

c. Repeat these configurations on both R2 and R3.

Step 9: Encrypt clear text passwords.

a. Use the **service password-encryption** command to encrypt the console, aux, and vty passwords.

```
R1(config)#service password-encryption
```

b. Issue the **show run** command. Can you read the console, aux, and vty passwords? Why or why not?

_____

c. Repeat this configuration on both R2 and R3.

Step 10: Save the basic running configuration for all three routers.

Save the running configuration to the startup configuration from the privileged EXEC prompt.

```
R1#copy running-config startup-config
```

Step 11: Save the configuration on R1 and R3 for later restoration.

Use HyperTerminal or another means such as copy and paste to save the R1 and R3 running configurations from Part 1 of this lab and edit them so that they can be used to restore the routers in Part 3 of the lab to configure the VPN with SDM.

Note: When editing the captured running config text, remove all occurrences of "- - More - -." Remove any commands that are not related to the items you configured in Part 1 of the lab, such as the Cisco IOS version number, no service pad, and so on. Many commands are entered automatically by the Cisco IOS software. Also replace the encrypted passwords with the correct ones specified previously and be sure to use the **no shutdown** command for interfaces that need to be enabled.

Part 2. Configure a Site-to-Site VPN with Cisco IOS

In Part 2 of this lab, you configure an IPsec VPN tunnel between R1 and R3 that passes through R2. You will configure R1 and R3 using the Cisco IOS CLI. You then review and test the resulting configuration.

Task 1. Configure Ipsec VPN Settings on R1 and R3

Step 1: Verify connectivity from the R1 LAN to the R3 LAN.

In this task, you verify that with no tunnel in place, the PC-A on the R1 LAN can ping the PC-C on R3 LAN.

a. From PC-A, ping the PC-C IP address of 192.168.3.3.

```
PC-A:\>ping 192.168.3.3
```

b. Were the results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Step 2: Enable IKE policies on R1 and R3.

IPsec is an open framework that allows the exchange of security protocols as new technologies, such as encryption algorithms, are developed.

There are two central configuration elements to the implementation of an Ipsec VPN:

- Implement Internet Key Exchange (IKE) parameters
- Implement Ipsec parameters

a. Verify that IKE is supported and enabled.

IKE Phase 1 defines the key exchange method used to pass and validate IKE policies between peers. In IKE Phase 2, the peers exchange and match IPsec policies for the authentication and encryption of data traffic.

IKE must be enabled for Ipsec to function. IKE is enabled by default on IOS images with cryptographic feature sets. If it is disabled for some reason, you can enable it with the command **crypto isakmp enable**. Use this command to verify that the router IOS supports IKE and that it is enabled.

```
R1(config)#crypto isakmp enable

R3(config)#crypto isakmp enable
```

Note: If you cannot execute this command on the router, you need to upgrade the IOS image to one with a feature set that includes the Cisco cryptographic services.

b. Establish an Internet Security Association and Key Management Protocol (ISAKMP) policy and view the available options.

To allow IKE Phase 1 negotiation, you must create an ISAKMP policy and configure a peer association involving that ISAKMP policy. An ISAKMP policy defines the authentication and encryption algorithms and hash function used to send control traffic between the two VPN endpoints. When an ISAKMP security association has been accepted by the IKE peers, IKE Phase 1 has been completed. IKE Phase 2 parameters will be configured later.

Issue the **crypto isakmp policy** *number* configuration command on R1 for policy 10.

```
R1(config)#crypto isakmp policy 10
```

c. View the various IKE parameters available using Cisco IOS help by typing a question mark (?).

```
R1(config-isakmp)# ?
ISAKMP commands:
  authentication  Set authentication method for protection suite
  default         Set a command to its defaults
  encryption      Set encryption algorithm for protection suite
  exit            Exit from ISAKMP protection suite configuration mode
  group           Set the Diffie-Hellman group
  hash            Set hash algorithm for protection suite
  lifetime        Set lifetime for ISAKMP security association
  no              Negate a command or set its defaults
```

Step 3: Configure ISAKMP policy parameters on R1 and R3.

Your choice of an encryption algorithm determines how confidential the control channel between the endpoints is. The hash algorithm controls data integrity, ensuring that the data received from a peer has not been tampered with in transit. The authentication type ensures that the packet was indeed sent and signed by the remote peer. The Diffie-Hellman group is used to create a secret key shared by the peers that has not been sent across the network.

a. Configure an authentication type of pre-shared keys. Use AES 256 encryption, SHA as your hash algorithm, and Diffie-Hellman group 5 key exchange for this IKE policy.

b. Give the policy a life time of 3600 seconds (one hour). Configure the same policy on R3. Older versions of Cisco IOS do not support AES 256 encryption and SHA as a hash algorithm. Substitute whatever encryption and hashing algorithm your router supports. Be sure the same changes are made on the other VPN endpoint so that they are in sync.

Note: You should be at the R1(config-isakmp)# at this point. The **crypto isakmp policy 10** command is repeated below for clarity.

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#hash sha
R1(config-isakmp)#group 5
R1(config-isakmp)#lifetime 3600
R1(config-isakmp)#end

R3(config)#crypto isakmp policy 10
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#encryption aes 256
R3(config-isakmp)#hash sha
R3(config-isakmp)#group 5
R3(config-isakmp)#lifetime 3600
R3(config-isakmp)#end
```

c. Verify the IKE policy with the **show crypto isakmp policy** command.

```
R1#show crypto isakmp policy
Global IKE policy
Protection suite of priority 10
   encryption algorithm: AES – Advanced Encryption Standard (256 bit
   keys).
   Hash algorithm:            Secure Hash Standard
   authentication method:     Pre-Shared Key
   Diffie-Hellman group:      #5 (1536 bit)
   lifetime:                  3600 seconds, no volume limit
```

Step 4: Configure pre-shared keys.

Because pre-shared keys are used as the authentication method in the IKE policy, configure a key on each router that points to the other VPN endpoint. These keys must match for authentication to be successful. The global configuration command **crypto isakmp key** *key-string* **address** *address* is used to enter a pre-shared key. Use the IP address of the remote peer, the remote interface that the peer would use to route traffic to the local router.

Which IP addresses should you use to configure the IKE peers, given the topology diagram and IP addressing table?

_____

_____

a. Each IP address that is used to configure the IKE peers is also referred to as the IP address of the remote VPN endpoint. Configure the pre-shared key of cisco123 on router R1 using the following command. Production networks should use a complex key. This command points to the remote peer R3 S0/0/1 IP address.

```
R1(config)#crypto isakmp key cisco123 address 10.2.2.1
```

b. The command for R3 points to the R1 S0/0/0 IP address. Configure the pre-shared key on router R1 using the following command.

```
R3(config)#crypto isakmp key cisco123 address 10.1.1.1
```

Step 5: Configure the IPsec transform set and life times.

a. The IPsec transform set is another crypto configuration parameter that routers negotiate to form a security association. To create an Ipsec transform set, use the **crypto ipsec transform-set** *tag* parameters. Use **?** to see which parameters are available.

```
R1(config)#crypto ipsec transform-set 50 ?
  ah-md5-hmac   AH-HMAC-MD5 transform
  ah-sha-hmac   AH-HMAC-SHA transform
  comp-lzs      IP Compression using the LZS compression algorithm
  esp-3des      ESP transform using 3DES(EDE) cipher (168 bits)
  esp-aes       ESP transform using AES cipher
  esp-des       ESP transform using DES cipher (56 bits)
  esp-md5-hmac  ESP transform using HMAC-MD5 auth
  esp-null      ESP transform w/o cipher
  esp-seal      ESP transform using SEAL cipher (160 bits)
  esp-sha-hmac  ESP transform using HMAC-SHA auth
```

b. On R1 and R3, create a transform set with tag 50 and use an Encapsulating Security Protocol (ESP) transform with an AES 256 cipher with ESP and the SHA hash function. The transform sets must match.

```
R1(config)#crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
R1(cfg-crypto-trans)#exit

R3(config)#crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
R3(cfg-crypto-trans)#exit
```

c. What is the function of the IPsec transform set?

_____

_____

d. You can also change the IPsec security association life times from the default of 3600 seconds or 4,608,000 kilobytes, whichever comes first. On R1 and R3, set the Ipsec security association life time to 30 minutes, or 1800 seconds.

```
R1(config)#crypto ipsec security-association lifetime seconds 1800

R3(config)#crypto ipsec security-association lifetime seconds 1800
```

Step 6: Define interesting traffic.

To make use of the Ipsec encryption with the VPN, it is necessary to define extended access lists to tell the router which traffic to encrypt. A packet that is permitted by an access list used for defining Ipsec traffic is encrypted if the Ipsec session is configured correctly. A packet that is denied by one of these access lists is not dropped, but sent unencrypted. Also, like any other access list, there is an implicit deny at the end, which, in this case, means the default action is to not encrypt traffic. If there is no Ipsec security association correctly configured, no traffic is encrypted, and traffic is forwarded as unencrypted.

a. In this scenario, the traffic you want to encrypt is traffic going from R1's Ethernet LAN to R3's Ethernet LAN, or vice versa. These access lists are used outbound on the VPN endpoint interfaces and must mirror each other.

b. Configure the IPsec VPN interesting traffic ACL on R1.

```
R1(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0
0.0.0.255
```

c. Configure the IPsec VPN interesting traffic ACL on R3.

```
R3(config)#access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0
0.0.0.255
```

d. Does IPsec evaluate whether the access lists are mirrored as a requirement to negotiate its security association?

_____

_____

Step 7: Create and apply a crypto map.

A crypto map associates traffic that matches an access list to a peer and various IKE and Ipsec settings. After the crypto map is created, it can be applied to one or more interfaces. The interfaces that it is applied to should be the ones facing the Ipsec peer.

To create a crypto map, use the global configuration command **crypto map** *name sequence-num type* to enter the crypto map configuration mode for that sequence number. Multiple crypto map statements can belong to the same crypto map and are evaluated in ascending numerical order. Enter the crypto map configuration mode on R1. Use a type of ipsec-isakmp, which means IKE is used to establish Ipsec security associations.

a. Create the crypto map on R1, name it CMAP, and use 10 as the sequence number. A message will display after the command is issued.

```
R1(config)#crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
```

b. Use the **match address** *access-list* command to specify which access list defines which traffic to encrypt.

```
R1(config-crypto-map)#match address 101
```

c. To view the list of possible **set** commands that you can do in a crypto map, use the help function.

```
R1(config-crypto-map)#set ?
Identity             Identity restriction.
Ip                   Interface Internet Protocol config commands
isakmp-profile       Specify isakmp Profile
nat                  Set NAT translation
peer                 Allowed Encryption/Decryption peer.
Pfs                  Specify pfs settings
security-association Security association parameters
transform-set        Specify list of transform sets in priority order
```

d. Setting a peer IP or host name is required, so set it to R3's remote VPN endpoint interface using the following command.

```
R1(config-crypto-map)#set peer 10.2.2.1
```

e. Hard code the transform set to be used with this peer, using the **set transform-set** *tag* command. Set the perfect forwarding secrecy type using the **set pfs** *type* command, and also modify the default IPsec security association life time with the **set security-association lifetime seconds** *seconds* command.

```
R1(config-crypto-map)#set pfs group5
R1(config-crypto-map)#set transform-set 50
```

```
R1(config-crypto-map)#set security-association lifetime seconds 900
R1(config-crypto-map)#exit
```

f. Create a mirrored matching crypto map on R3.

```
R3(config)#crypto map CMAP 10 ipsec-isakmp
R3(config-crypto-map)#match address 101
R3(config-crypto-map)#set peer 10.1.1.1
R3(config-crypto-map)#set pfs group5
R3(config-crypto-map)#set transform-set 50
R3(config-crypto-map)#set security-association lifetime seconds 900
R3(config-crypto-map)#exit
```

g. The last step is applying the maps to interfaces. Note that the security associations (SAs) will not be established until the crypto map has been activated by interesting traffic. The router will generate a notification that crypto is now on.

h. Apply the crypto maps to the appropriate interfaces on R1 and R3.

```
R1(config)#interface S0/0/0
R1(config-if)#crypto map CMAP
*Jan 28 04:09:09.150: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config)#end

R3(config)#interface S0/0/1
R3(config-if)#crypto map CMAP
*Jan 28 04:10:54.138: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config)#end
```

Task 2. Verify Site-to-Site IPsec VPN Configuration

Step 1: Verify the Ipsec configuration on R1 and R3.

Previously, you used the **show crypto isakmp policy** command to show the configured ISAKMP policies on the router. Similarly, the **show crypto ipsec transform-set** command displays the configured Ipsec policies in the form of the transform sets.

```
R1#show crypto ipsec transform-set
Transform set 50: { esp-256-aes esp-sha-hmac }
will negotiate = { Tunnel, },

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },


R3#show crypto ipsec transform-set
Transform set 50: { esp-256-aes esp-sha-hmac }
will negotiate = { Tunnel, },

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },
```

Use the **show crypto map** command to display the crypto maps that will be applied to the router.

```
R1#show crypto map
Crypto Map "CMAP" 10 ipsec-isakmp
  Peer = 10.2.2.1
  Extended IP access list 101
  access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

  Current peer: 10.2.2.1
  Security association lifetime: 4608000 kilobytes/900 seconds
  PFS (Y/N): Y
  DH group:  group5
  Transform sets={
         50: { esp-256-aes esp-sha-hmac  } ,
        }
  Interfaces using crypto map MYMAP: Serial0/0/0

R3#show crypto map
Crypto Map "CMAP" 10 ipsec-isakmp
  Peer = 10.1.1.1
  Extended IP access list 101
  access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255

  Current peer: 10.1.1.1
  Security association lifetime: 4608000 kilobytes/900 seconds
  PFS (Y/N): Y
  DH group:  group5
  Transform sets={
         50: { esp-256-aes esp-sha-hmac  } ,
        }
  Interfaces using crypto map MYMAP: Serial0/0/1
```

Note: The output of these **show** commands does not change if interesting traffic goes across the connection. You test various types of traffic in the next task.

Task 3. Verify IPsec VPN Operation

Step 1: Display isakmp security associations.

The **show crypto isakmp sa** command reveals that no IKE Sas exist yet. When interesting traffic is sent, this command output will change.

```
R1#show crypto isakmp sa

dst   src   state       conn-id slot status
```

Step 2: Display Ipsec security associations.

The **show crypto ipsec sa** command shows the unused SA between R1 and R3. Note the number of packets sent across and the lack of any security associations listed toward the bottom of the output. The output for R1 is shown here.

```
R1#show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: CMAP, local addr 10.1.1.1

   protected vrf: (none)
```

```
local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
current_peer 10.2.2.1 port 500
  PERMIT, flags={origin_is_acl,}
 #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
 #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. Failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 0, #recv errors 0

  local crypto endpt.: 10.1.1.1, remote crypto endpt.: 10.2.2.1
  path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
  current outbound spi: 0x0(0)

  inbound esp sas:
  inbound ah sas:
  inbound pcp sas:
  outbound esp sas:
  outbound ah sas:
  outbound pcp sas:
```

a. Why have no security associations (SAs) been negotiated?

_____
_____

Step 3: Generate some uninteresting test traffic and observe the results.

Ping from R1 to the R3 S0/0/1 interface IP address 10.2.2.1. Were the pings successful? _____

Issue the **show crypto isakmp sa** command. Was an SA created between R1 and R3? _____

Ping from R1 to the R3 Fa01 interface IP address 192.168.3.1. Were the pings successful? _____

a. Issue the **show crypto isakmp sa** command again. Was an SA created for these pings? Why or why not?

_____
_____
_____
_____

b. Issue the command **debug eigrp packets**. You should see EIGRP hello packets passing between R1 and R3.

```
R1#debug eigrp packets
EIGRP Packets debugging is on
    (UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB,
SIAQUERY, SIAREPLY)
R1#
*Jan 29 16:05:41.243: EIGRP: Received HELLO on Serial0/0/0 nbr 10.1.1.2
*Jan 29 16:05:41.243:   AS 101, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ
un/rely 0/0 pe
erQ un/rely 0/0
*Jan 29 16:05:41.887: EIGRP: Sending HELLO on Serial0/0/0
*Jan 29 16:05:41.887:   AS 101, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ
un/rely 0/0
R1#
```

```
*Jan 29 16:05:43.143: EIGRP: Sending HELLO on FastEthernet0/1
*Jan 29 16:05:43.143:   AS 101, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ
un/rely 0/0
R1#
```

Turn off debugging with the **no debug eigrp packets** or **undebug all** command.

Issue the **show crypto isakmp sa** command again. Was an SA created between R1 and R3? Why or why not?

_____

_____

Step 4: Generate some interesting test traffic and observe the results.

a. Use an extended ping from R1 to the R3 Fa01 interface IP address 192.168.3.1. Extended ping allows you to control the source address of the packets. Respond as shown in the following example. Press enter to accept the defaults, except where a specific response is indicated.

```
R1#ping
Protocol [ip]:
Target IP address: 192.168.3.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:

Packet sent with a source address of 192.168.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 92/92/92 ms
```

b. Issue the **show crypto isakmp sa** command again.

```
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.2.2.1        10.1.1.1        QM_IDLE           1001    0 ACTIVE
```

c. Why was an SA created between R1 and R3 this time?

_____

_____

d. What are the endpoints of the IPsec VPN tunnel? _____

e. Ping from PC-A to PC-C. Were the pings successful? _____

f. Issue the **show crypto ipsec sa** command. How many packets have been transformed between R1 and R3?

_____R1**#show crypto ipsec sa**

```
interface: Serial0/0/0
    Crypto map tag: CMAP, local addr 10.1.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
    #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. Failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.1.1.1, remote crypto endpt.: 10.2.2.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0xC1DD058(203280472)

     inbound esp sas:
      spi: 0xDF57120F(3747025423)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2005, flow_id: FPGA:5, crypto map: CMAP
        sa timing: remaining key lifetime (k/sec): (4485195/877)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xC1DD058(203280472)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2006, flow_id: FPGA:6, crypto map: CMAP
        sa timing: remaining key lifetime (k/sec): (4485195/877)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

g. The previous example used pings to generate interesting traffic. What other types of traffic would result in an SA forming and tunnel establishment?

_____
_____
_____

Part 3. Configure a Site-to-Site IPsec VPN with SDM

In Part 3 of this lab, you configure an Ipsec VPN tunnel between R1 and R3 that passes through R2. In Task 2, you configure R1 using Cisco SDM. In Task 3, you mirror those settings to R3 using SDM utilities. You then review and test the resulting configuration.

Task 1. Restore Router R1 and R3 to the Basic Settings

To avoid confusion as to what was entered in Part 2 of the lab, start by restoring R1 and R3 to the basic configuration as described in Part 1 of this lab.

Step 1: Erase and reload the router.

a. Connect to the router console, and enter privileged EXEC mode.

b. Erase the startup config and then issue the **reload** command to restart the router.

Step 2: Restore the basic configuration.

a. When the router restarts, enter privileged EXEC mode with the **enable** command, and then enter global config mode. Use the HyperTerminal **Transfer > Send File** function, copy and paste or use another method to load the basic startup config for R1 and R3 that was created and saved in Part 1 of this lab.

b. Save the running config to the startup config for R1 and R3 using the **copy run start** command.

c. Test connectivity by pinging from host PC-A to PC-C. If the pings are not successful, troubleshoot the router and PC configurations before continuing.

Task 2. Configure IPsec VPN Settings on R1 Using SDM

Step 1: Configure the enable secret password and HTTP router access prior to starting SDM.

a. From the CLI, configure the enable secret password for use with SDM on R1 and R3.

```
R1(config)#enable secret cisco12345

R3(config)#enable secret cisco12345
```

b. Enable the HTTP server on R1 and R3.

```
R1(config)#ip http server

R3(config)#ip http server
```

Step 2: Access SDM and set command delivery preferences.

a. Run the SDM application, or open a browser on PC-A and start SDM by entering the R1 IP address 192.168.1.1 in the address field.

> **Note:** You might be prompted by Internet Explorer to allow ActiveX during several of these steps. Click **Allow**.

b. Log in with no username and the enable secret password **cisco12345**.

c. In the Authentication Required dialog box, leave the Username field blank and enter **cisco12345** in the Password field. Click **Yes**.

d. If the IOS IPS login dialog displays, click the **Cancel** button to bypass this option.

e. Select **Edit** > **Preferences** to configure SDM to allow you to preview the commands before sending them to the router. In the User Preferences window, check the **Preview commands before delivering to router** check box and click **OK**.

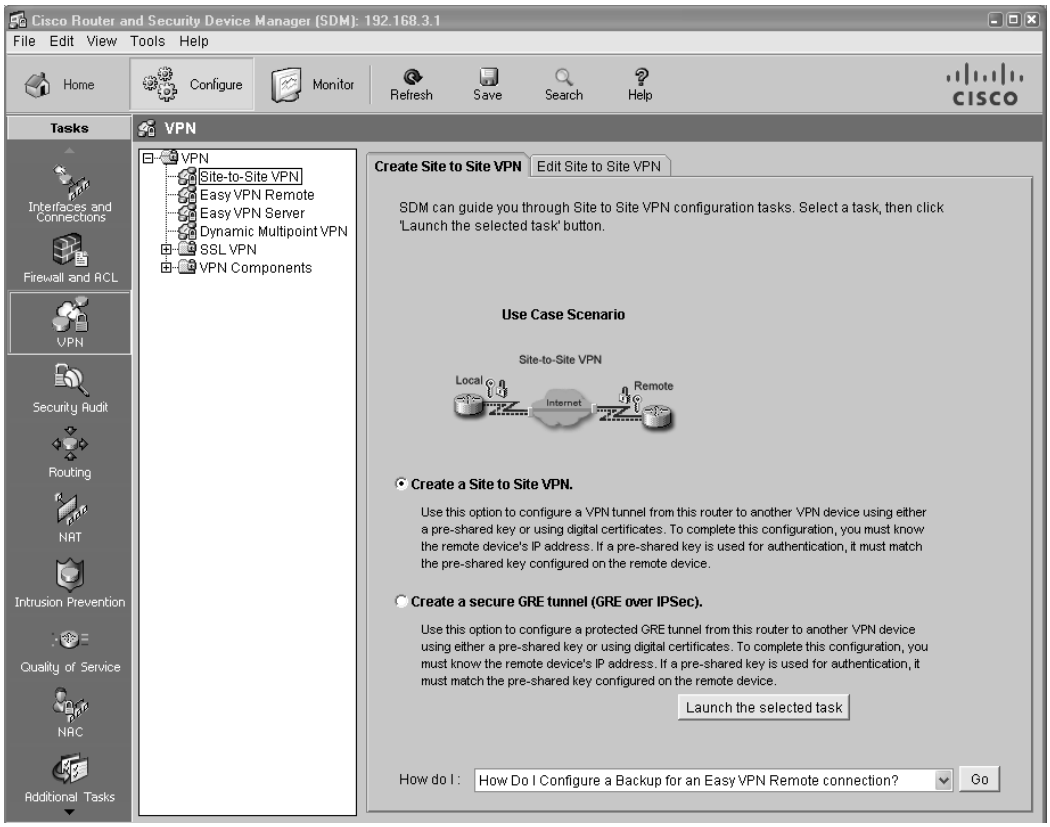
Step 3: Start the SDM VPN wizard to configure R1.

a. Click the **Configure** button at the top of the SDM screen, and then click the **VPN** button. Select **Site-to-Site VPN** from the list of options. The default option is Create Site-to-Site VPN. Read through the description of this option.

b. What must you know to complete the configuration?

_____

_____



c. Click the **Launch the selected task** button to begin the SDM Site-to-Site VPN wizard.

d. On the initial Site-to-Site VPN wizard window, the **Quick Setup** option is selected by default. Click the **View Details** button to see what settings this option uses. What type of encryption does the default transform set use? _____

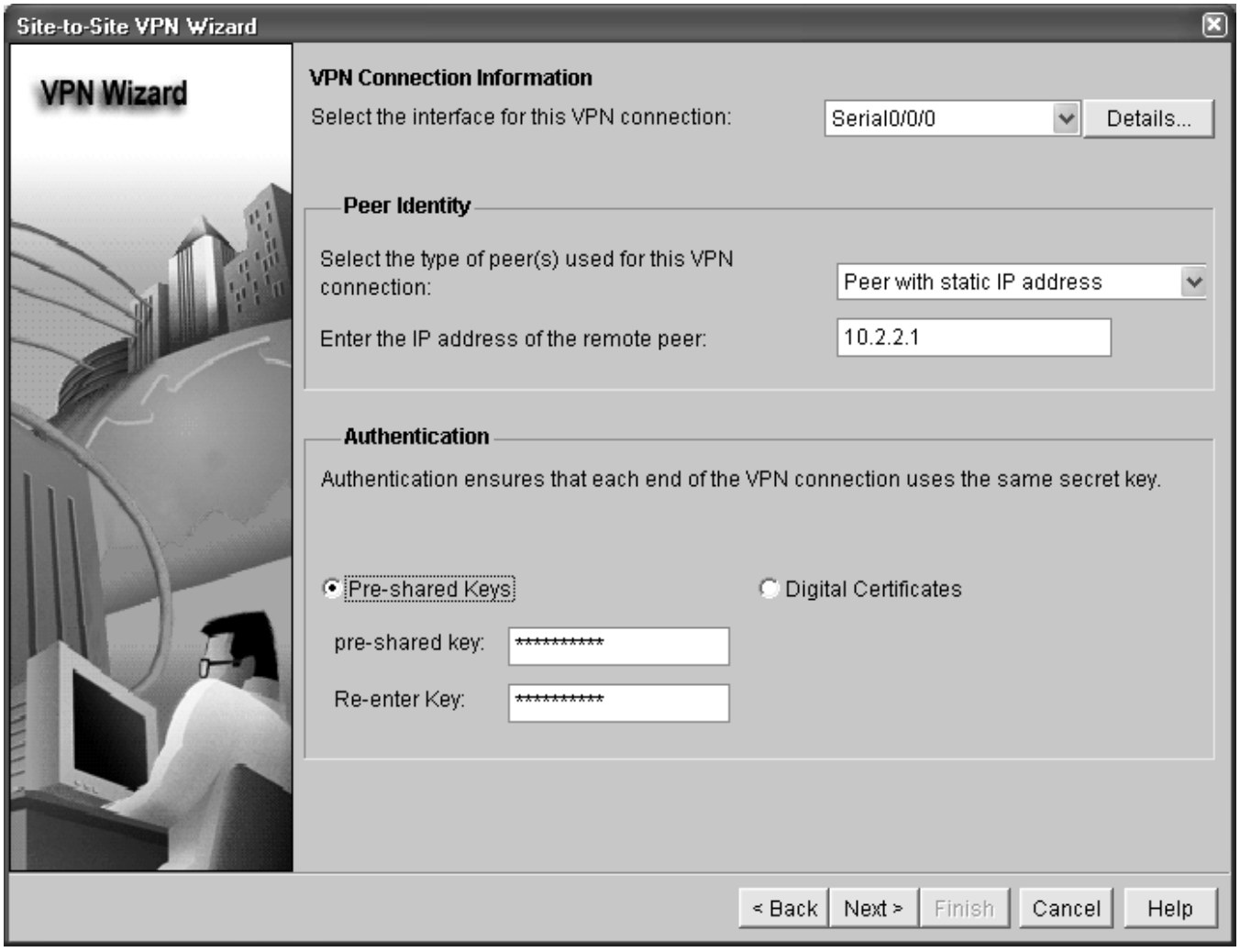
e. From the initial Site-to-Site VPN wizard window, select the **Step by Step** wizard, and then click **Next**. Why would you use this option over the Quick setup option? _____

Step 4: Configure basic VPN connection information settings.

a. From the VPN Connection Information window, select the interface for the connection, which should be R1 Serial0/0/0.

b. In the Peer Identity section, select **Peer with static address** and enter the IP address of remote peer R3 S0/0/1 (10.2.2.1).

c. In the Authentication section, click **Pre-shared keys**, and enter the pre-shared VPN key **cisco12345**. Re-enter the key for confirmation. This key is what protects the VPN and keeps it secure. When finished, your screen should look similar to the following. Once you have entered these settings correctly, click **Next**.



Step 5: Configure IKE policy parameters.

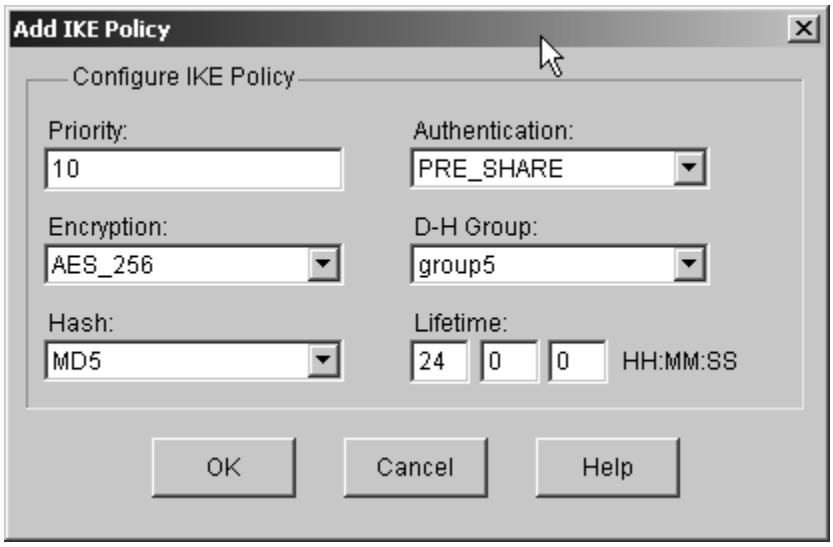
IKE policies are used while setting up the control channel between the two VPN endpoints for key exchange. This is also referred to as the IKE secure association (SA). In contrast, the IPsec policy is used during IKE Phase II to negotiate an Ipsec security association to pass target data traffic.

In the IKE Proposals window, a default policy proposal is displayed. You can use this one or create a new one. What function does this IKE proposal serve?

_____

a. Click the **Add** button to create a new IKE policy.

b. Set up the security policy as shown in the Add IKE Policy dialog box below. These settings are matched later on R3. When finished, click **OK** to add the policy. Then click **Next.**



c. Click the **Help** button to assist you with answering the following questions. What is the function of the encryption algorithm in the IKE policy?

_____
_____

d. What is the purpose of the hash function?

_____
_____

e. What function does the authentication method serve?

_____
_____

f. How is the Diffie-Hellman group in the IKE policy used?

_____
_____

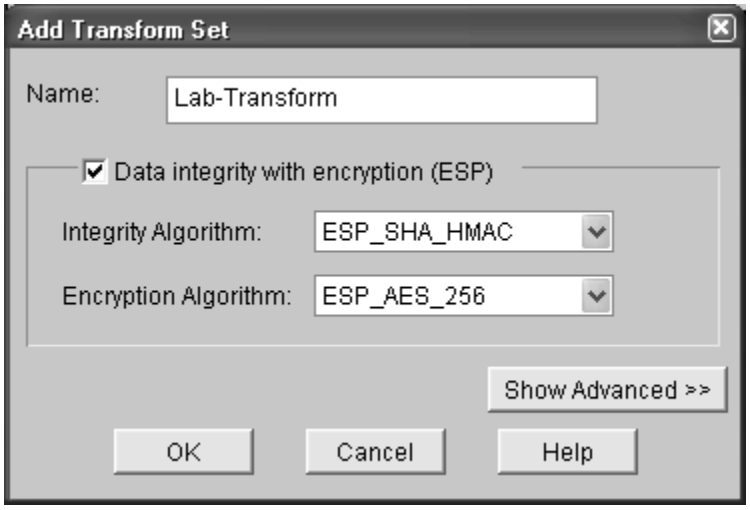
g. What event happens at the end of the IKE policy's lifetime? _____

Step 6: Configure a transform set.

The transform set is the IPsec policy used to encrypt, hash, and authenticate packets that pass through the tunnel. The transform set is the IKE Phase 2 policy.

a. An SDM default transform set is displayed. Click the **Add** button to create a new transform set.

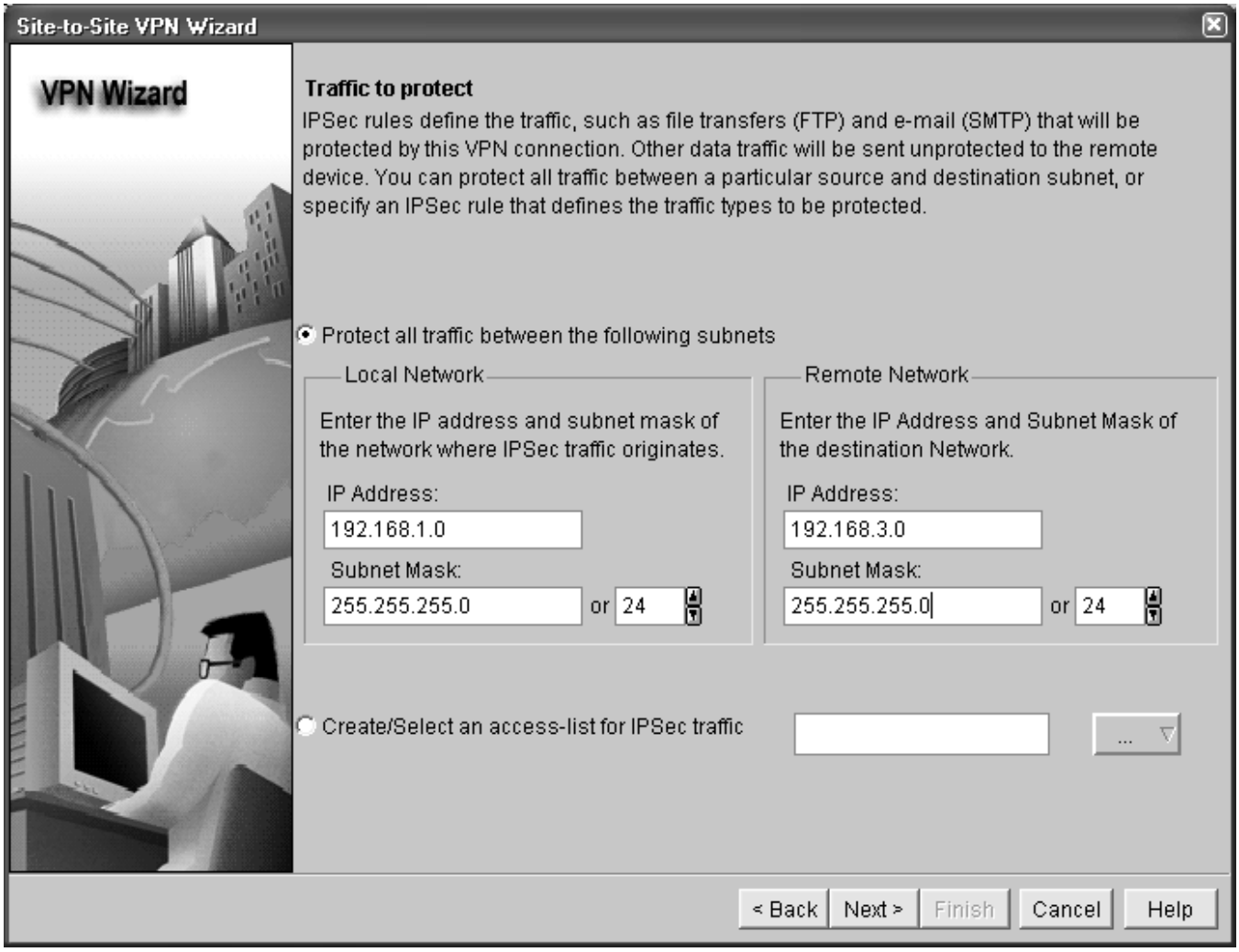
b. Set up the transform set as shown in the Transform Set dialog box below. These settings are matched later on R3. When finished, click **OK** to add the transform set. Then click **Next.**



Step 7: Define interesting traffic.

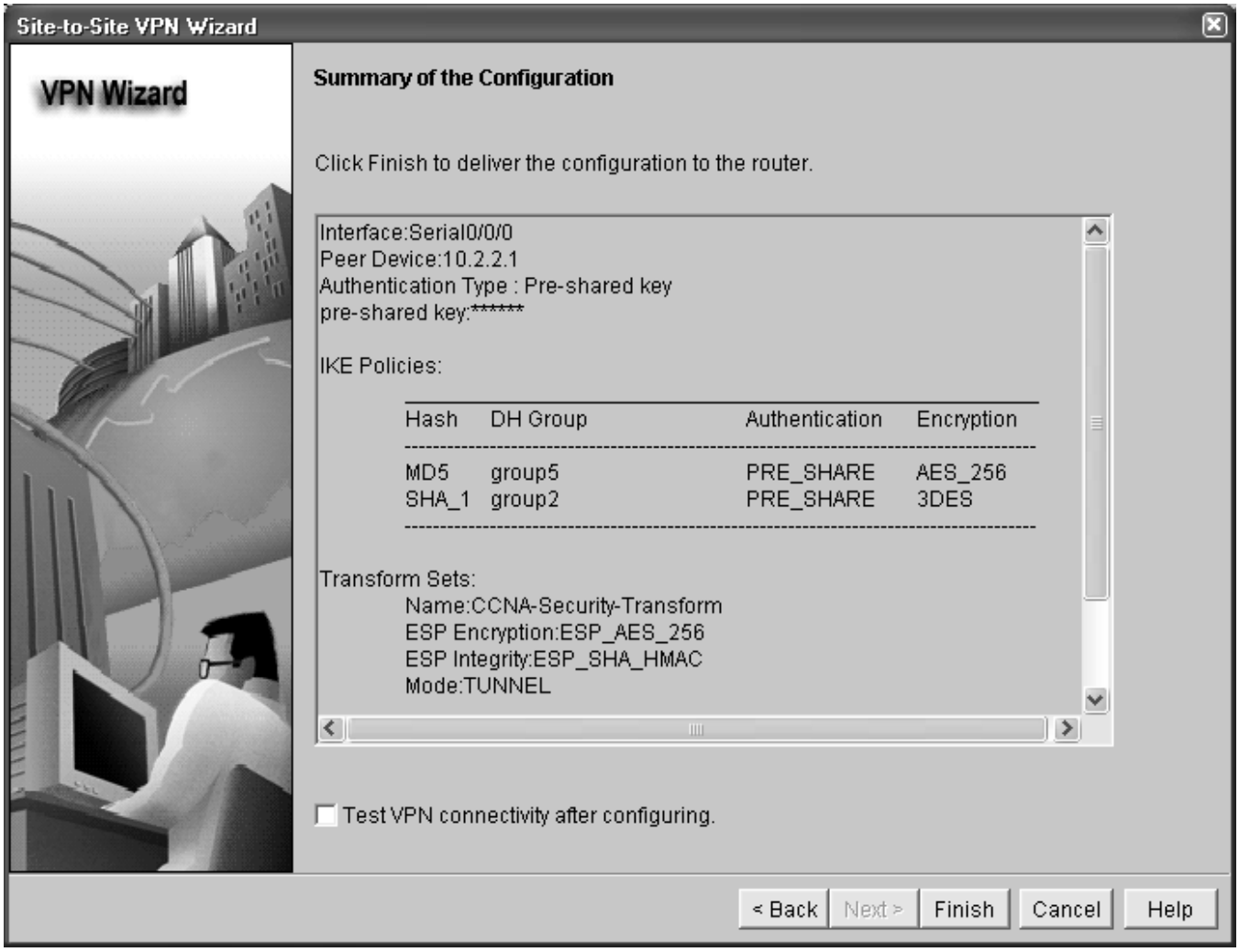
You must define interesting traffic to be protected through the VPN tunnel. Interesting traffic will be defined through an access list when applied to the router. If you enter source and destination subnets, SDM generates the appropriate simple access list for you.

In the Traffic to protect window, enter the information as shown below. These are the opposite of the settings configured on R3 later in the lab. When finished, click **Next.**



Step 8: Review the summary configuration and deliver commands to the router.

a. Review the summary of the Configuration window. It should look similar to the one below. Do not select the checkbox for Test VPN connectivity after configuring. This is done after configuring R3.



b. In the Deliver Configuration to router window, select **Save running config to router's startup config** and click the **Deliver** button. After the commands have been delivered, click **OK**. How many commands were delivered? _____

Task 3. Create a Mirror Configuration for R3

Step 1: Use SDM on R1 to generate a mirror configuration for R3.

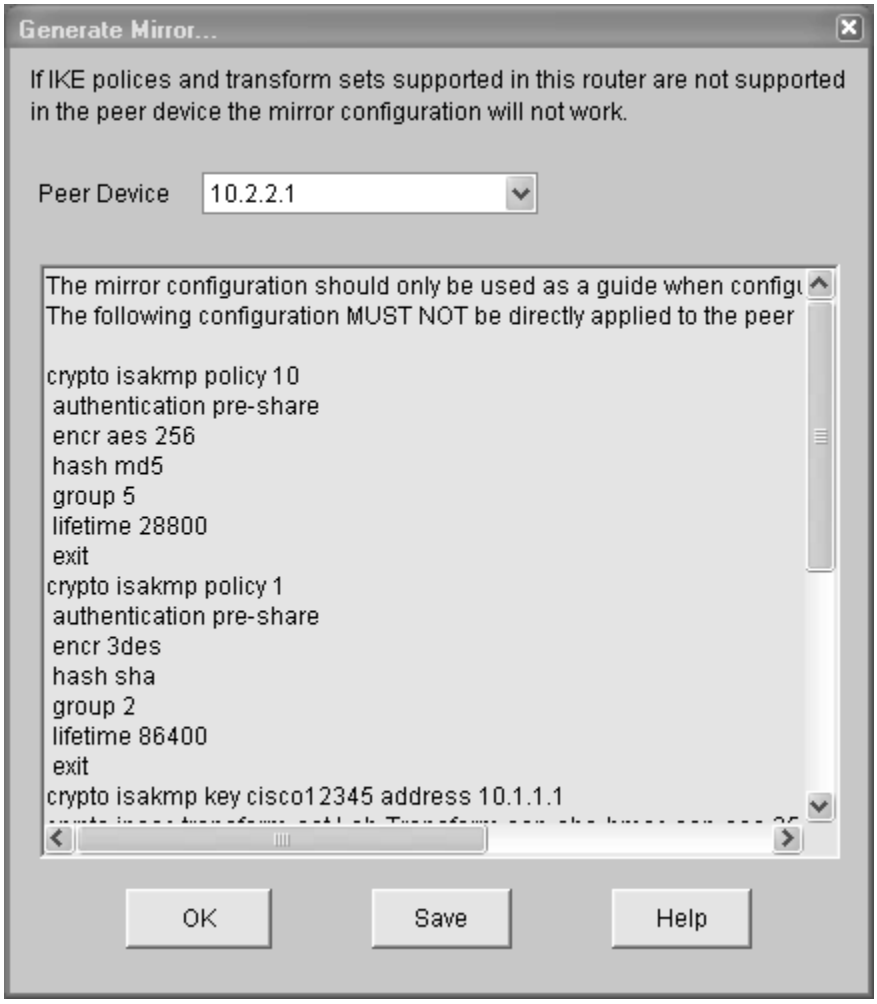
a. On R1, select **VPN > Site-to-Site VPN** and click the **Edit Site-to-Site VPN** tab. You should see the VPN configuration you just created on R1 listed. What is the description of the VPN?

_____

b. What is the status of the VPN and why?

_____

c. Select the VPN policy you just configured on R1 and click the **Generate Mirror** button in the lower right of the window. The Generate Mirror window displays the commands necessary to configure R3 as a VPN peer. Scroll through the window to see all the commands generated.



d. The text at the top of the window states that the configuration generated should only be used as a guide for setting up a site-to-site VPN. What commands are missing to allow this crypto policy to function on R3? _____

Hint: Look at the description entry following the **`crypto map SDM_CMAP_1`** command.

Step 2: Save the configuration commands for R3.

a. Click the **Save** button to create a text file for use in the next task.

b. Save the commands to the desktop or other location and name it VPN-Mirror-Cfg-for-R3.txt.

Note: You can also copy the commands directly from the **Generate Mirror** window.

c**.** (Optional) Edit the file to remove the explanation text at the beginning and the description entry following the **`crypto map SDM_CMAP_1`** command.

Task 4. Apply the Mirror Configuration to R3 and Verify the Configuration

Step 1: Access the R3 CLI and copy the mirror commands.

Note: You can also use SDM on R3 to create the appropriate VPN configuration, but copying and pasting the mirror commands generated from R1 is easier.

On R3, enter privileged EXEC mode and then global config mode.

Copy the commands from the text file into the R3 CLI.

Step 2: Apply the crypto map to the R3 S0/0/1 interface.

```
R3(config)#interface s0/0/1
R3(config-if)#crypto map SDM_CMAP_1
*Jan 30 13:00:38.184: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Step 3: Verify the VPN configuration on R3 using Cisco IOS.

a. Display the running config beginning with the first line that contains the string “0/0/1” to verify that the crypto map is applied to S0/0/1.

```
R3#sh run | beg 0/0/1
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 crypto map SDM_CMAP_1
```

b. On R3, use the **show crypto isakmp policy** command to show the configured ISAKMP policies on the router. Note that the default SDM policy is also present.

```
R3#show crypto isakmp policy

Global IKE policy
Protection suite of priority 1
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit

Protection suite of priority 10
        encryption algorithm:   AES - Advanced Encryption Standard (256
bit keys
).
        Hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               28800 seconds, no volume limit
```

c. In the above output, how many ISAKMP policies are there? _____

d. Issue the **show crypto ipsec transform-set** command to display the configured IPsec policies in the form of the transform sets.

```
R3#show crypto ipsec transform-set
Transform set Lab-Transform: { esp-256-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
```

```
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },
```

e. Use the **show crypto map** command to display the crypto maps that will be applied to the router.

```
R3#show crypto map
Crypto Map "SDM_CMAP_1" 1 ipsec-isakmp
        Description: Apply the crypto map on the peer router's
interface having
IP address 10.2.2.1 that connects to this router.
        Peer = 10.1.1.1
        Extended IP access list SDM_1
            access-list SDM_1 permit ip 192.168.3.0 0.0.0.255
192.168.1.0 0.0.0.255
        Current peer: 10.1.1.1
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                Lab-Transform:  { esp-256-aes esp-sha-hmac  } ,
        }
        Interfaces using crypto map SDM_CMAP_1:
                Serial0/0/1
```

f. In the above output, the ISAKMP policy being used by the crypto map is the SDM default policy with sequence number priority 1, indicated by the number 1 in the first output line: Crypto Map "SDM_CMAP_1" 1 ipsec-isakmp. Why is it not using the one you created in the SDM session — the one shown with priority 10 in Step 3b above?

_____

g. (Optional) You can force the routers to use the more stringent policy that you created by changing the crypto map references in the R1 and R3 router configs as shown below. If this is done, the default ISAKMP policy 1 can be removed from both routers.

```
R1(config)#interface s0/0/0
R1(config-if)#no crypto map SDM_CMAP_1
R1(config-if)#exit
*Jan 30 17:01:46.099: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
R1(config)#no crypto map SDM_CMAP_1 1
R1(config)#crypto map SDM_CMAP_1 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)#description Tunnel to 10.2.2.1
R1(config-crypto-map)#set peer 10.2.2.1
R1(config-crypto-map)#set transform-set Lab-Transform
R1(config-crypto-map)#match address 100
R1(config-crypto-map)#exit
R1(config)#int s0/0/0
R1(config-if)#crypto map SDM_CMAP_1
R1(config-if)#e
*Jan 30 17:03:16.603: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

R3(config)#interface s0/0/1
R3(config-if)#no crypto map SDM_CMAP_1
R3(config-if)#exit
R3(config)#no crypto map SDM_CMAP_1 1
R3(config)#crypto map SDM_CMAP_1 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
```

```
R3(config-crypto-map)#description Tunnel to 10.1.1.1
R3(config-crypto-map)#set peer 10.1.1.1
R3(config-crypto-map)#set transform-set Lab-Transform
R3(config-crypto-map)#match address 100
R3(config-crypto-map)#exit
R3(config)#int s0/0/1
R3(config-if)#crypto map SDM_CMAP_1
R3(config-if)#
*Jan 30 22:18:28.487: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Task 5. Test the VPN Configuration Using SDM on R1.

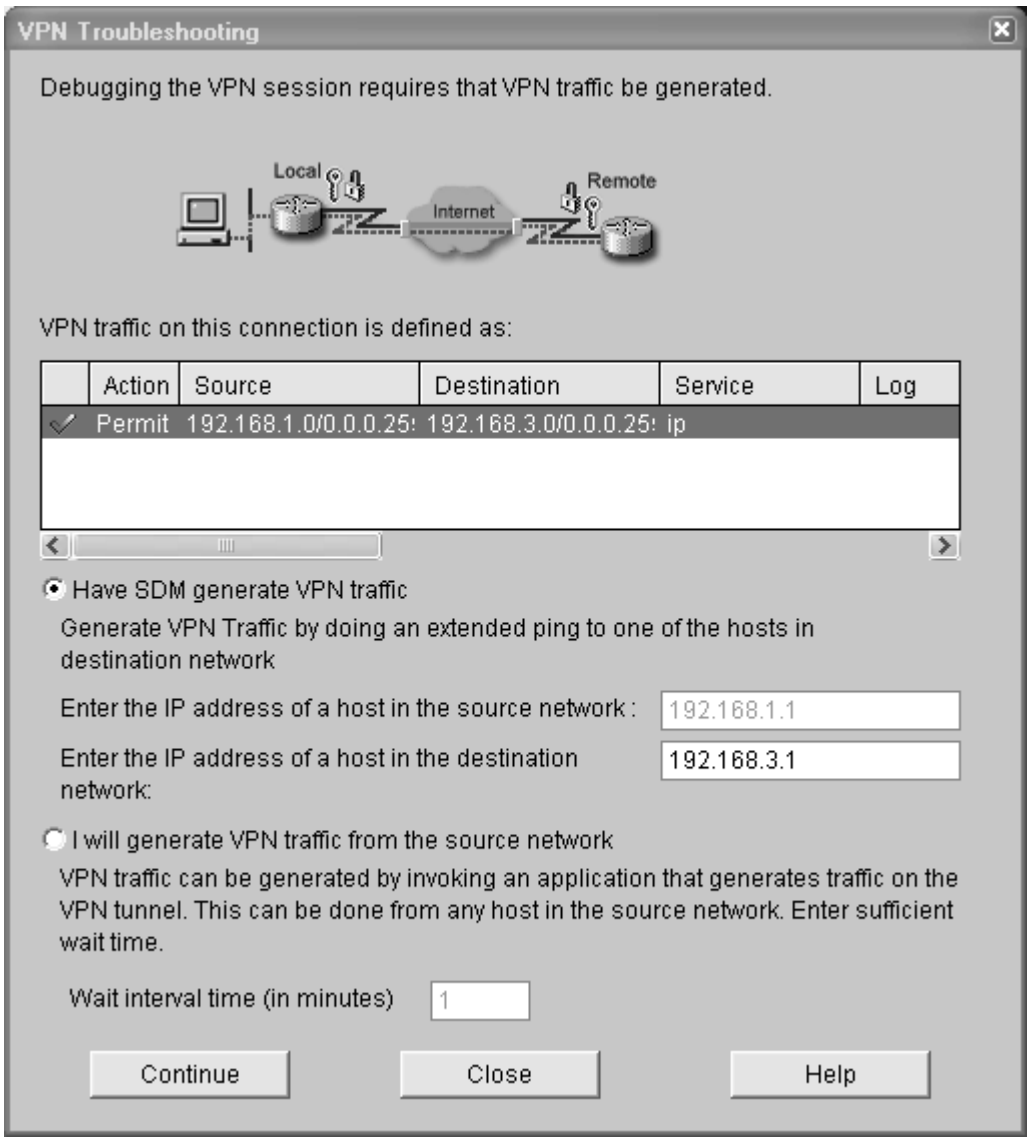
a. On R1, use SDM to test the IPsec VPN tunnel between the two routers. Select **VPN > Site-to-Site VPN** and click the **Edit Site-to-Site VPN** tab.

From the Edit Site to Site VPN tab, select the VPN and click **Test Tunnel**.

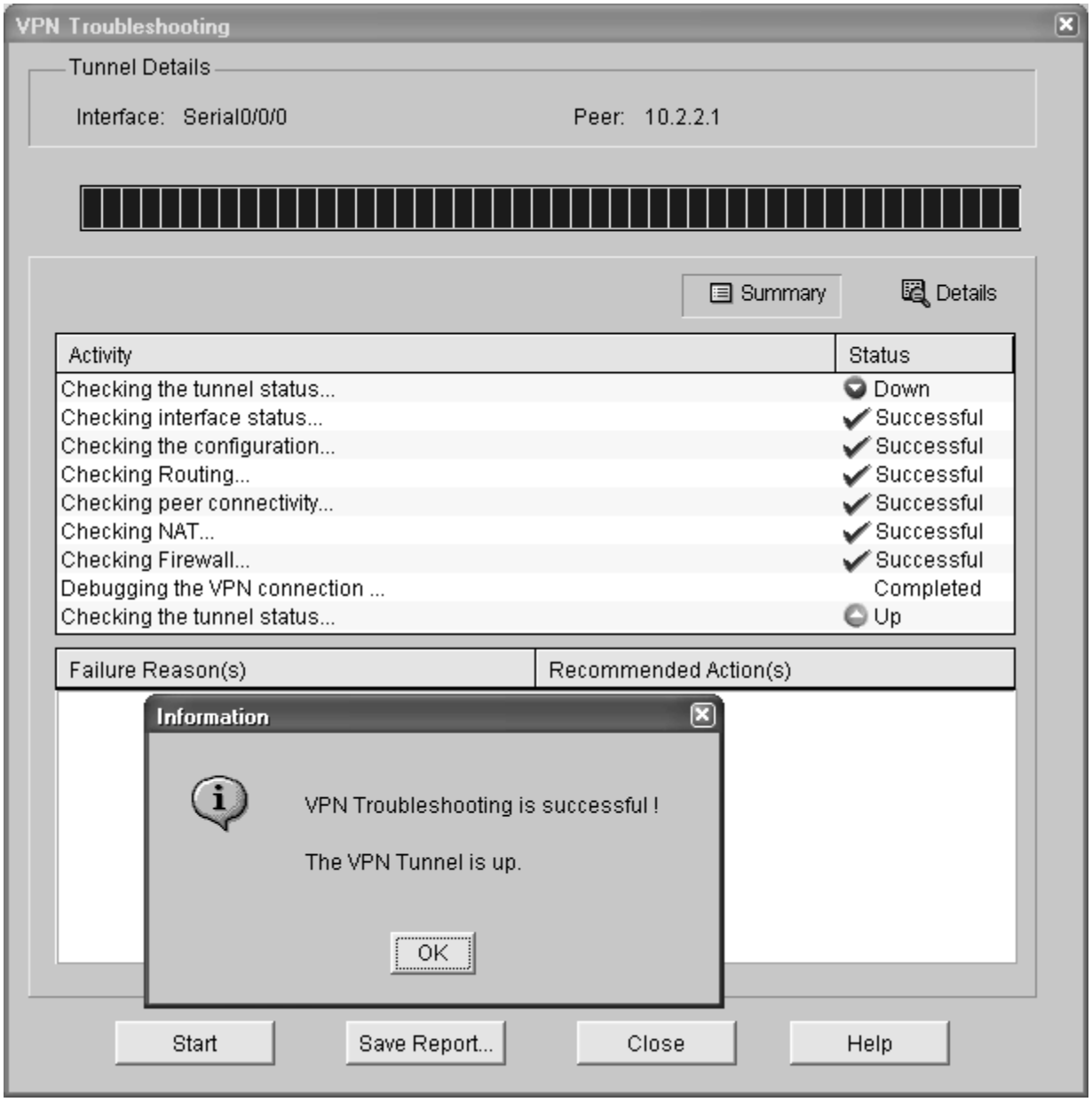
b. When the VPN Troubleshooting window displays, click the **Start** button to have SDM start troubleshooting the tunnel.

c. When the SDM Warning window displays indicating that SDM will enable router debugs and generate some tunnel traffic, click **Yes** to continue.

d. In the next VPN Troubleshooting window, the IP address of the R1 Fa0/1 interface in the source network is displayed by default (192.168.1.1). Enter the IP address of the R3 Fa0/1 interface in the destination network field (192.168.3.1) and click **Continue** to begin the debugging process.



e. If the debug is successful and the tunnel is up, you should see the screen below. If the testing fails, SDM displays failure reasons and recommended actions. Click **OK** to remove the window.



f. You can save the report if desired; otherwise, click **Close**.

Note: If you want to reset the tunnel and test again, you can click the **Clear Connection** button from the Edit Suite-to-Site VPN window. This can also be accomplished at the CLI using the **`clear crypto session`** command.

g**.** Display the running config for R3 beginning with the first line that contains the string 0/0/1 to verify that the crypto map is applied to S0/0/1.

```
R3#sh run | beg 0/0/1
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 crypto map SDM_CMAP_1
<output omitted>
```

h. Issue the **`show crypto isakmp sa`** command on R3 to view the security association created.

```
R3#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.2.2.1        10.1.1.1        QM_IDLE           1001    0 ACTIVE
```

i. Issue the **show crypto ipsec sa** command. How many packets have been transformed between R1 and R3? _____

```
R3#show crypto ipsec sa

interface: Serial0/0/1
    Crypto map tag: SDM_CMAP_1, local addr 10.2.2.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   current_peer 10.1.1.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 116, #pkts encrypt: 116, #pkts digest: 116
    #pkts decaps: 116, #pkts decrypt: 116, #pkts verify: 116
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.2.2.1, remote crypto endpt.: 10.1.1.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/1
     current outbound spi: 0x207AAD8A(544910730)

     inbound esp sas:
      spi: 0xAF102CAE(2937072814)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2007, flow_id: FPGA:7, crypto map: SDM_CMAP_1
        sa timing: remaining key lifetime (k/sec): (4558294/3037)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x207AAD8A(544910730)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2008, flow_id: FPGA:8, crypto map: SDM_CMAP_1
        sa timing: remaining key lifetime (k/sec): (4558294/3037)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

Task 6. Reflection

Would traffic on the Fast Ethernet link between PC-A and the R1 Fa0/0 interface be encrypted by the site-to-site IPsec VPN tunnel? Why or why not?

_____
_____

What are some factors to consider when configuring site-to-site IPsec VPNs using the manual CLI compared to using the SDM VPN wizard GUI?

_____
_____

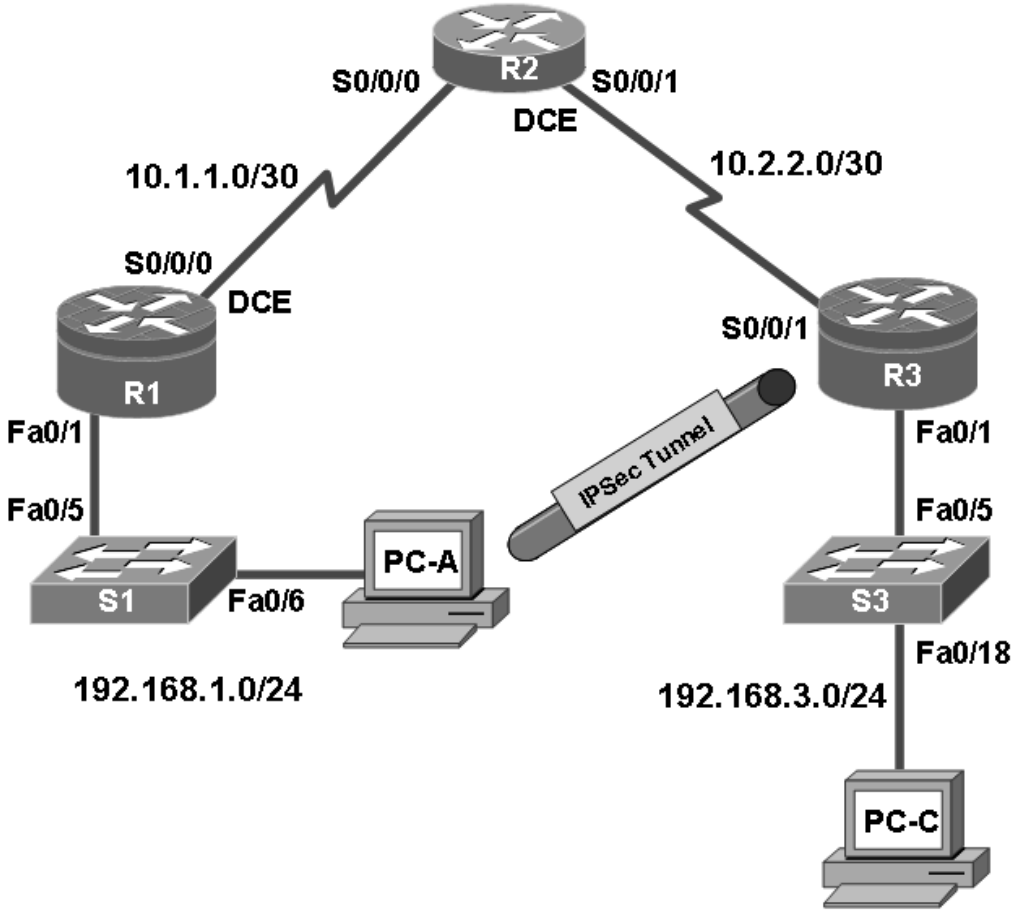
Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1700	Fast Ethernet 0 (FA0)	Fast Ethernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2600	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
2800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Chapter 8: Lab B: Configuring a Remote Access VPN Server and Client

Topology



IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	FA0/1	192.168.1.1	255.255.255.0	N/A	S1 FA0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	FA0/1	192.168.3.1	255.255.255.0	N/A	S3 FA0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 FA0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 FA0/18

Objectives

Part 1: Basic Router Configuration

- Configure host names, interface IP addresses, and access passwords.
- Configure static routing.

Part 2: Configuring a Remote Access VPN

- Configure a zone-based firewall (ZBF) on R3 using SDM.
- Configure Router R3 to support Cisco Easy VPN Server using SDM.
- Configure the Cisco VPN Client on PC-A and connect to R3.
- Verify the configuration.
- Test VPN functionality.

Background

VPNs can provide a secure method of transmitting data over a public network, such as the Internet. A common VPN implementation is used for remote access to a corporate office from a telecommuter location such as a small office or home office (SOHO).

In this lab, you build a multi-router network and configure the routers and hosts. You configure a remote access IPsec VPN between a client computer and a simulated corporate network. You start by using SDM to configure a zoned-based firewall (ZBF) to prevent connections from outside the corporate network. You also use SDM to configure Cisco Easy VPN Server on the corporate gateway router. Next, you configure the Cisco VPN Client on a host and connect to the corporate network through a simulated ISP router.

The Cisco VPN Client allows organizations to establish end-to-end, encrypted (IPsec) VPN tunnels for secure connectivity for mobile employees or teleworkers. It supports Cisco Easy VPN, which allows the client to receive security policies upon a VPN tunnel connection from the central site VPN device (Cisco Easy VPN Server), minimizing configuration requirements at the remote location. Easy VPN is a scalable solution for remote access deployments for which it is impractical to individually configure policies for multiple remote PCs.

Router R1 represents a remote site, and R3 represents the corporate headquarters. Host PC-A simulates an employee connecting from home or a small office over the Internet. Router R2 simulates an Internet ISP router and acts as a passthrough with no knowledge of the VPN connection running through it.

Note: The router commands and output in this lab are from a Cisco 1841 with Cisco IOS Release 12.4(20)T (Advanced IP image). Other routers and Cisco IOS versions can be used. See the Router Interface Summary table at the end of the lab to determine which interface identifiers to use based on the equipment in the lab. Depending on the router model and Cisco IOS version, the commands available and output produced might vary from what is shown in this lab.

Note: Make sure that the routers and the switches have been erased and have no startup configurations.

Required Resources

- 3 routers with Cisco 1841 with Cisco IOS Release 12.4(20)T1 or comparable (2 routers with SDM 2.5 installed)
- 2 switches (Cisco 2960 or comparable)

- PC-A - Windows XP or Vista (with Cisco VPN Client)
- PC-C (Windows XP or Vista)
- Serial and Ethernet cables as shown in the topology
- Rollover cables to configure the routers via the console

Part 1. Basic Router Configuration

In Part 1, you set up the network topology and configure basic settings, such as the interface IP addresses and static routing. Perform the steps on the routers as indicated.

Step 1: Cable the network as shown in the topology.

Attach the devices shown in the topology diagram, and cable as necessary.

Step 2: Configure basic settings for all routers.

a. Configure host names as shown in the topology.

b. Configure the physical interface IP addresses as shown in the IP addressing table.

c. Configure a clock rate for the routers with a DCE serial cable attached to their serial interface.

```
R1(config)#interface S0/0/0
R1(config-if)#clock rate 64000
```

d. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

```
R1(config)#no ip domain-lookup
```

Step 3: Configure static default routes on R1 and R3.

Configure a static default route from R1 to R2 and from R3 to R2.

```
R1(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.2

R3(config)#ip route 0.0.0.0 0.0.0.0 10.2.2.2
```

Step 4: Configure static routes on R2.

Configure a static route from R2 to the R1 LAN.

```
R2(config)#ip route 192.168.1.0 255.255.255.0 10.1.1.1
```

Configure a static route from R2 to the R3 LAN.

```
R2(config)#ip route 192.168.3.0 255.255.255.0 10.2.2.1
```

Step 5: Configure PC host IP settings.

Configure a static IP address, subnet mask, and default gateway for PC-A and PC-C, as shown in the IP addressing table.

Step 6: Verify connectivity between PC-A and R3.

From PC-A, ping the R3 S0/0/1 interface at IP address 10.2.2.1.

```
PC-A:\>ping 10.2.2.1
```

Are the results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Step 7: Configure a minimum password length.

Note: Passwords in this lab are set to a minimum of 10 characters, but are relatively simple for the benefit of performing the lab. More complex passwords are recommended in a production network.

Use the **security passwords** command to set a minimum password length of 10 characters.

```
R1(config)#security passwords min-length 10
```

Step 8: Configure the enable secret password and console and vty lines.

a. Configure the enable secret password **cisco12345** on R1.

```
R1(config)#enable secret cisco12345
```

b. Configure a console password and enable login for router R1. For additional security, the **exec-timeout** command causes the line to log out after 5 minutes of inactivity. The **logging synchronous** command prevents console messages from interrupting command entry.

Note: To avoid repetitive logins during this lab, the **exec-timeout** can be set to 0 0, which prevents it from expiring. However, this is not considered a good security practice.

```
R1(config)#line console 0
R1(config-line)#password ciscoconpass
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
R1(config-line)#logging synchronous
```

c. Configure the password on the vty lines for router R1.

```
R1(config)#line vty 0 4
R1(config-line)#password ciscovtypass
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
```

d. Repeat these configurations on R2 and R3.

Step 9: Encrypt clear text passwords.

a. Use the **service password-encryption** command to encrypt the console, aux, and vty passwords.

```
R1(config)#service password-encryption
```

b. Issue the **show run** command. Can you read the console, aux, and vty passwords? Why or why not?

_____

c. Repeat this configuration on R2 and R3.

Step 10: Configure a login warning banner on routers R1 and R3.

Configure a warning to unauthorized users with a message-of-the-day (MOTD) banner.

```
R1(config)#banner motd $Unauthorized access strictly prohibited and
prosecuted to the full extent of the law$
```

Step 11: Save the basic running configuration for all three routers.

Save the running configuration to the startup configuration from the privileged EXEC prompt.

```
R1#copy running-config startup-config
```

Part 2. Configuring a Remote Access VPN

In Part 2 of this lab, you configure a firewall and a remote access IPsec VPN. R3 is configured as a VPN server using SDM, and PC-A is configured as a Cisco VPN Client.

Task 1. Prepare R3 for SDM Access

Step 1: Configure HTTP router access and a AAA user prior to starting SDM.

a. Enable the HTTP server on R3.

```
R3(config)#ip http server
```

Note: For added security, you can enable the HTTP secure server on R3 using the **ip http secure-server** command. The HTTP server and the HTTP secure server are disabled by default.

b. Create an admin01 account on R3 with privilege level 15 and a password of admin01pass for use with AAA.

```
R3(config)#username admin01 privilege 15 password 0 admin01pass
```

Step 2: Access SDM and set command delivery preferences.

a. Run the SDM application or open a browser on PC-C. Start SDM by entering the R3 Fa0/1 IP address **192.168.3.1** in the address field.

b. Log in with no username and the enable secret password **cisco12345**.

c. In the Authentication Required dialog box, enter **cisco12345** in the **Password** field and click **OK**.

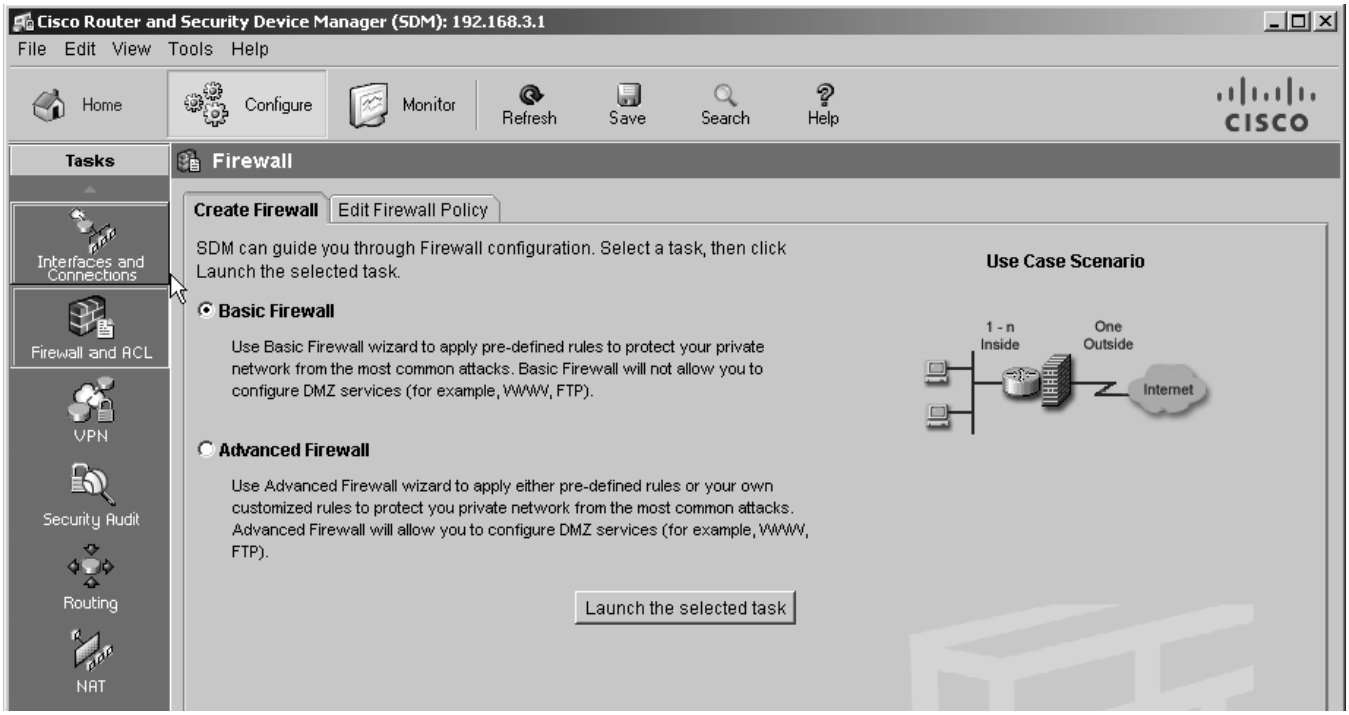
d. If the IOS IPS Login dialog box appears, enter the enable secret password **cisco12345**.

e. Select **Edit** > **Preferences** to allow you to preview the commands before sending them to the router. In the User Preferences window, check the **Preview commands before delivering to router** check box and click **OK**.

Task 2. Configure a ZBF Firewall on R3

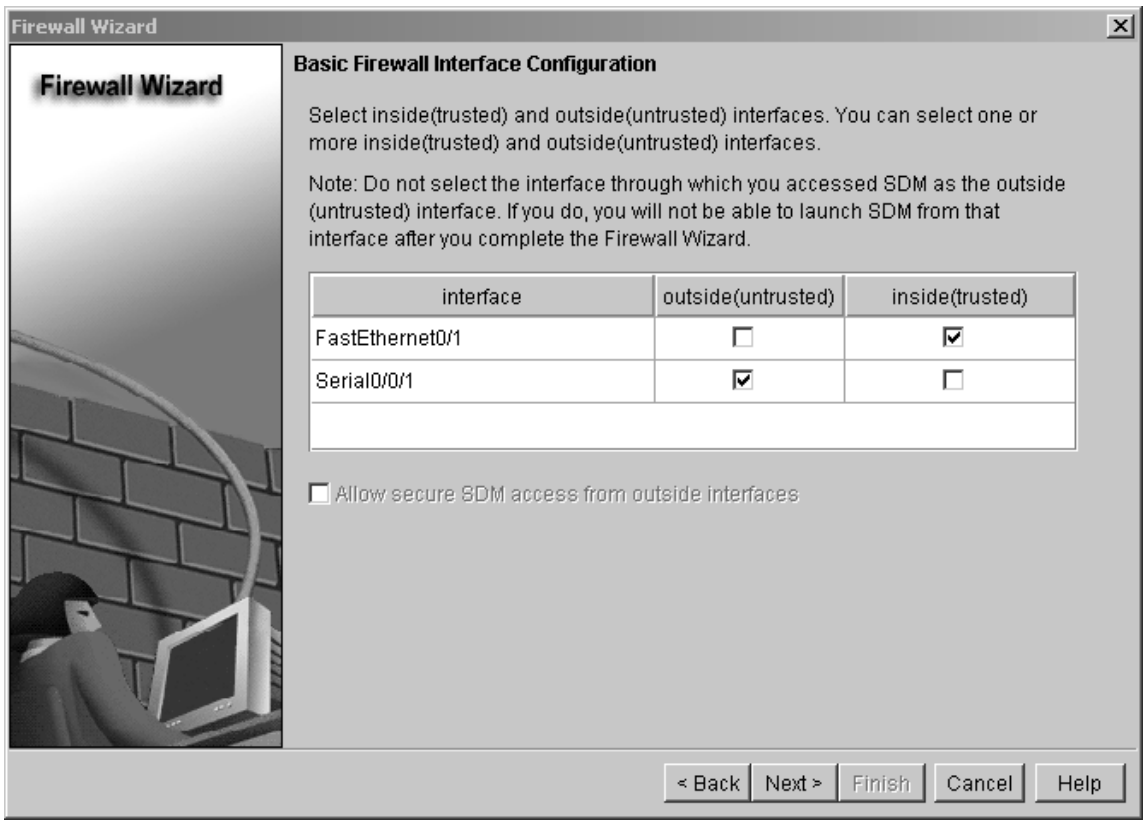
Step 1: Use the SDM Firewall Wizard to configure a zone-based firewall (ZBF) on R3.

a. Click the **Configure** button at the top of the SDM screen, and then click **Firewall and ACL.**



b. Select **Basic Firewall** and click the **Launch the selected task** button. On the Basic Firewall Configuration wizard screen, click **Next**.

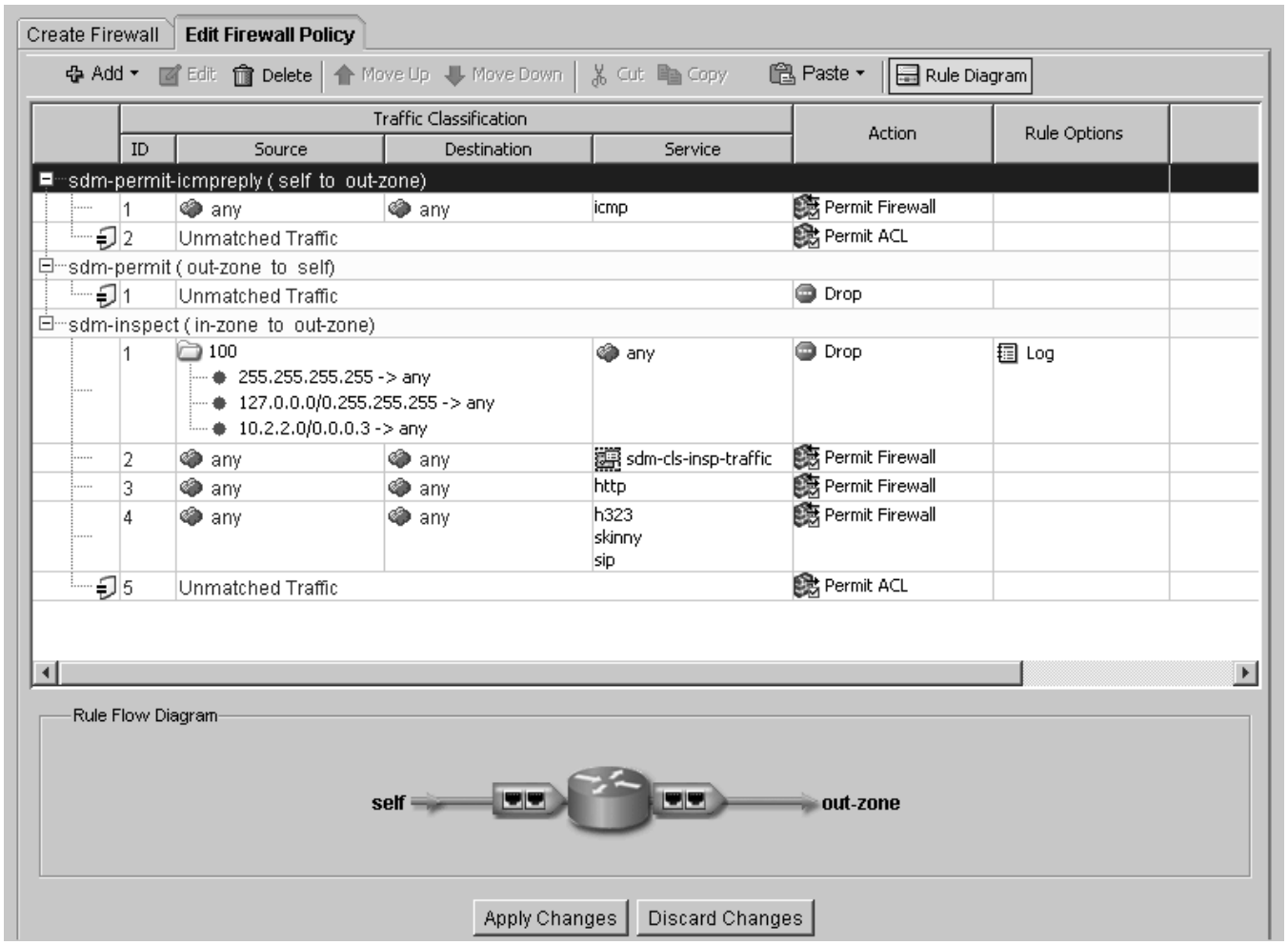
c. Check the **Inside (trusted)** check box fo**r FastEthernet0/1** and the **Outside (untrusted)** check box fo**r Serial0/0/1.** Click **Next**. Click **OK** when the SDM launch warning for Serial0/0/1 is displayed.



d. In the next window, select **Low Security** for the security level and click **Next**.

e. In the Summary window, click **Finish**.

f. Click **Deliver** to send the commands to the router. Click **OK** in the Commands Delivery Status window. Click **OK** on the Information window. You are returned to the Edit Firewall Policy tab as follows.



Step 2: Verify firewall functionality.

a. From PC-C, ping the R2 interface S0/0/1 at IP address 10.2.2.2.

Are the pings successful? Why or why not?

_____

b. From external router R2, ping PC-C at IP address 192.168.3.3

Are the pings successful? Why or why not?

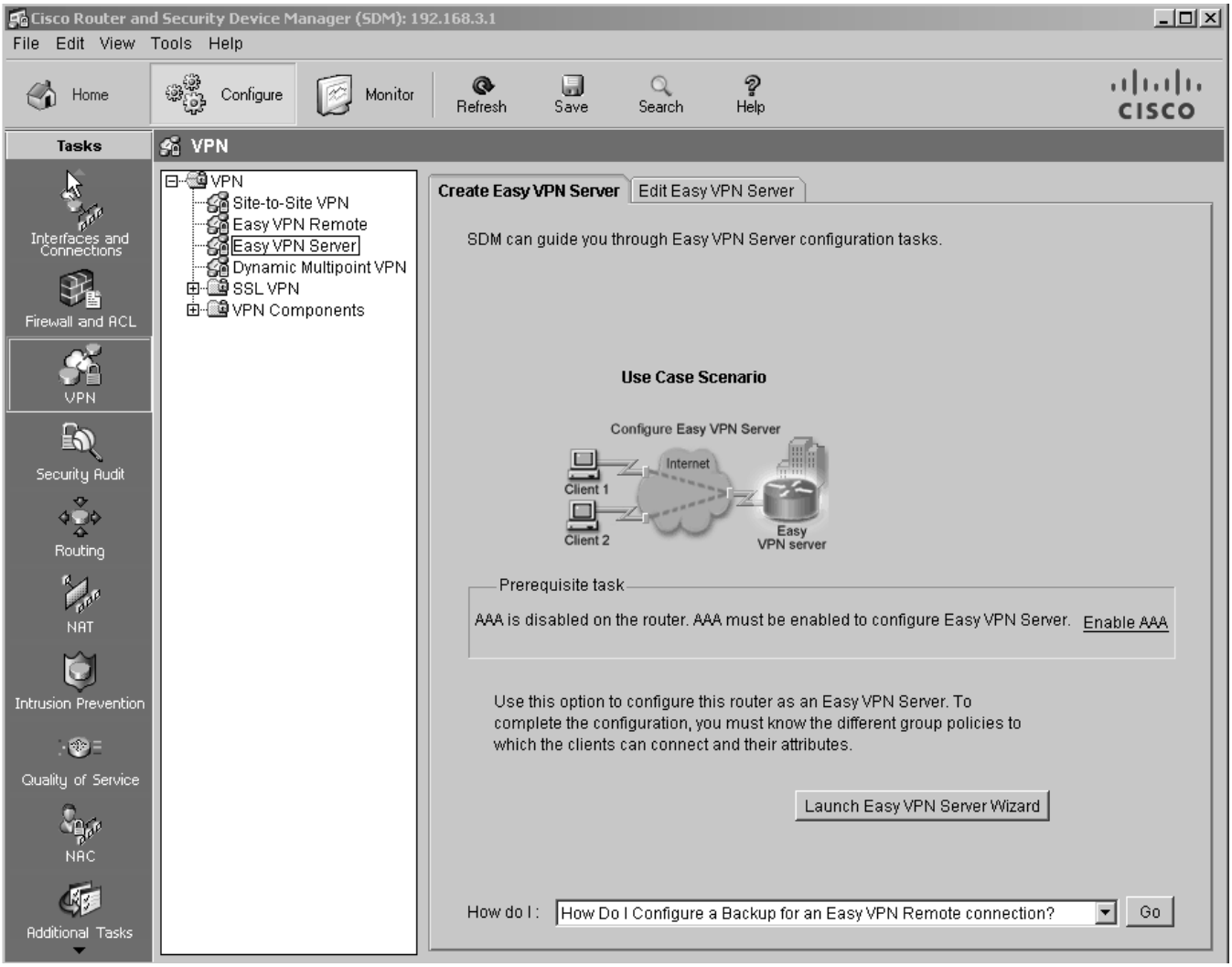
_____

Task 3. Use the SDM VPN Wizard to Configure the Easy VPN Server

Step 1: Launch the Easy VPN Server wizard and configure AAA services.

a. Click the **Configure** button at the top of the SDM home screen. Click the **VPN** task button to view the VPN configuration page.

b. Select **Easy VPN Server** from the main VPN window, and then click **Launch Easy VPN Server Wizard**.



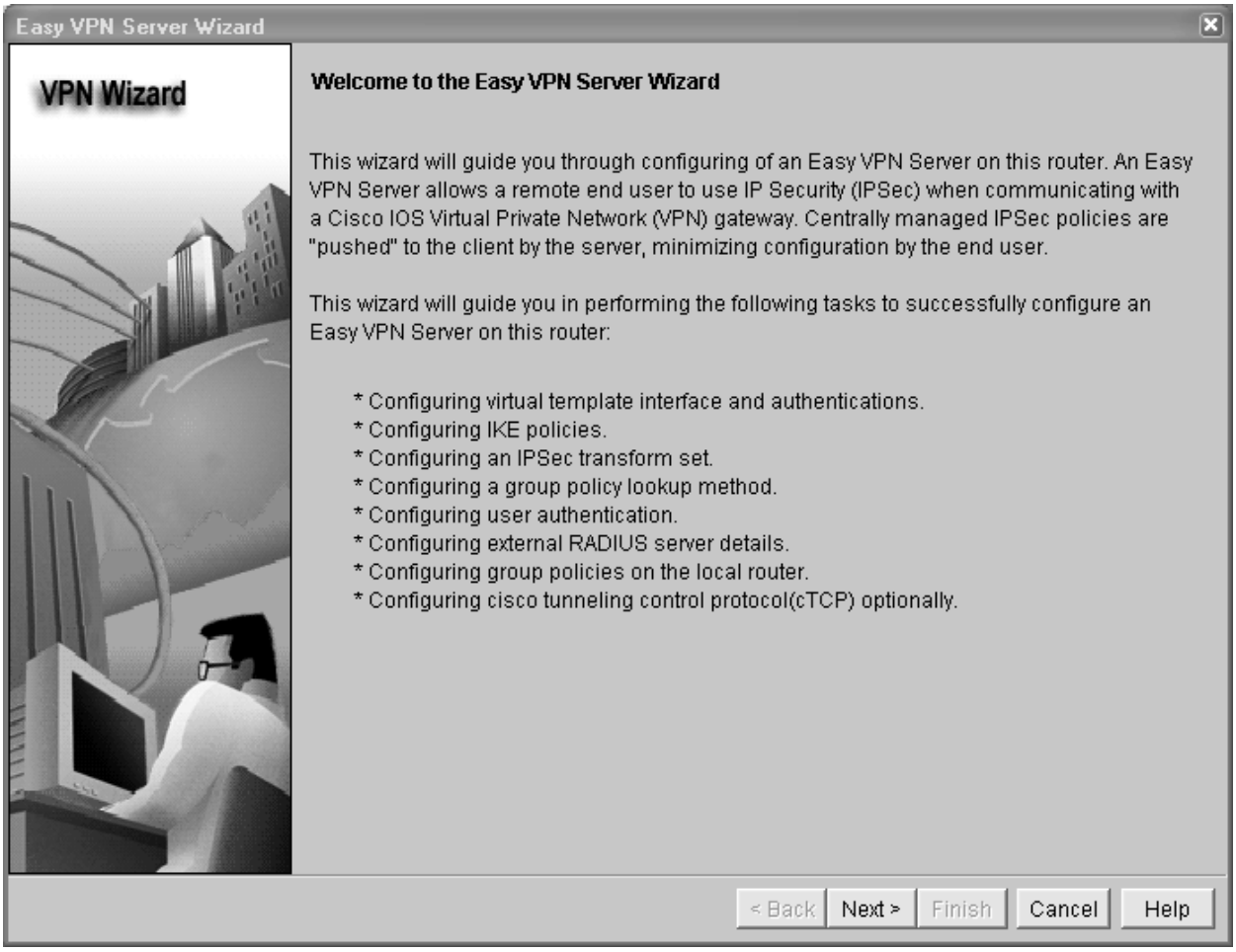
c. The Easy VPN Server wizard checks the router configuration to see if AAA is enabled. If AAA is not enabled, the Enable AAA window displays. AAA must be enabled on the router before the Easy VPN Server configuration starts. Click **Yes** to continue with the configuration.

d. When prompted to deliver the configuration to the router, click **Deliver**.

e. In the Command Delivery Status window, click **OK**. When the message “AAA has been successfully enabled on the router” displays, click **OK**.

f. When returned to the Easy VPN Server wizard window, click **Next**.

g. Now that AAA is enabled, you can start the Easy VPN Server wizard by clicking the **Launch Easy VPN Server Wizard** button. Read through the descriptions of the tasks that the wizard guides you through.



How does the client receive the IPsec policies? _____

How does the Easy VPN remote server configuration differ from the site-to-site?

_____

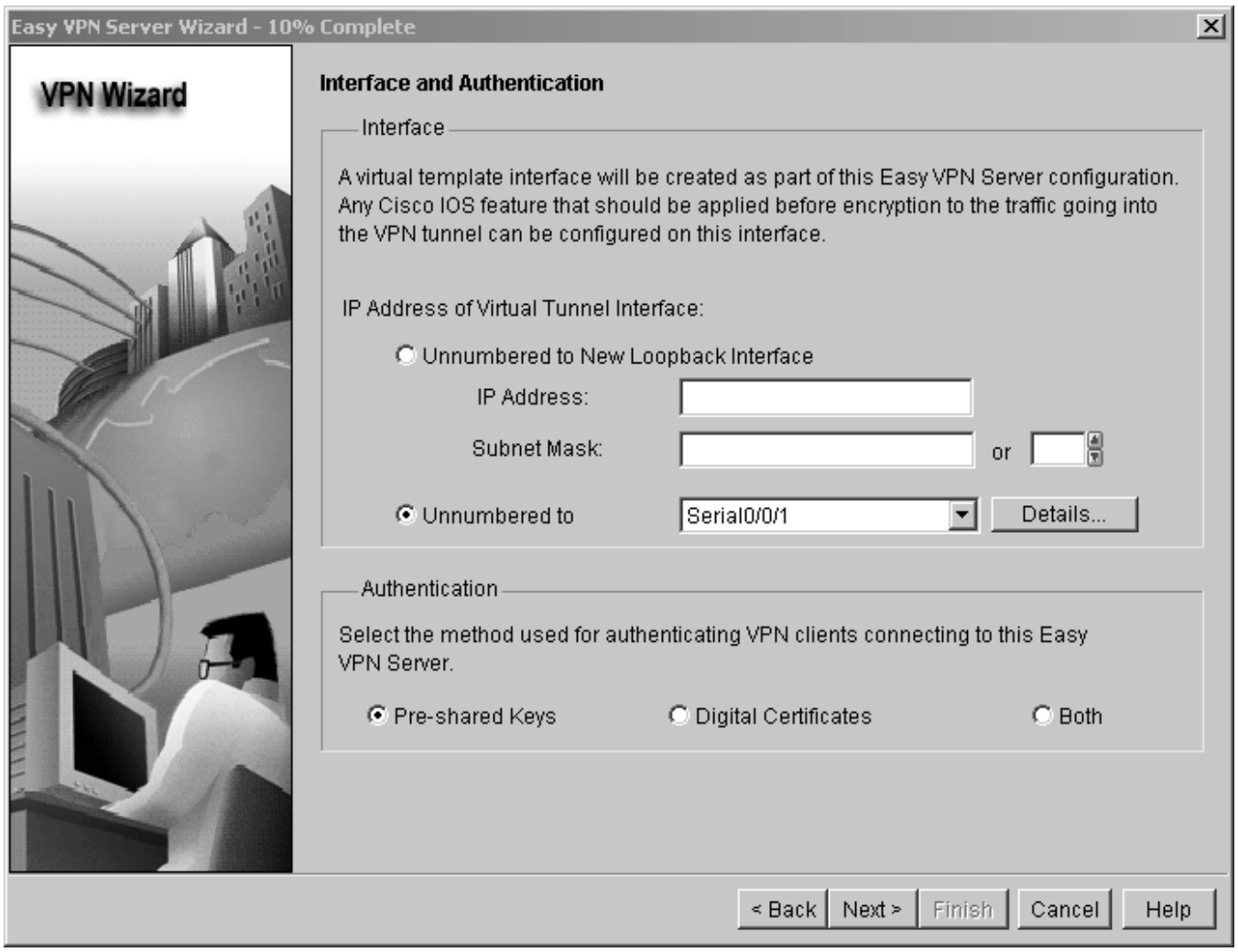
_____

h. Click **Next** when you are finished answering the above questions.

Step 2: Configure the virtual tunnel interface and authentication.

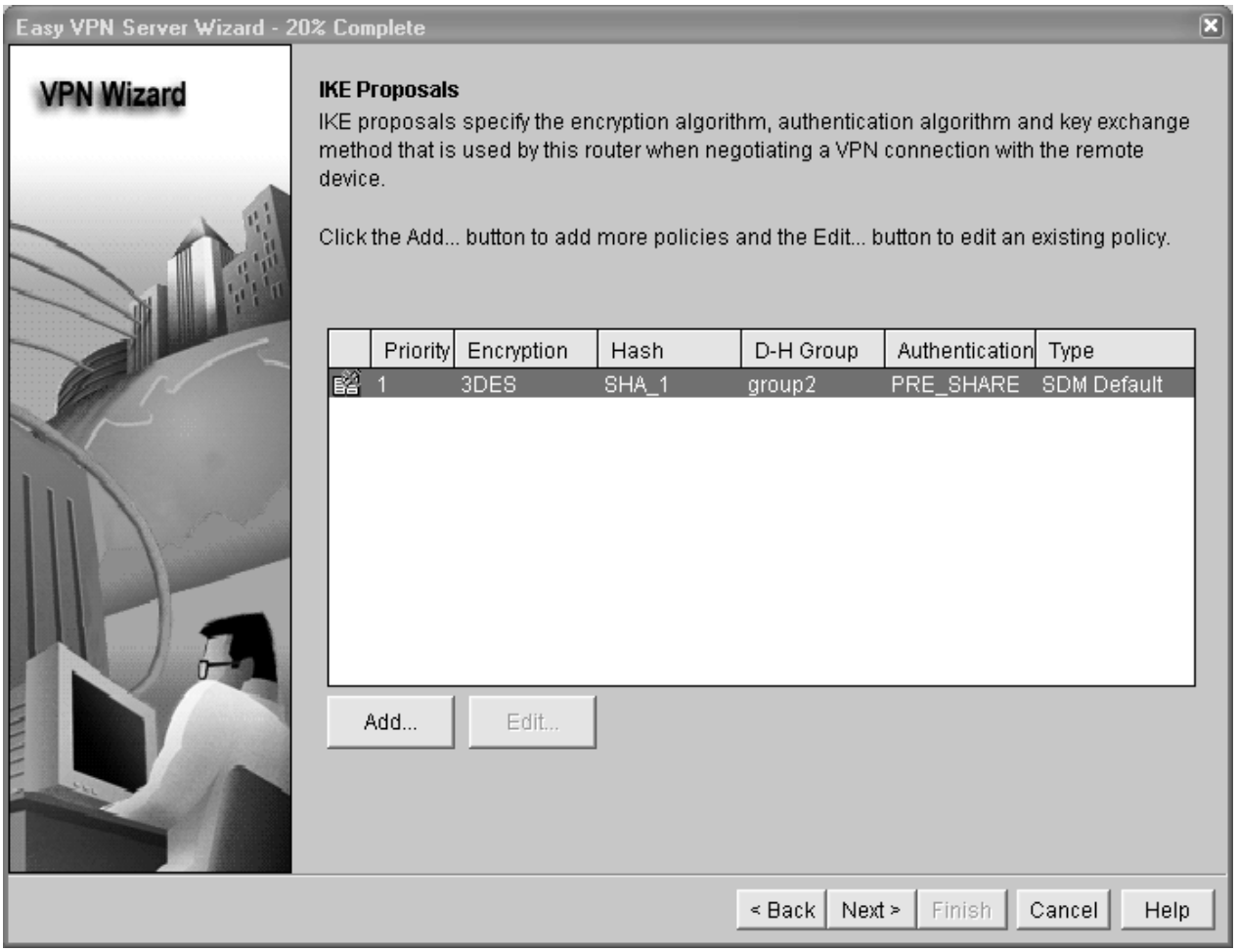
a. Select the interface on which the client connections terminate. Click the **Unnumbered to** radio button and select the Serial0/0/1 interface from the pull-down menu.

b. Select **Pre-shared Keys** for the authentication type and click **Next** to continue.


Easy VPN Server Wizard - 10% Complete
VPN Wizard
Interface and Authentication
Interface
A virtual template interface will be created as part of this Easy VPN Server configuration. Any Cisco IOS feature that should be applied before encryption to the traffic going into the VPN tunnel can be configured on this interface.
IP Address of Virtual Tunnel Interface:
Unnumbered to New Loopback Interface
IP Address:
Subnet Mask:
or
Unnumbered to
Serial0/0/1
Details...
Authentication
Select the method used for authenticating VPN clients connecting to this Easy VPN Server.
Pre-shared Keys
Digital Certificates
Both
< Back
Next >
Finish
Cancel
Help

Step 3: Select an IKE proposal.

a. In the IKE Proposals window, the default IKE proposal is used for R3.



What is the encryption method used with the default IKE policy? _____

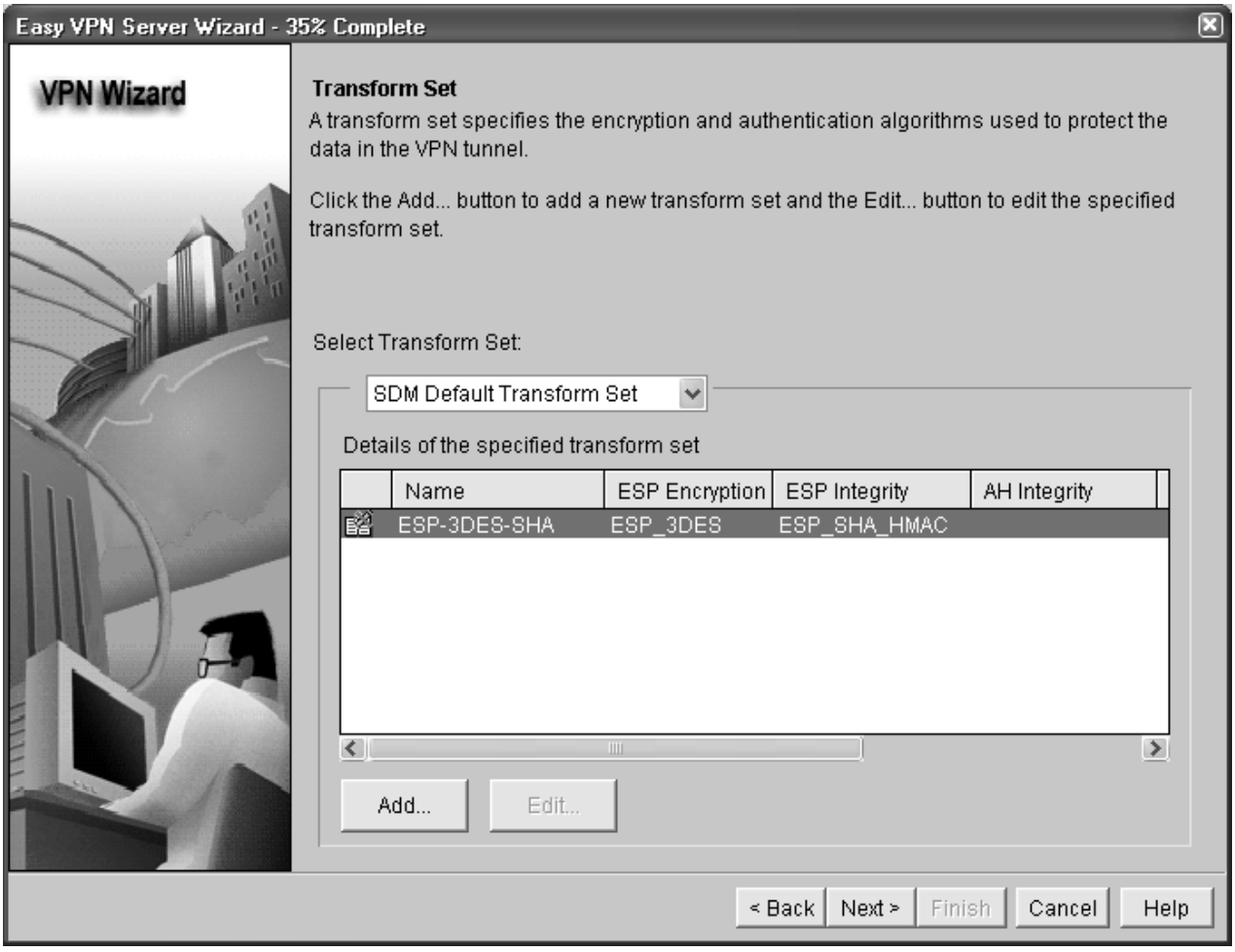
What is the hash algorithm used to ensure that the keys have not been tampered with? _____

b. Click **Next** to accept the default IKE policy.

Note: Configurations on both sides of the tunnel must match exactly. The Cisco VPN Client automatically selects the proper configuration for itself. Therefore, an IKE configuration is not necessary on the client PC.

Step 4: Select the transform set.

a. In the Transform Set window, the default SDM transform set is used. What ESP encryption method is used with the default transform set? _____



b. Click **Next** to accept the default transform set.

Step 5: Specify group authorization and group policy lookup.

a. In the Group Authorization and Group Policy Lookup window, select the **Local** option.

b. Click **Next** to create a new AAA method list for group policy lookup that uses the local router database.

Step 6: Configure user authentication (XAuth).

a. In the User Authentication (Xauth) window, you can specify to store user information on an external server, such as a RADIUS server or a local database, or both. Select the **Enable User Authentication** check box and accept the default of **Local Only**.

Where does the router look for valid user accounts and passwords to authenticate remote VPN users when they attempt to log in?

_____

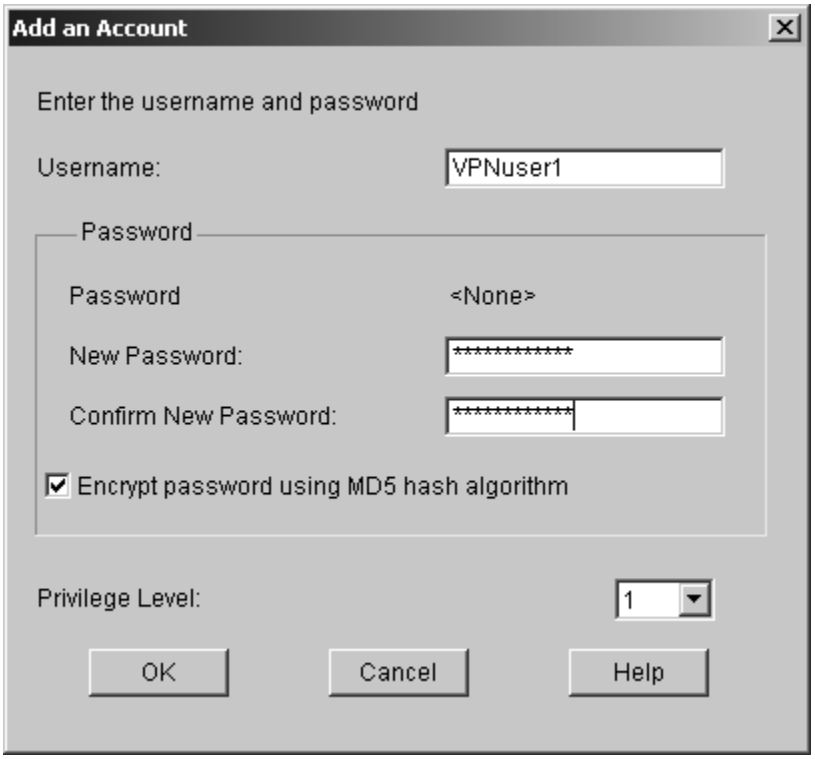
b. Click the **Add User Credentials** button. In the User Accounts window, you can view currently defined users or add new users.

What is the name of the user currently defined and what is the user privilege level? _____

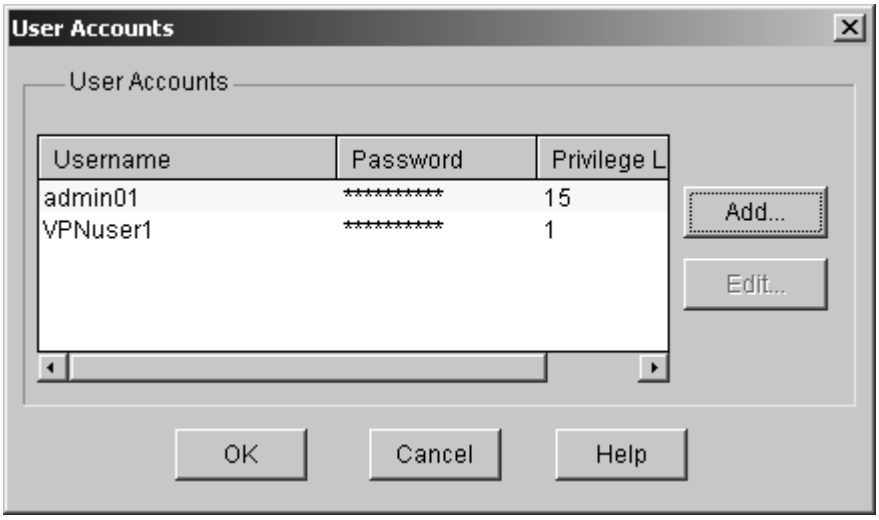
How was this user defined? _____

c. In the User Accounts window, click the **Add** button to add another user. Enter the username **VPNuser1** with a password of **VPNuser1pass**. Select the check box for encrypting the password using the MD5 hash algorithm. Leave the privilege level at 1.

What is the range of privilege level that can be set for a user? _____



d. Click **OK** to accept the VPNuser1 entries, and then click **OK** to close the User Accounts window.



e. In the User Authentication (XAuth) window, click **Next** to continue.

Step 7: Specify group authorization and user group policies.

In the Group Authorization and User Group Policies window, you must create at least one group policy for the VPN server.

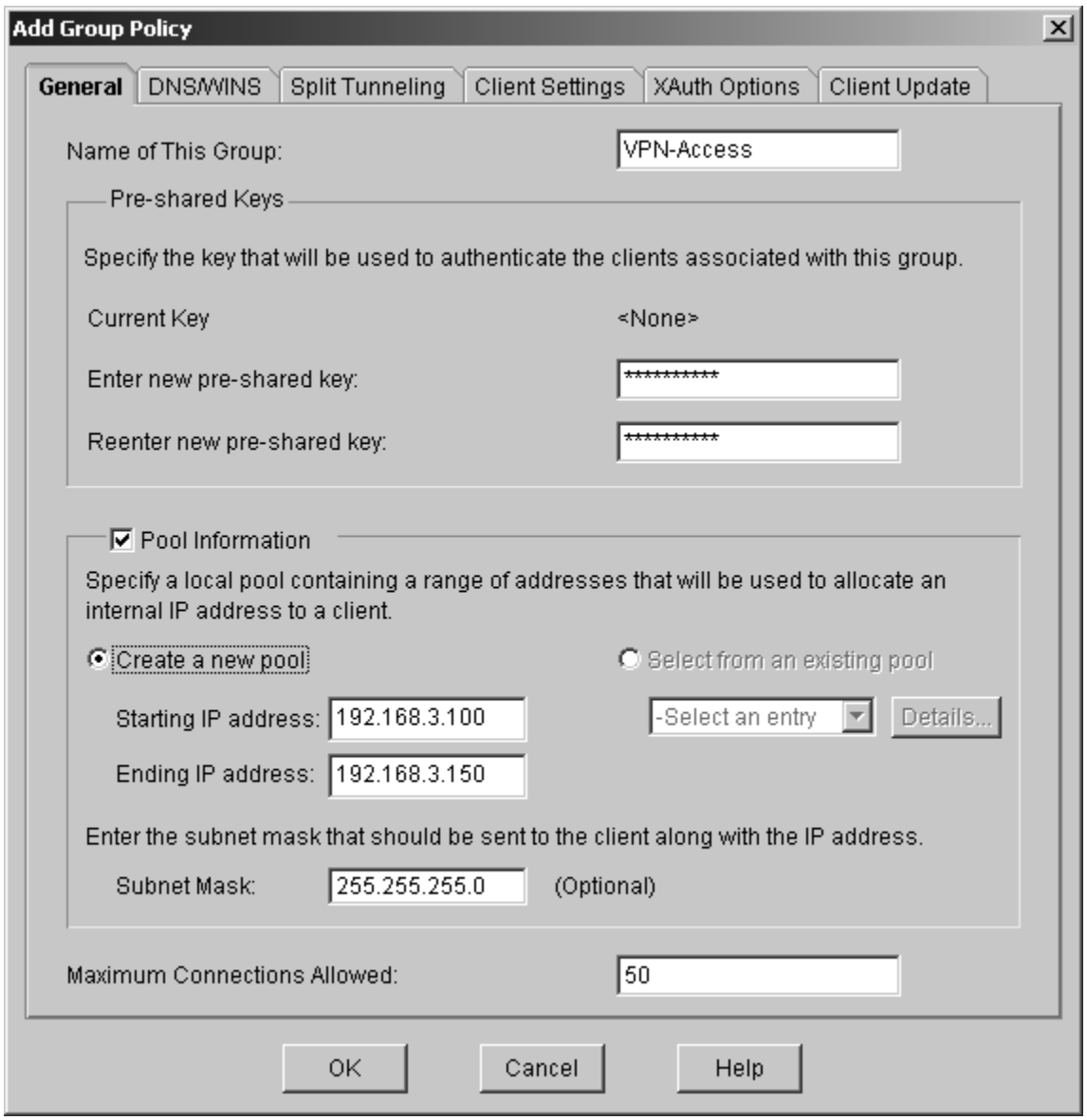
a. Click **Add** to create a group policy.

b. In the Add Group Policy window, enter **VPN-Access** as the name of this group. Enter a new pre-shared key of **cisco12345** and then re-enter it.

c. Leave the **Pool Information** box checked and enter a starting address of **192.168.3.100**, an ending address of **192.168.3.150**, and a subnet mask of **255.255.255.0**.

d. Enter **50** for the **Maximum Connections Allowed**.

e. Click **OK** to accept the entries.

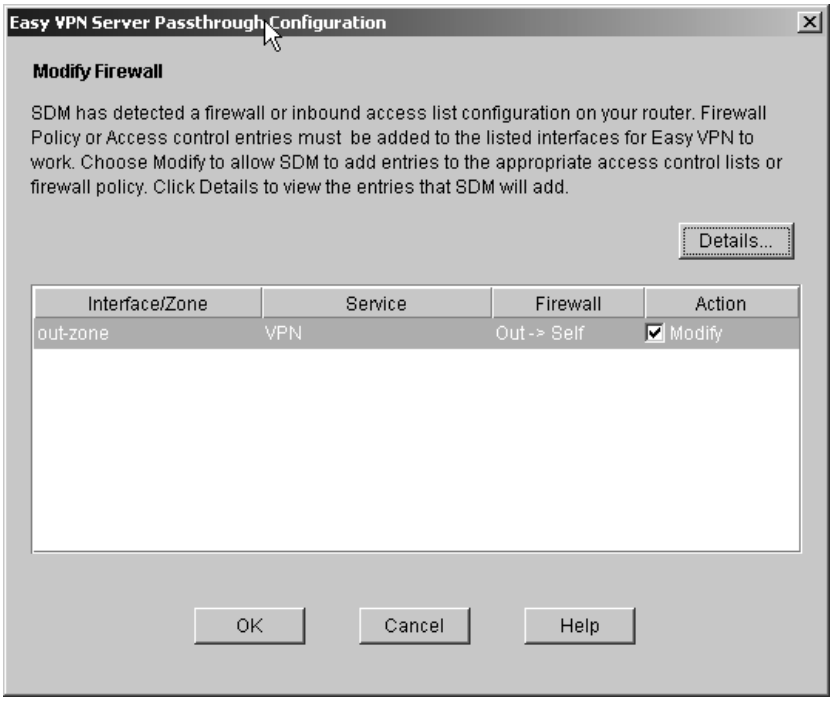


f. An SDM warning message displays indicating that the IP addresses in the pool and the IP address of the FastEthernet0/1 interface are in the same subnet. Click **Yes** to continue.

g. When you return to the Group Authorization window, check the **Configure Idle Timer** check box and enter one hour (**1**). This disconnects idle users if there is no activity for one hour and allows others to connect. Click **Next** to continue.

h. When the Cisco Tunneling Control Protocol (cTCP) window displays, do not enable cTCP. Click **Next** to continue.

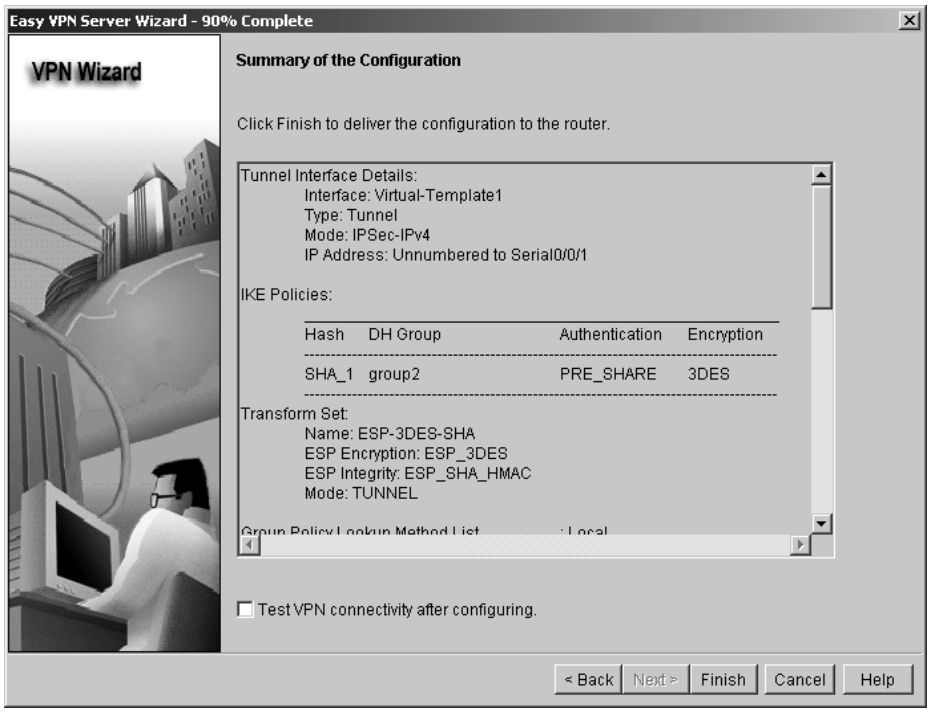
i. When the Easy VPN Server Passthrough Configuration window displays, make sure that the **Action Modify** check box is checked. This option allows SDM to modify the firewall on S0/0/1 to allow IPsec VPN traffic to reach the internal LAN. Click **OK** to continue.



Step 8: Review the configuration summary and deliver the commands.

a. Scroll through the commands that SDM will send to the router. Do not check the check box to test the VPN. Click **Finish**.

b. When prompted to deliver the configuration to the router, click **Deliver**.



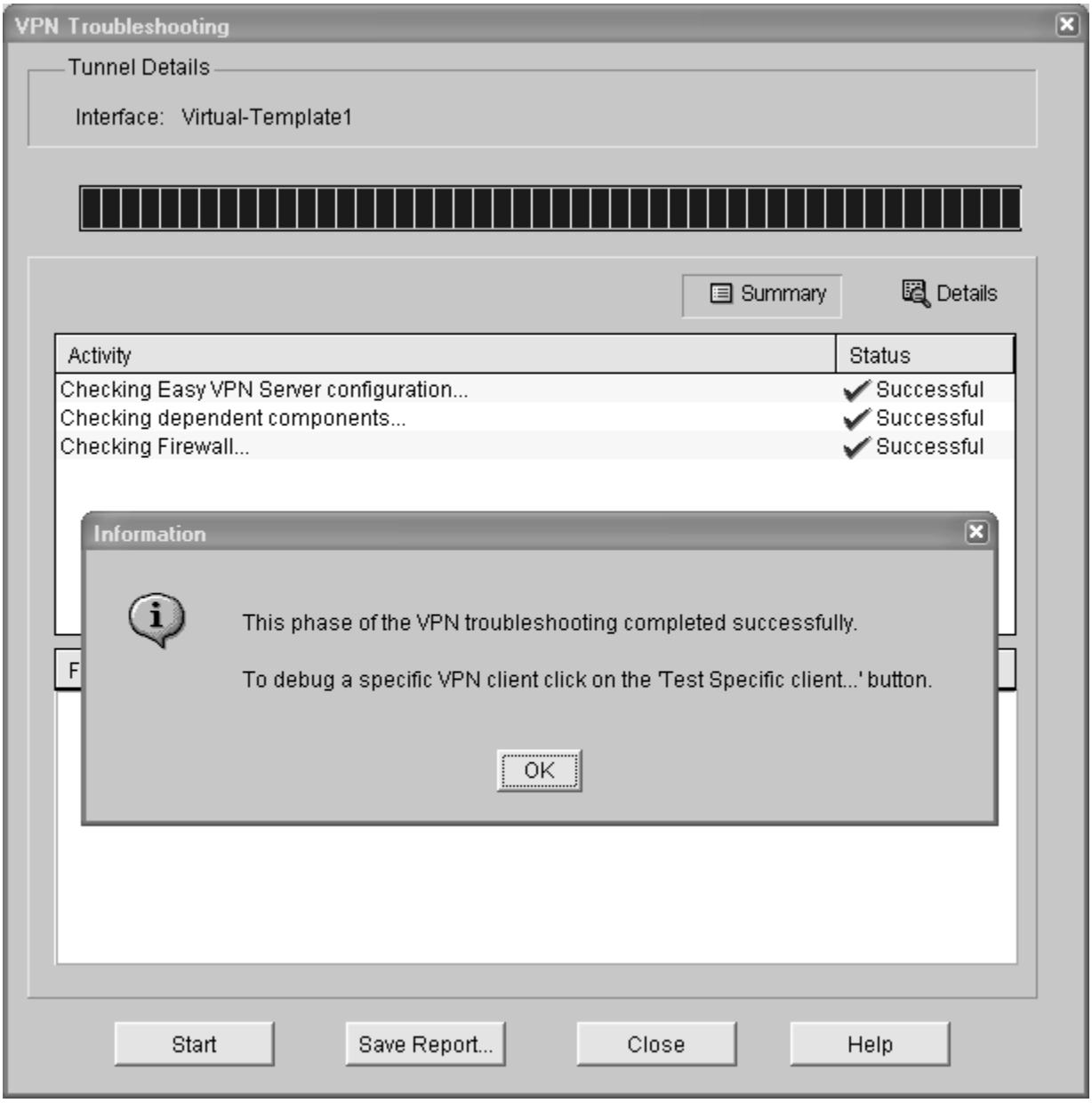
c. In the Command Delivery Status window, click **OK**. How many commands are delivered? _____

Step 9: Test the VPN Server.

a. You are returned to the main VPN window with the **Edit Easy VPN Server** tab selected. Click the **Test VPN Server** button in the lower right corner of the screen.

b. In the VPN Troubleshooting window, click the **Start** button.

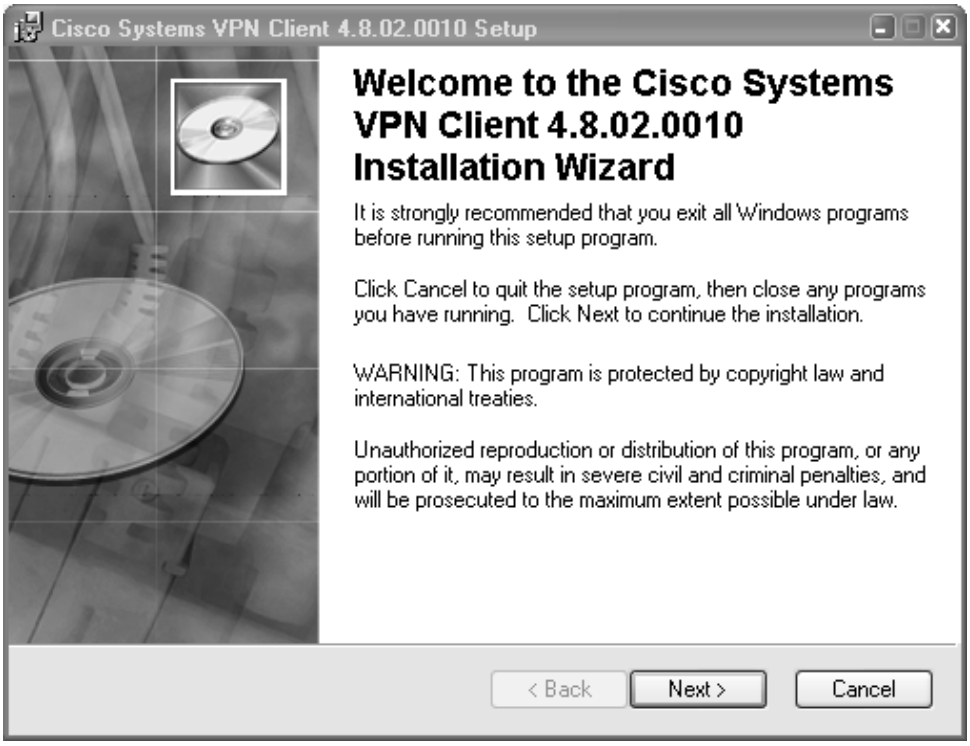
c. Your screen should look similar to the one below. Click **OK** to close the information window. Click **Close** to exit the VPN Troubleshooting window.



Task 4. Use the Cisco VPN Client to Test the Remote Access VPN

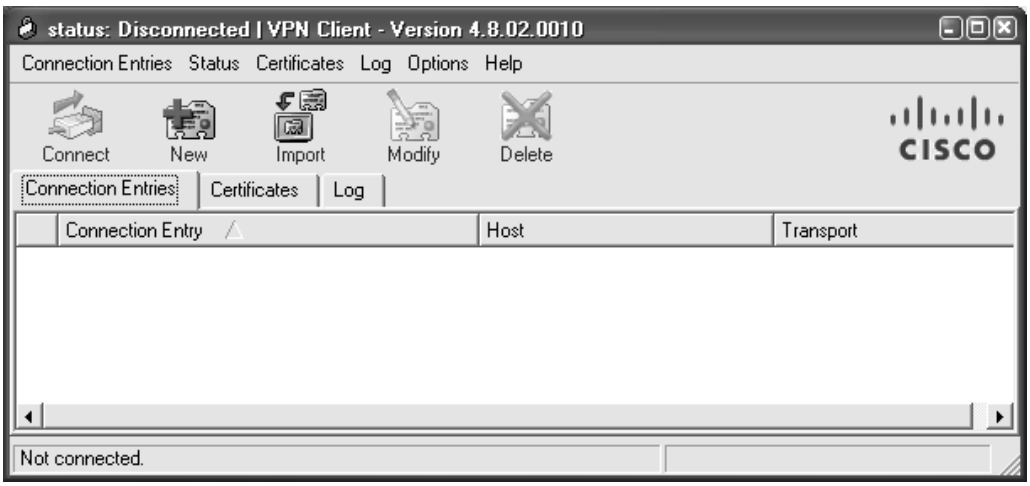
Step 1: (Optional) Install the Cisco VPN client.

If the Cisco VPN Client software on host PC-A is not installed, install it now. If you do not have the Cisco VPN Client software, contact your instructor.



Step 2: Configure PC-A as a VPN client to access the R1 VPN server.

a. Start the Cisco VPN Client and select **Connection Entries > New,** or click the **New** icon with the red plus sign (+) on it.



b. Enter the following information to define the new connection entry. Click **Save** when you are finished.

Connection Entry: **VPN-R3**

Description: **Connection to R3 internal network**

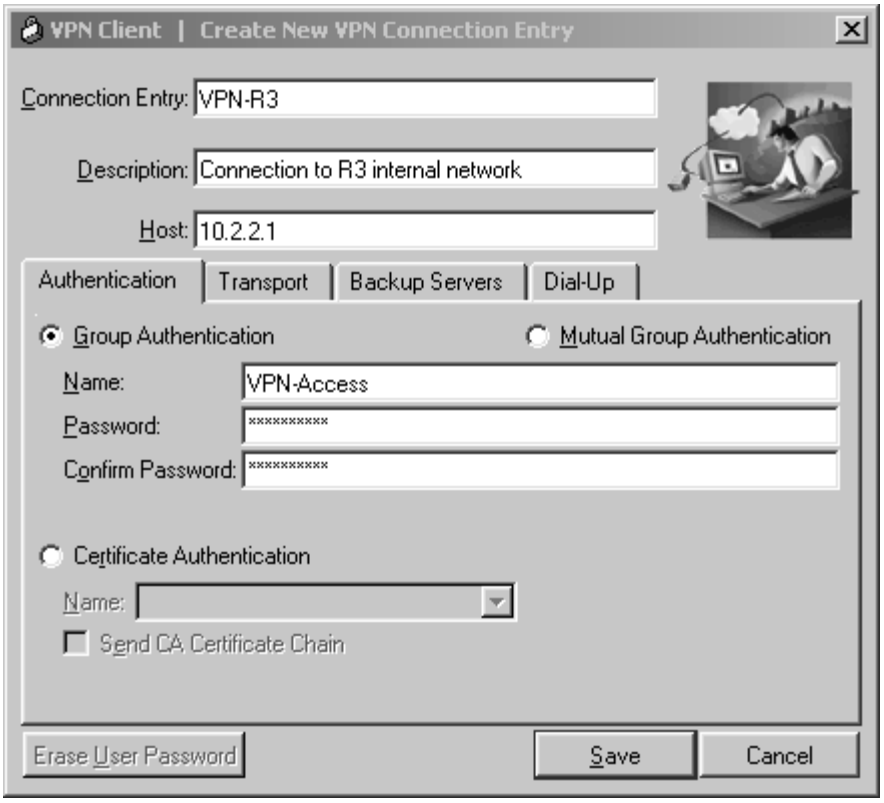
Host: **10.2.2.1** (IP address of the R3 S0/0/1 interface)

Group Authentication Name: **VPN-Access** (defines the address pool configured in Task 2)

Password: **cisco12345** (pre-shared key configured in Task 2)

Confirm Password: **cisco12345**

Note: The group authentication name and password are case-sensitive and must match the ones created on the VPN Server.



Step 3: Test access from PC-A without a VPN connection.

In the previous step, you created a VPN connection entry on the VPN client computer PC-A but have not activated it, so the VPN tunnel is not yet up.

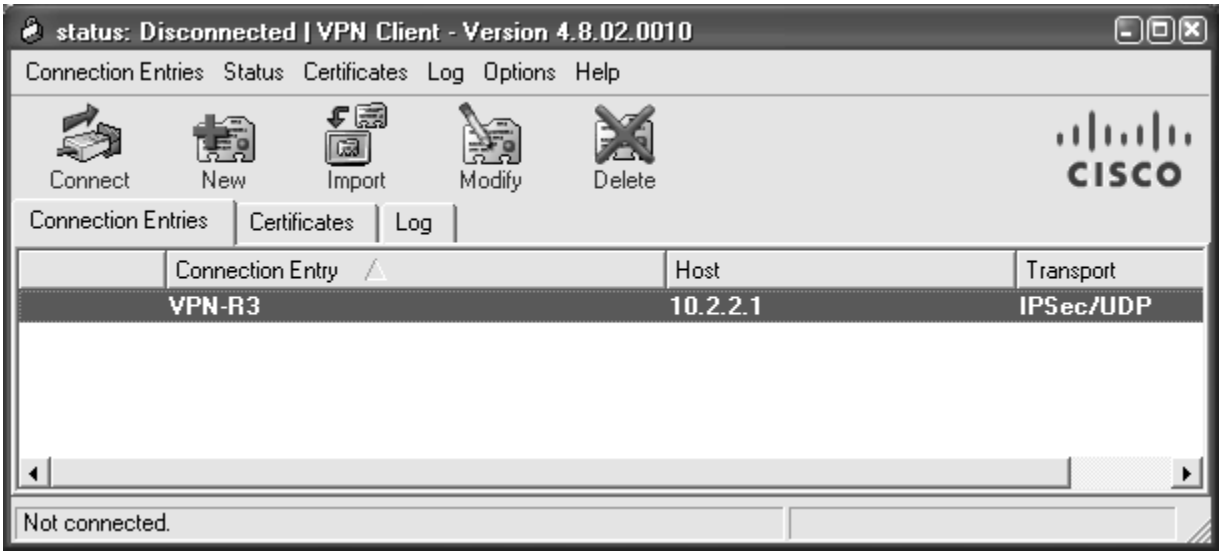
Open a command prompt on PC-A and ping the PC-C IP address at 192.168.3.3 on the R3 LAN. Are the pings successful? Why or why not?

_____

_____

Step 4: Establish a VPN connection and log in.

a. Select the newly created connection VPN-R3 and click the **Connect** icon. You can also double-click the connection entry.



b. Enter the previously created username **VPNuser1** in the VPN Client User Authentication dialog box and enter the password **VPNuser1pass**. Click **OK** to continue. The VPN Client window minimizes to a lock icon in the tools tray of the taskbar. When the lock is closed, the VPN tunnel is up. When it is open, the VPN connection is down.

Task 5. Verify the VPN Tunnel Between the Client, Server, and Internal Network

Step 1: Open the VPN Client icon.

a. Double-click the VPN lock icon to expand the VPN Client window.

What does it say about the connection status at the top of the window? _____

b. From the PC-A command line, issue the **`ipconfig`** command.

What is the IP address of the first Local Area Connection? _____

What is the IP address of Local Area Connection 2? _____

Step 2: Close the VPN connection and reopen it.

a. Click the **Disconnect** icon in the VPN Client window to close the VPN-R3 connection.

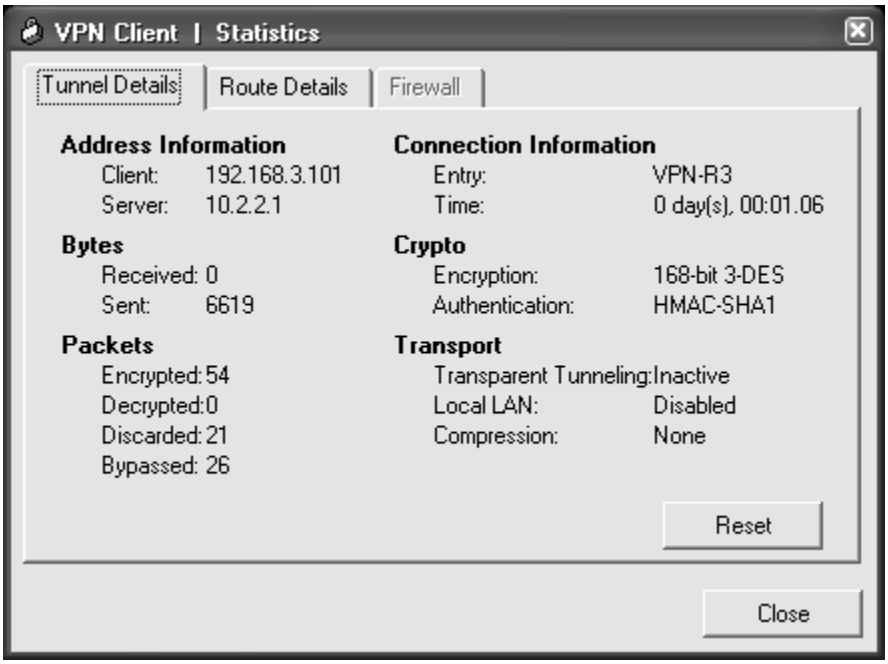
b. Click the **Connect** icon and log in again as VPNuser1.

What is the IP address of Local Area Connection 2 now? _____

Note: Each time you disconnect and reconnect to the VPN server, you receive a new IP address until the limit is reached.

Step 3: Check the tunnel statistics.

a. Select **Status** > **Statistics**. Click the **Tunnel Details** tab.



b. What is the current address obtained from the R3 VPN server and what is the range of addresses that can be assigned?

_____

What is the VPN server address? _____

How many packets have been encrypted? _____

What is the encryption method? _____

What is the authentication method? _____

c. Leave the VPN Client Statistics window open.

Step 4: Test access from the client PC-A using the VPN connection.

With the VPN connection from computer PC-A to router R3 activated, open a command prompt on PC-A and ping the PC-C IP address at 192.168.3.3 on the R3 LAN. Are the pings successful? Why or why not? _____

How many packets have now been encrypted? _____

Step 5: Check the Cisco IOS message on R3 when the tunnel is created.

Open the console connection for R3 and locate the message displayed indicating that the virtual interface came up when the VPN Client connection was made.

What is the name of the interface on R3 that is activated for the VPN? _____

Step 6: Verify the VPN connection information for PC-A.

From the PC-A command prompt, issue the **`ipconfig /all`** command to see the network connections.

a. What is the configuration for the first Local Area Connection?

IP Address: _____
Subnet Mask: _____
Default Gateway: _____
Description: _____

b. What is the configuration for Local Area Connection 2?

IP Address: _____
Subnet Mask: _____
Default Gateway: _____
Description: _____

Step 7: Telnet from PC-A to R3.

From the PC-A command prompt, telnet to R3 at the Fa0/1 IP address 192.168.3.1. Log in as admin01 with a password of admin01pass. What is the router command prompt and why is this?

_____

a. Issue the **`show run`** command to view the various commands generated by SDM to configure the VPN Server.

b. Issue the **`show users`** command to see connections to router R3. What connections are present?

_____

c. Close the Telnet connection using the **`quit`** or **`exit`** command.

Task 6. Reflection

Why is VPN a good option for remote users?

_____

Router Interface Summary Table

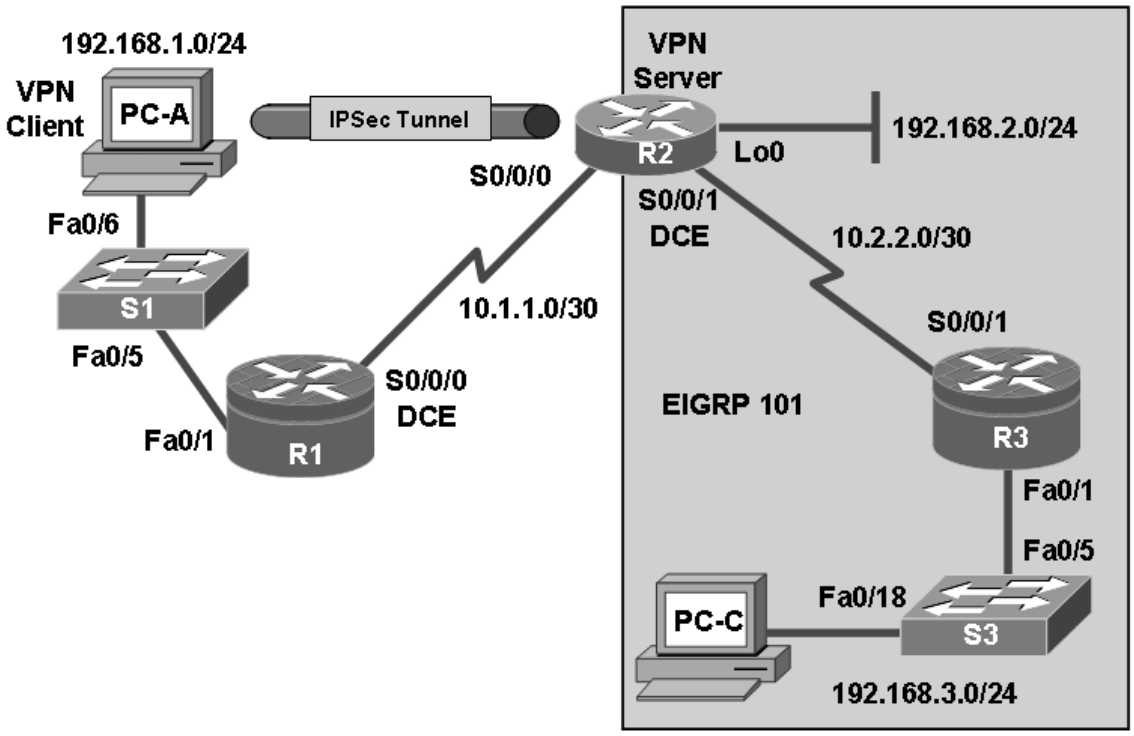
Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1700	Fast Ethernet 0 (FA0)	Fast Ethernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2600	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)

Router Interface Summary				
2800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Chapter 8: Lab C (Optional): Configuring a Remote Access VPN Server and Client

Topology



IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	FA0/1	192.168.1.1	255.255.255.0	N/A	S1 FA0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
	Loopback 0	192.168.2.1	255.255.255.0	N/A	N/A
R3	FA0/1	192.168.3.1	255.255.255.0	N/A	S3 FA0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 FA0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 FA0/18

Objectives

Part 1: Basic Router Configuration

- Configure host names, interface IP addresses, and access passwords.

- Configure the EIGRP dynamic routing protocol on R2 and R3.

Part 2: Configuring a Remote Access VPN

- Configure a router to support an Easy VPN server using SDM.
- Configure the Cisco VPN client on PC-A and connect to R2.
- Verify the configuration.
- Test VPN functionality.

Background

VPNs can provide a secure method of transmitting data over a public network, such as the Internet. A common VPN implementation is used for remote access to a corporate office from a telecommuter location such as a small office or home office (SOHO).

In this lab, you build a multi-router network and configure the routers and hosts. You configure a remote access IPsec VPN between a client computer and a simulated corporate network. You use SDM to configure a Cisco Easy VPN server on the corporate edge gateway router and configure the Cisco VPN client on a host. You then connect to the corporate network through a simulated ISP router.

The Cisco VPN client allows organizations to establish end-to-end, encrypted (Ipsec) VPN tunnels for secure connectivity for mobile employees or teleworkers. It supports Cisco Easy VPN, which allows the client to receive security policies upon a VPN tunnel connection from the central site VPN device (Cisco Easy VPN Server), minimizing configuration requirements at the remote location. This is a scalable solution for remote access deployments where it is impractical to individually configure policies for multiple remote PCs.

Note: The router commands and output in this lab are from a Cisco 1841 with Cisco IOS Release 12.4(20)T (Advanced IP image). Other routers and Cisco IOS versions can be used. See the Router Interface Summary table at the end of the lab to determine which interface identifiers to use based on the equipment in the lab. Depending on the router model and Cisco IOS version, the commands available and output produced might vary from what is shown in this lab.

Note: Make sure that the routers and the switches have been erased and have no startup configurations.

Required Resources

- 3 routers with SDM 2.5 installed (Cisco 1841 with Cisco IOS Release 12.4(20)T1 or comparable)

Note: This lab requires that R2 have a comparable IOS and hardware characteristics to R1 and R2 in order for it to play the role of the VPN server.

- 2 switches (Cisco 2960 or comparable)
- PC-A (Windows XP or Vista, with Cisco VPN Client)
- PC-C (Windows XP or Vista)
- Serial and Ethernet cables as shown in the topology
- Rollover cables to configure the routers via the console

Part 1. Basic Router Configuration

In Part 1 of this lab, you set up the network topology and configure basic settings, such as the interface IP addresses, dynamic routing, device access, and passwords.

Note: Perform all tasks on routers R1, R2, and R3. The procedure for R1 is shown here as an example.

Step 1: Cable the network as shown in the topology.

Attach the devices shown in the topology diagram, and cable as necessary.

Step 2: Configure basic settings for each router.

a. Configure host names as shown in the topology.

b. Configure the physical interface IP addresses as shown in the IP addressing table.

c. Configure the logical loopback 0 interface on R2. This simulates the network from which the remote access clients receive addresses (192.168.2.0/24). It is not necessary to use the **no shutdown** command because loopback interfaces are up by default.

```
R2(config)#interface Loopback 0
R2(config-if)#ip address 192.168.2.1 255.255.255.0
```

d. Configure a clock rate for the serial router interfaces with a DCE serial cable attached.

```
R1(config)#interface S0/0/0
R1(config-if)#clock rate 64000
```

Step 3: Disable DNS lookup.

To prevent the router from attempting to translate incorrectly entered commands, disable DNS lookup.

```
R1(config)#no ip domain-lookup
```

Step 4: Configure the EIGRP routing protocol on R2 and R3.

Note: R2 and R3 exchange routes in EIGRP AS 101. R1 is acting as an ISP router and does not participate in the EIGRP routing process.

a. On R2, use the following commands.

```
R2(config)#router eigrp 101
R2(config-router)#network 10.1.1.0 0.0.0.3
R2(config-router)#network 10.2.2.0 0.0.0.3
R2(config-router)#network 192.168.2.0 0.0.0.255
R2(config-router)#no auto-summary
```

b. On R3, use the following commands.

```
R3(config)#router eigrp 101
R3(config-router)#network 192.168.3.0 0.0.0.255
R3(config-router)#network 10.2.2.0 0.0.0.3
R3(config-router)#no auto-summary
```

Step 5: Configure a static default route on R2.

Router R1 represents a connection to the Internet. A default route is configured on R2 for all traffic whose destination network does not exist in the R2 routing table.

Note: Without the default route configured on R2, R2 cannot respond to the SDM HTTP connection from PC-A later in the lab. Because R1 is not part of the EIGRP domain and is not advertising the PC-A LAN, R2 does not know about the 192.168.1.0/24 network.

a. Configure a static default route on R2 that points to the R1 S0/0/0 interface IP address.

```
R2(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.1
```

b. Redistribute the static default into EIGRP so that R3 also learns the route.

```
R2(config)#router eigrp 101
R2(config-router)#redistribute static
```

Step 6: Configure PC host IP settings.

a. Configure a static IP address, subnet mask, and default gateway for PC-A, as shown in the IP addressing table.

b. Configure a static IP address, subnet mask, and default gateway for PC-C, as shown in the IP addressing table.

Step 7: Verify basic network connectivity.

a. Ping from PC-A to the R2 S0/0/0 interface at IP address 10.1.1.2. Are the results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Note: PC-A should be able to ping external R2 interface S0/0/0 but is not able to ping any of the internal EIGRP network IP addresses on R2 and R3.

b. Ping from R2 to PC-C on the R3 LAN. Are the results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Note: If you can ping from R2 to PC-C, you have demonstrated that the EIGRP routing protocol is configured and functioning correctly. If you cannot ping but the device interfaces are up and IP addresses are correct, use the **show run** and **show ip route** commands to help identify routing protocol-related problems.

Step 8: Configure a minimum password length.

Note: Passwords in this lab are set to a minimum of 10 characters but are relatively simple for the benefit of performing the lab. More complex passwords are recommended in a production network.

Use the **security passwords** command to set a minimum password length of 10 characters.

```
R1(config)#security passwords min-length 10
```

Step 9: Configure the basic console and vty lines.

a. Configure a console password and enable login for router R1. For additional security, the **exec-timeout** command causes the line to log out after 5 minutes of inactivity. The **logging synchronous** command prevents console messages from interrupting command entry.

Note: To avoid repetitive logins during this lab, the **exec-timeout** can be set to 0 0, which prevents it from expiring. However, this is not considered a good security practice.

```
R1(config)#line console 0
R1(config-line)#password ciscoconpass
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
R1(config-line)#logging synchronous
```

b. Configure the password on the vty lines for router R1.

```
R1(config)#line vty 0 4
R1(config-line)#password ciscovtypass
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
```

c. Repeat these configurations on both R2 and R3.

Step 10: Encrypt clear text passwords.

a. Use the **service password-encryption** command to encrypt the console, aux, and vty passwords.

```
R1(config)# service password-encryption
```

b. Issue the **show run** command. Can you read the console, aux, and vty passwords? Why or why not?

_____

c. Repeat this configuration on both R2 and R3.

Step 11: Save the basic running configuration for all three routers.

Save the running configuration to the startup configuration from the privileged EXEC prompt.

```
R1#copy running-config startup-config
```

Part 2. Configuring a Remote Access VPN

In Part 2 of this lab, you configure a remote access Ipsec VPN. R2 is configured as an Easy VPN server using SDM, and the Cisco VPN client is configured on PC-A. The PC-A host simulates an employee connecting from home over the Internet. Router R1 simulates an Internet ISP router.

Task 1. Prepare R2 for SDM Access and Easy VPN Server Setup

Step 1: Configure the enable secret password and HTTP router access prior to starting SDM.

a. From the CLI, configure the enable secret password for use with SDM on R2.

```
R2(config)#enable secret cisco12345
```

b. Enable the HTTP server on R2.

```
R2(config)#ip http server
```

c. Create an admin account on R2 with privilege level 15 for use with AAA.

```
R2(config)#username admin privilege 15 password 0 cisco12345
```

Step 2: Access SDM and set command delivery preferences.

a. Run the SDM application or open a browser on PC-A and start SDM by entering the R2 S0/0/0 IP address **10.1.1.2** in the address field.

b. Log in with no username and the enable secret password **cisco12345**.

c. In the Authentication Required dialog box, enter **cisco12345** in the **Password** field and click **Yes**.

d. If the Cisco IOS IPS login dialog box displays, enter the enable secret password of **cisco12345**.

e. Select **Edit** > **Preferences** to configure SDM to allow you to preview the commands before sending them to the router. In the User Preferences window, check the **Preview commands before delivering to router** check box and click **OK**.

Task 2. Use the SDM VPN Wizard to Configure the Easy VPN Server

Step 1: Launch the Easy VPN server wizard and configure AAA services.

a. Click the **Configure** button at the top of the SDM home screen.

b. Click the **VPN** button under Tasks to view the VPN configuration page.

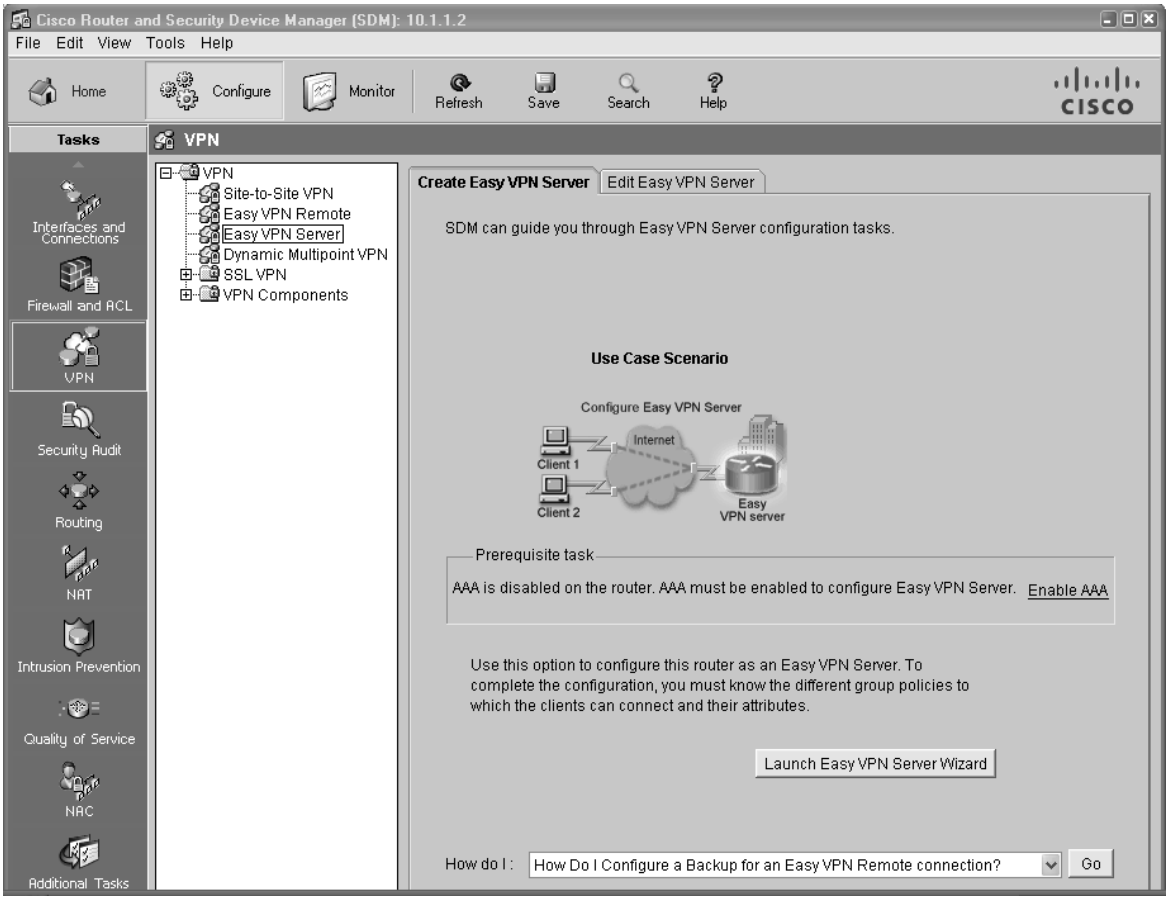
c. Select **Easy VPN Server** from the main VPN window, and then click **Launch Easy VPN Server Wizard**.

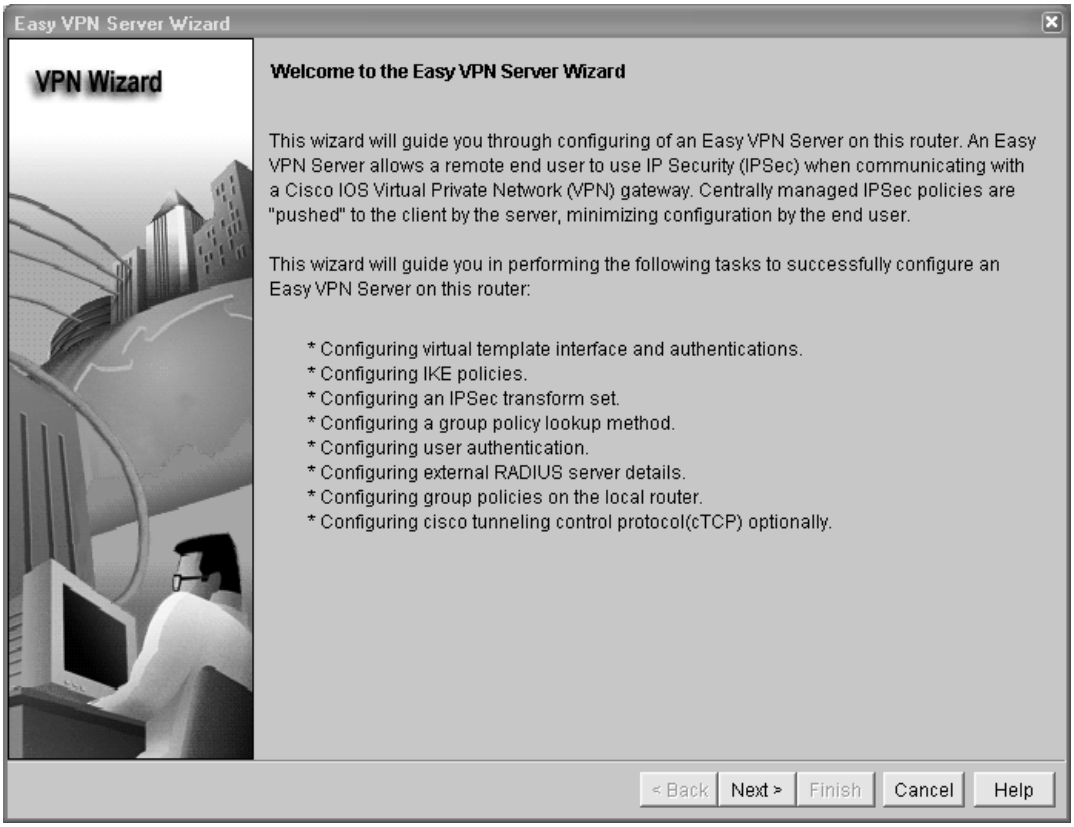
d. The Easy VPN Server wizard checks the router configuration to see if AAA is enabled. If not, the Enable AAA window displays. AAA must be enabled on the router before the Easy VPN Server configuration starts. Click **Yes** to continue with the configuration.

e. If prompted to deliver the configuration to the router, click **Deliver**.

f. In the Command Delivery Status window, click **OK**. When the message “AAA has been successfully enabled on the router” displays, click **OK**.

g. Now that AAA is enabled, you can start the Easy VPN Server Wizard by clicking the **Launch Easy VPN Server Wizard** button. Read through the descriptions of the tasks that the wizard guides you through.


Cisco Router and Security Device Manager (SDM): 10.1.1.2
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
VPN
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Additional Tasks
VPN
Site-to-Site VPN
Easy VPN Remote
Easy VPN Server
Dynamic Multipoint VPN
SSL VPN
VPN Components
Create Easy VPN Server
Edit Easy VPN Server
SDM can guide you through Easy VPN Server configuration tasks.
Use Case Scenario
Configure Easy VPN Server
Internet
Client 1
Client 2
Easy VPN server
Prerequisite task
AAA is disabled on the router. AAA must be enabled to configure Easy VPN Server.
Enable AAA
Use this option to configure this router as an Easy VPN Server. To complete the configuration, you must know the different group policies to which the clients can connect and their attributes.
Launch Easy VPN Server Wizard
How do I :
How Do I Configure a Backup for an Easy VPN Remote connection?
Go


Easy VPN Server Wizard
VPN Wizard
Welcome to the Easy VPN Server Wizard
This wizard will guide you through configuring of an Easy VPN Server on this router. An Easy VPN Server allows a remote end user to use IP Security (IPSec) when communicating with a Cisco IOS Virtual Private Network (VPN) gateway. Centrally managed IPSec policies are "pushed" to the client by the server, minimizing configuration by the end user.
This wizard will guide you in performing the following tasks to successfully configure an Easy VPN Server on this router:
* Configuring virtual template interface and authentications.
* Configuring IKE policies.
* Configuring an IPSec transform set.
* Configuring a group policy lookup method.
* Configuring user authentication.
* Configuring external RADIUS server details.
* Configuring group policies on the local router.
* Configuring cisco tunneling control protocol(cTCP) optionally.
< Back
Next >
Finish
Cancel
Help

How does the client receive the IPsec policies? _____

How does the Easy VPN remote server configuration differ from the site-to-site?

_____

_____

h. Click **Next** when you are finished answering the above questions.

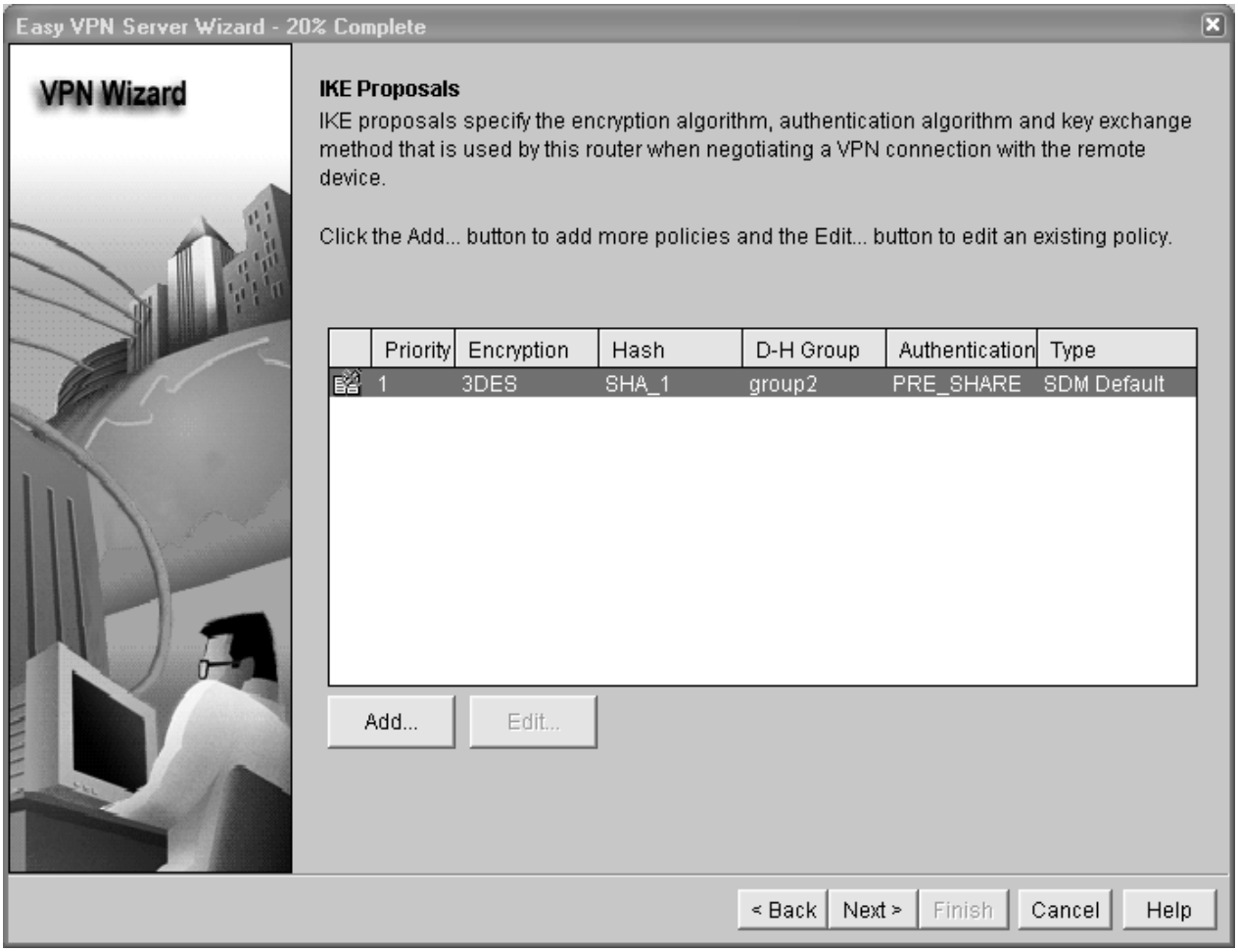
Step 2: Configure the virtual tunnel interface and authentication.

a. Select the interface on which the client connections terminate. Click the **Unnumbered to** radio button, and select the Serial0/0/0 interface from the pull-down menu.

b. Select **Pre-shared Keys** for the authentication type and click **Next** to continue.

Step 3: Select the IKE proposal.

a. In the Internet Key Exchange (IKE) Proposals window, the default IKE proposal is used for R2.



What is the encryption method used with the default IKE policy? _____

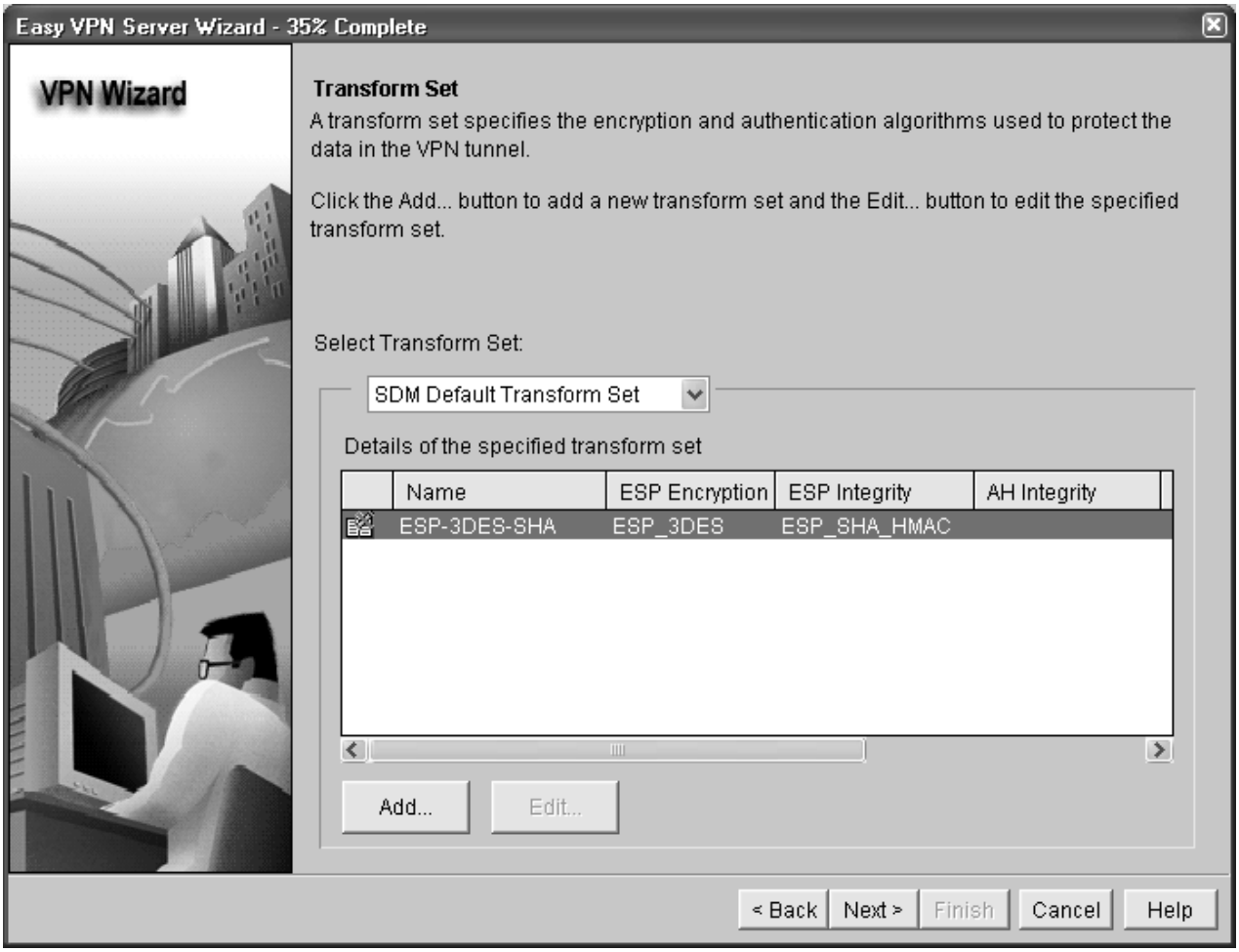
What is the hash algorithm used to ensure that the keys have not been tampered with? _____

b. Click **Next** to accept the default IKE policy.

Note: Configurations on both sides of the tunnel must match exactly. However, the Cisco VPN client automatically selects the proper configuration for itself. Therefore, no IKE configuration is necessary on the client PC.

Step 4: Select the transform set.

a. In the Transform Set window, the default SDM default transform set is used. What is the ESP encryption method used with the default transform set? _____



b. Click **Next** to accept the default transform set.

Step 5: Specify group authorization and group policy lookup.

a. In the Group Authorization and Group Policy Lookup window, select the **Local** option because a RADIUS server is not available.

b. Click **Next** to create a new AAA method list for the group policy lookup that uses the local router database.

Step 6: Configure User Authentication (XAuth).

a. In the User Authentication (XAuth) window, you can specify to store user information on an external server, such as a RADIUS server or a local database or both. Check the **Enable User Authentication** check box and accept the default of **Local Only**.

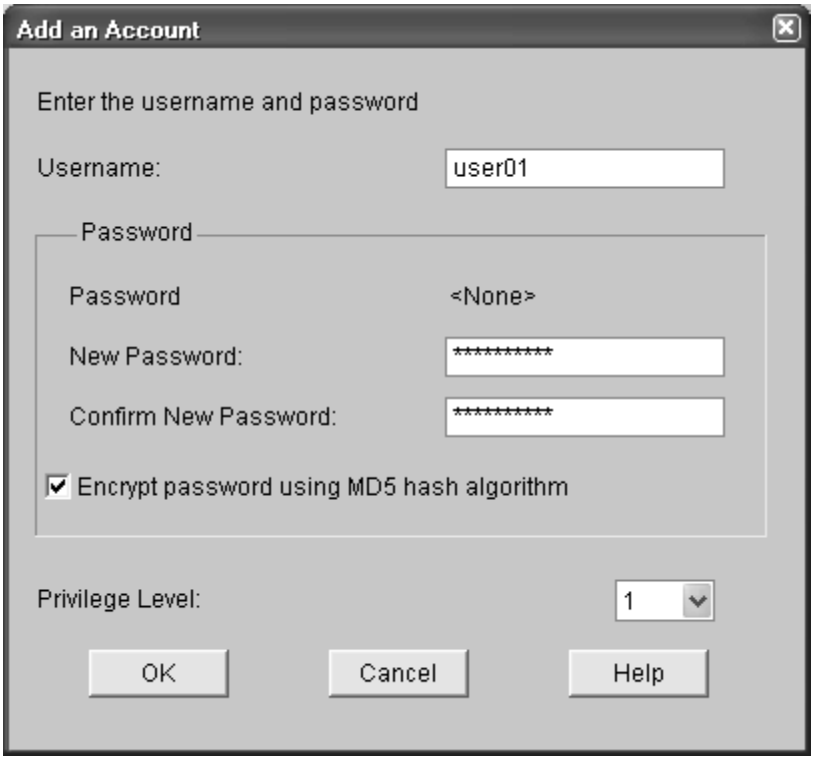
Where does the router look for valid user account and passwords to authenticate remote VPN users when they attempt to log in? _____

b. Click the **Add User Credentials** button. In the User Accounts window, you can view currently defined users or add new users. What is the name of the user currently defined, and what is the user privilege level? _____

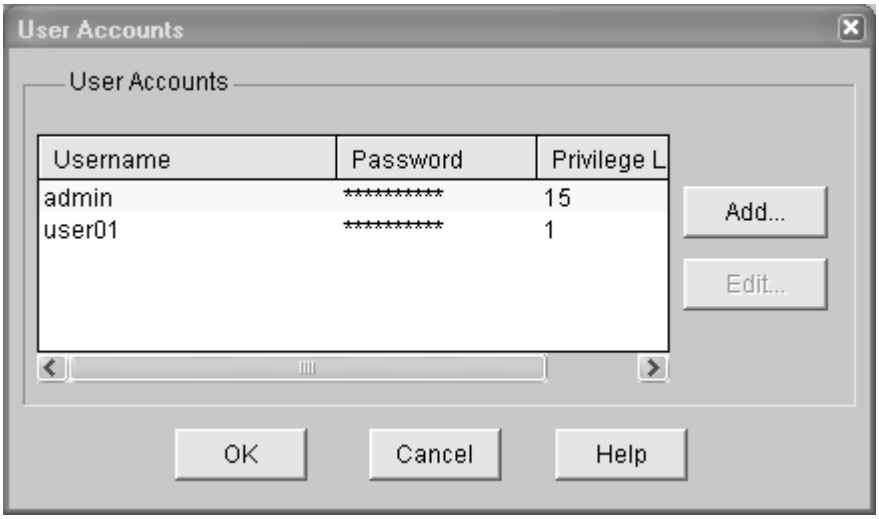
How was this user defined? _____

c. In the User Accounts window, click the **Add** button to add another user. Enter the username user01 with a password of user01pass, and select the check box for encrypting the password using the MD5 hash algorithm. Leave the privilege level at 1.

What is the range of privilege levels that can be set for a user? _____



d. Click **OK** to accept the user01 entries, and then click **OK** to close the User Accounts window.



e. In the User Authentication (XAuth) window, click **Next** to continue.

Step 7: Specify group authorization and user group policies.

In the Group Authorization and User Group Policies window, you must create at least one group policy for the VPN server.

a. Click **Add** to create a group policy.

b. In the Add Group Policy window, enter **VPN-Access** as the name of this group. Enter a new pre-shared key of **cisco12345** and then re-enter it.

c. Leave the **Pool Information** box checked. Enter a starting address of **192.168.2.101**, an ending address of **192.168.2.150**, and a subnet mask of **255.255.255.0**.

d. Enter 50 for the **Maximum Connections Allowed**.

e. Click **OK** to accept the entries.

f. An SDM warning message displays indicating that the IP addresses in the pool and the IP address of the Loopback0 interface are in the same subnet. Click **Yes** to confirm.

Why use an IP network for the VPN clients pool that is associated with a loopback interface?

_____

How does R3 route traffic to the VPN clients?

_____

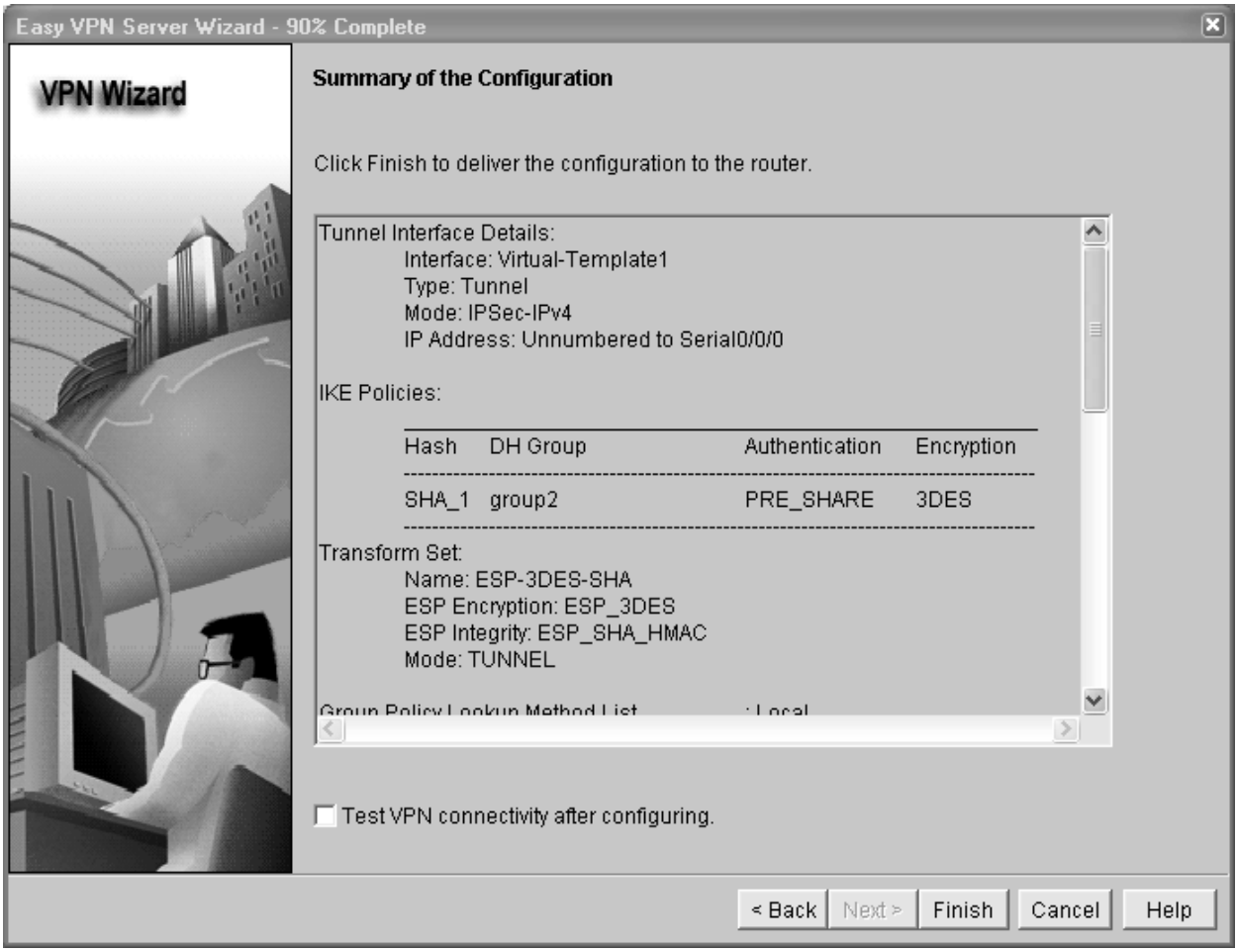
g. When you return to the Group Authorization window, check the **Configure Idle Timer** check box and enter one hour (**1**). This disconnects idle users if there is no activity for one hour and allows others to connect. Click **Next** to continue.

h. When the Cisco Tunneling Control Protocol (cTCP) window displays, do not enable cTCP. Click **Next** to continue.

Step 8: Review the configuration summary and deliver the commands.

a. Scroll through the commands that SDM will send to the router. Do not select the check box **Test VPN connectivity**. Click **Finish**.

b. If prompted to deliver the configuration to the router, click **Deliver**.



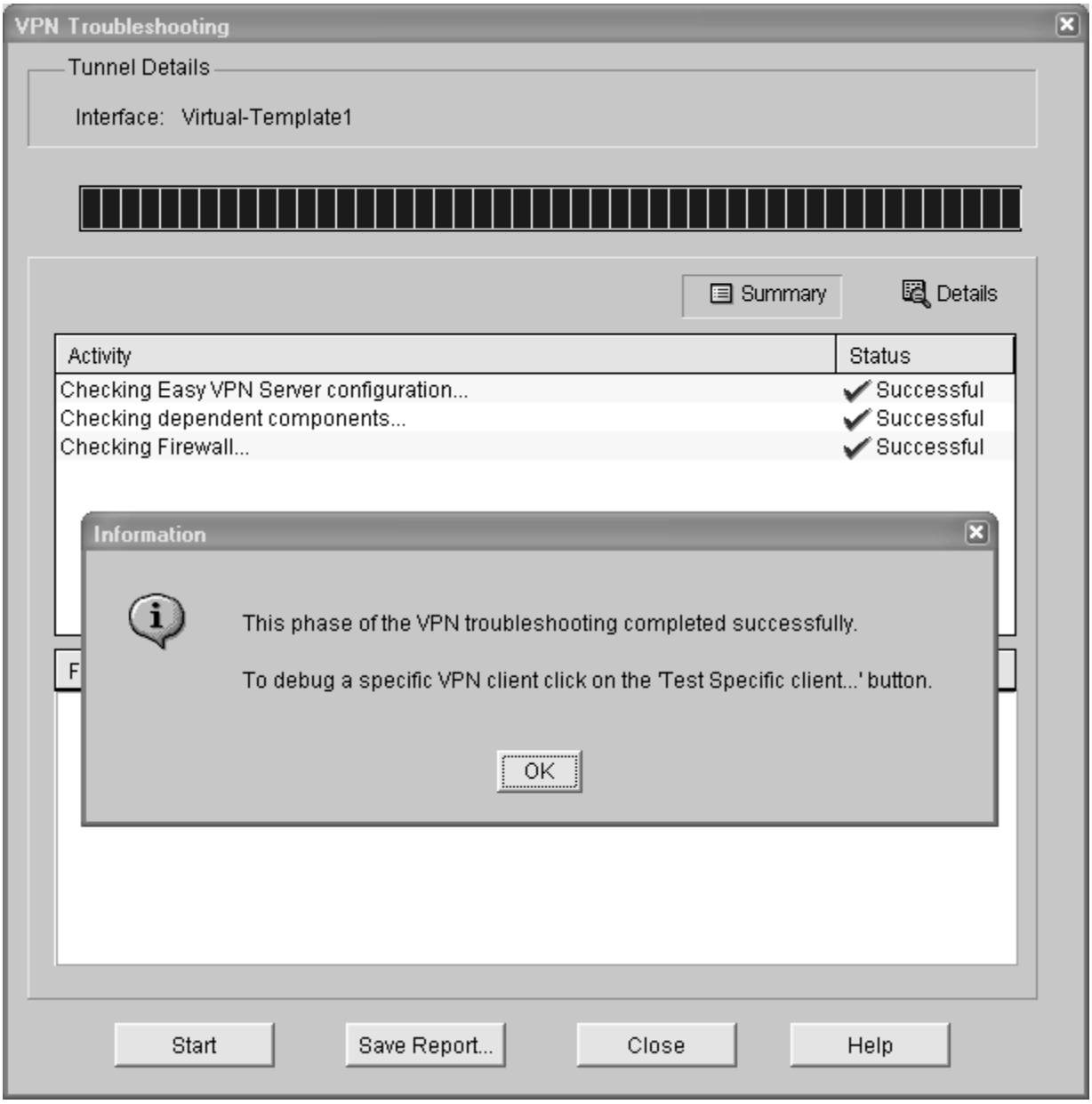
c. In the Command Delivery Status window, click **OK**. How many commands were delivered? _____

Step 9: Test the VPN server.

a. You are returned to the main VPN window with the **Edit Easy VPN Server** tab selected. Click the **Test VPN Server** button in the bottom right corner of the screen.

b. In the VPN Troubleshooting window, click the **Start** button.

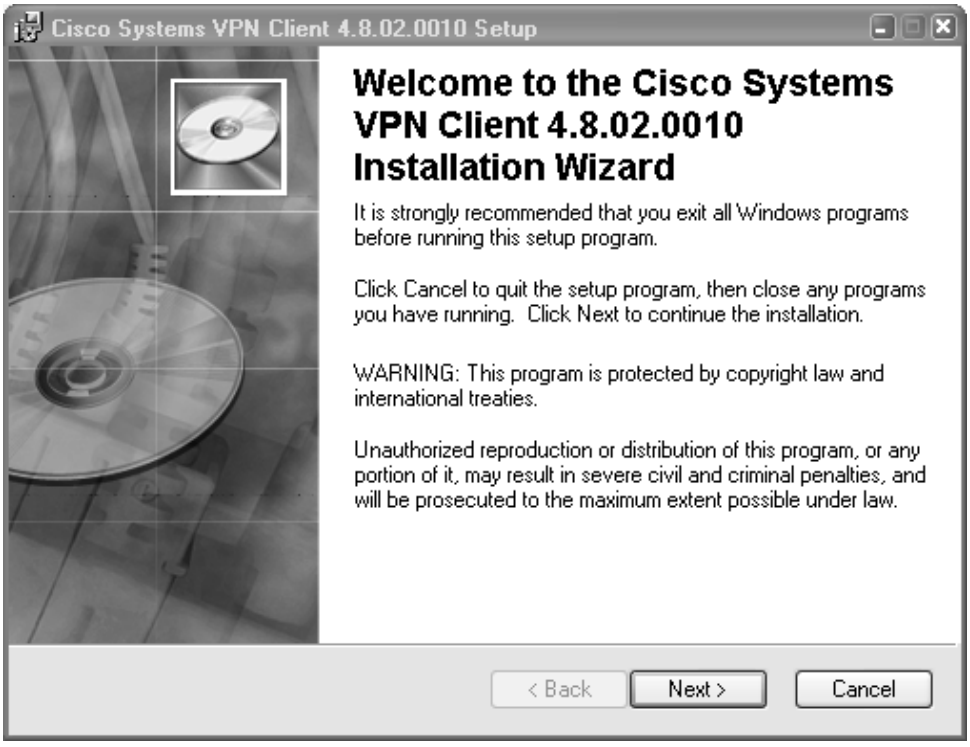
c. Your screen should look similar to the one below. Click **OK** to close the information window. Click **Close** to exit the VPN Troubleshooting window.



Task 3. Use the Cisco VPN Client to Test the Remote Access VPN

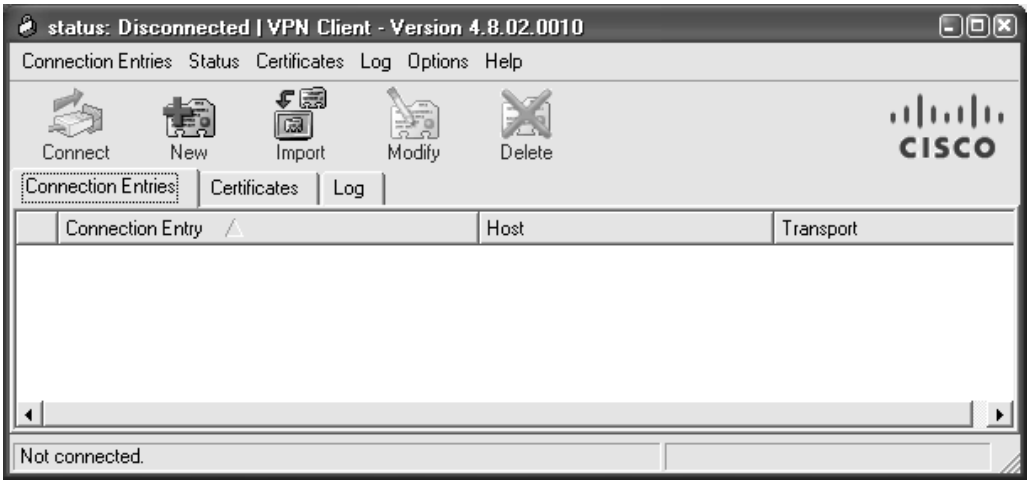
Step 1: (Optional) Install the Cisco VPN client.

If not already installed, install Cisco VPN client software on host PC-A. If you do not have the Cisco VPN client software, contact your instructor.



Step 2: Configure PC-A as a VPN client to access the R2 VPN server.

Start the Cisco VPN client and select **Connection Entries > New** or click the **New** icon.



Enter the following information to define the new connection entry. Click **Save** when you are finished.

Connection Entry: **VPN-R2**

Description: **Connection to R2 internal network**

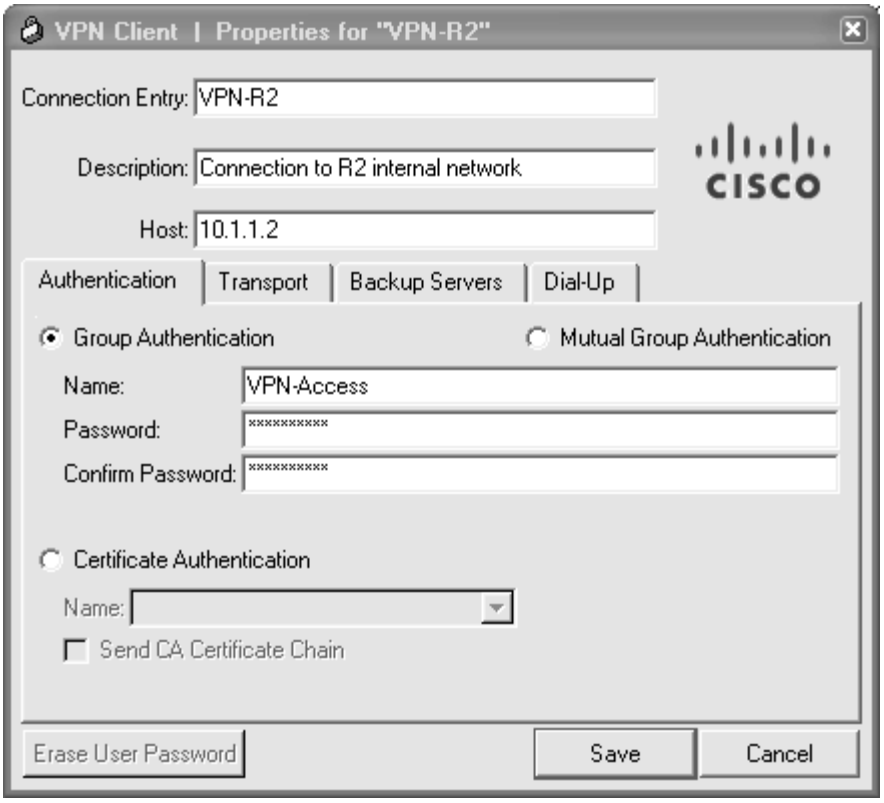
Host: **10.1.1.2** (IP address of the R2 S0/0/0 interface)

Group Authentication Name: **VPN-Access** (Defines the address pool configured in Task 2)

Password: **cisco12345** (Pre-shared key configured in Task 2)

Confirm Password: **cisco12345**

Note: The group authentication name and password are case-sensitive and must match the ones created on the VPN server.



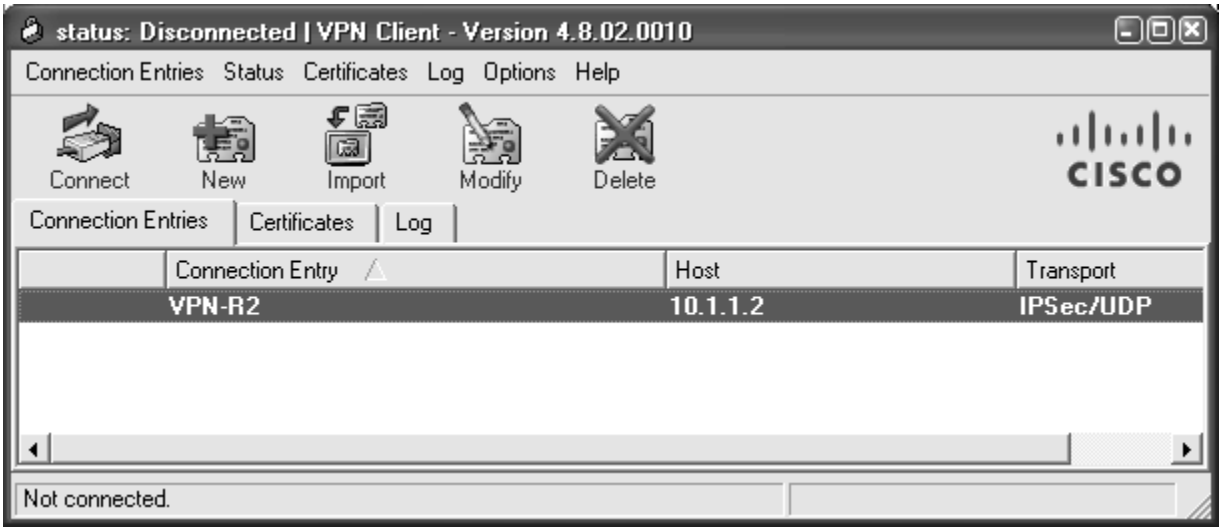
Step 3: Test access from PC-A without a VPN connection.

Open a command prompt on PC-A, and ping the PC-C IP address at 192.168.3.3 on the R3 LAN. Are the pings successful? Why or why not?

Note: After creating a VPN connection entry, you must activate it. Currently, the VPN tunnel is not up.

Step 4: Establish a VPN connection and login.

a. Select the newly created connection VPN-R2 and click the **Connect** icon. You can also double-click the connection entry.



b. Enter the username **admin** created previously on the VPN router, and enter the password **cisco12345**.

c. Click **OK** to continue. The VPN Client window minimizes to a lock icon in the tools tray of the taskbar. When the lock is closed, the VPN tunnel is up. When it is open, the VPN connection is down.

Task 4. Verify the VPN Tunnel between the Client, Server, and Internal Network

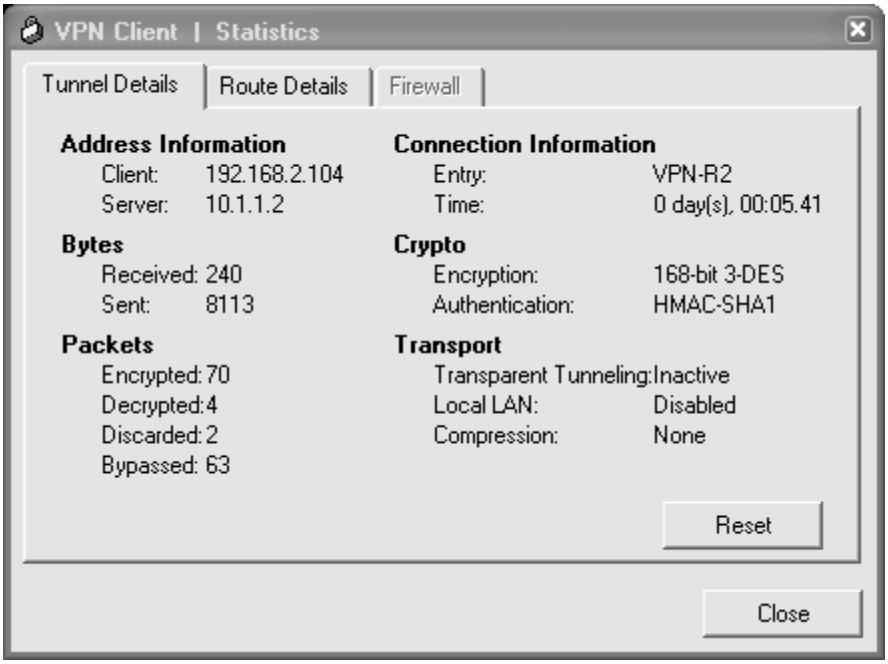
Step 1: Check the VPN Client status.

Double-click the VPN lock icon to expand the VPN Client window.

What does it say about the connection status at the top of the window? _____

Step 2: Check the tunnel statistics.

Select **Status** > **Statistics** to display the **Tunnel Details** tab.



What is the Client IP address obtained from the VPN server?

_____

Note: Each time you disconnect and reconnect to the VPN server, you receive a new IP address until the limit is reached.

a. What is the VPN server address? _____

b. How many packets have been encrypted? _____

c. What is the encryption method being used? _____

d. What is the authentication being used? _____

Step 3: Check the Cisco IOS messages on R2 when the tunnel is created.

Open the console connection for R2 and locate the message displayed indicating that the virtual interface came up when the VPN Client connection was made.

```
R2#
*Feb  2 16:09:08.907: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Virtual-Access2, changed state to up
R2#
```

Step 4: Verify the VPN connection.

From the PC-A command prompt, issue the **`ipconfig /all`** command to see the network connections currently in use.

a. What is the configuration for the first local area connection?

IP Address: _____
Subnet Mask: _____
Default Gateway: _____
Description:

b. What is the configuration for Local Area Connection 2?

IP Address: _____
Subnet Mask: _____
Default Gateway: _____
Description: _____

Step 5: Test the access from the client with the VPN connection.

With the VPN connection from computer PC-A to router R2 activated, open a command prompt on PC-A and ping the PC-C IP address at 192.168.3.3 on the R3 LAN. Are the pings successful? Why or why not?

_____
_____

Step 6: Telnet to R2 from PC-A.

From the PC-A command prompt, telnet to R2 at the Lo0 IP address 192.168.2.1 Log in as **admin** with the password **cisco12345**. What is the router command prompt and why is this?

_____

a. Issue the **`show run`** command to view the various commands generated by SDM to configure the VPN server.

b. Issue the **`show users`** command to see the connections to router R2. What connections are present?

_____

c. Exit the Telnet session with the **`quit`** or **`exit`** command.

d. Right-click the VPN Client icon in the tools tray and select **Disconnect,** or click the VPN-R2 connection and click the **Disconnect** icon.

e. Open the VPN client connection again but this time log in as **user01** with the password **user01pass**.

f. Telnet from PC-A to R2 again at the Lo0 IP address 192.168.2.1. Log in as **user01** with the password **user01pass**. What is the router command prompt and why is this?

_____

Note: You could have telnetted to R2 from the first VPN session and logged in as user01, but this process demonstrates the VPN disconnect and connect process and verifies that user01 is set up properly.

Task 5. Reflection

Why is VPN a good option for remote users?

Router Interface Summary Table

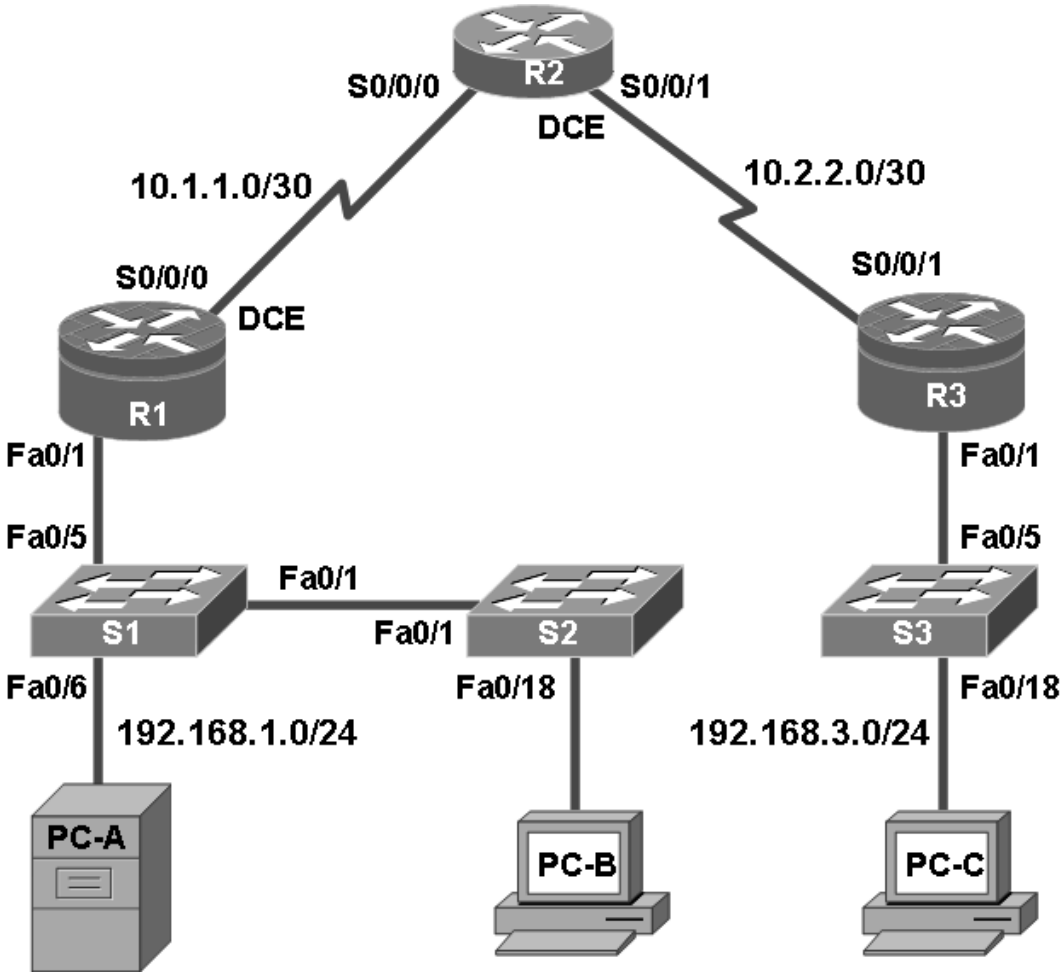
Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1700	Fast Ethernet 0 (FA0)	Fast Ethernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Router Interface Summary				
2600	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
2800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Chapter 9: Lab A: Security Policy Development and Implementation

Topology



IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	FA0/1	192.168.1.1	255.255.255.0	N/A	S1 FA0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	FA0/1	192.168.3.1	255.255.255.0	N/A	S3 FA0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1	N/A
S2	VLAN 1	192.168.1.12	255.255.255.0	192.168.1.1	N/A
S3	VLAN 1	192.168.3.11	255.255.255.0	192.168.3.1	N/A

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 FA0/6
PC-B	NIC	192.168.1.2	255.255.255.0	192.168.1.1	S2 FA0/18
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 FA0/18

Objectives

Part 1: Create a Basic Security Policy

- Use Cisco Security Policy Builder to create a policy.
- Develop a network device configuration policy.

Part 2: Basic Network Device Configuration

- Configure host names, interface IP addresses, and passwords.
- Configure static routing.

Part 3: Secure Network Routers

- Configure passwords and a login banner.
- Configure SSH access and disable Telnet.
- Configure HTTP secure server access.
- Configure a synchronized time source using NTP.
- Configure router syslog support.
- Configure centralized authentication using AAA and RADIUS.
- Use Cisco IOS to disable unneeded services and secure against login attacks.
- Use SDM to disable unneeded services.
- Configure a CBAC firewall.
- Configure a ZBF firewall.
- Configure Intrusion Prevention System (IPS) using Cisco IOS and SDM.
- Back up and secure the Cisco IOS image and configuration files.

Part 4: Secure Network Switches

- Configure passwords, and a login banner.
- Configure management VLAN access.
- Configure a synchronized time source Using NTP.
- Configure syslog support.

- Configure SSH access.
- Configure AAA and RADIUS.
- Secure trunk ports.
- Secure access ports.
- Protect against STP attacks.
- Configure port security and disable unused ports.

Part 5: Configure VPN Remote Access

- Use SDM to configure Easy VPN Server.
- Use the Cisco VPN Client to test the remote access VPN.

Background

A comprehensive security policy covers three main areas: governing policies, end-user policies, and technical policies. Technical policies can include email, remote access, telephony, applications, and network policies, such as device access controls and logging. The focus of this lab is technical network policies and security measures that can be configured for network devices.

In Part 1 of this lab, you use the Cisco Security Policy Builder tool to create a basic security policy. You customize the policy by changing the generic names in the document to a company name of your choice.

You also develop a Network Device Security Guidelines document as a supplement to the basic security policy. This document addresses specific router and switch security measures and describes the security requirements to be implemented on the infrastructure equipment. The basic Security Policy and the Network Device Security Guidelines are presented to your instructor for review prior to starting Part 2 of the lab.

In Part 2, you build the network and configure basic device settings. In Parts 3 and 4, you secure routers and switches. In Part 5, you configure a router for VPN remote access. The Network Device Security Guidelines policy is used as the guiding document.

The fictitious company you are working for has two locations connected by an ISP. Router R1 represents a remote site, and R3 represents the corporate headquarters. Router R2 represents the ISP.

Note: The router commands and output in this lab are from a Cisco 1841 with Cisco IOS Release 12.4(20)T (Advanced IP image). The switch commands and output are from a Cisco WS-C2960-24TT-L with Cisco IOS Release 12.2(46)SE (C2960-LANBASEK9-M image). Other routers, switches, and Cisco IOS versions can be used. See the Router Interface Summary table at the end of the lab to determine which interface identifiers to use based on the equipment in the lab. Depending on the router or switch model and Cisco IOS version, the commands available and output produced might vary from what is shown in this lab.

Note: Make sure that the routers and switches have been erased and have no startup configurations.

Required Resources

- 2 routers with SDM 2.5 installed (Cisco 1841 with Cisco IOS Release 12.4(20)T1 Advanced IP Service or comparable)
- 1 router (Cisco 1841 with Cisco IOS Release 12.4(20)T1 IP Base or comparable)

- 3 switches (Cisco 2960 with Cisco IOS Release 12.2(46)SE C2960-LANBASEK9-M image or comparable)
- PC-A: Windows XP, Vista, or Windows Server (with RADIUS, TFTP, and syslog servers plus PuTTY and Cisco VPN Client software available)
- PC-B: Windows XP or Vista
- PC-C: Windows XP or Vista (with RADIUS, TFTP, and syslog servers plus PuTTY software available; SuperScan is optional)
- Serial and Ethernet cables as shown in the topology
- Rollover cables to configure the routers via the console
- Access to the Internet and an email account.

Part 1. Create a Security Policy

In Part 1, you use the Cisco Security Policy Builder tool to create a basic security policy. You customize the policy to meet specific needs. Present this document in a formal manner, with a title page, administrative overview, and policy components.

This tool provides businesses a sample network security policy that is then tailored to their requirements.

Task 1. Use Cisco Security Policy Builder to Create a Basic Security Policy (Chapter 9)

Step 1: Access the Cisco Security Policy Builder tool.

a. Open a browser and access the Cisco Security Policy Builder (SPB) tool at http://www.ciscowebtools.com/spb.

Note: You do not need a CCO account to access this tool.

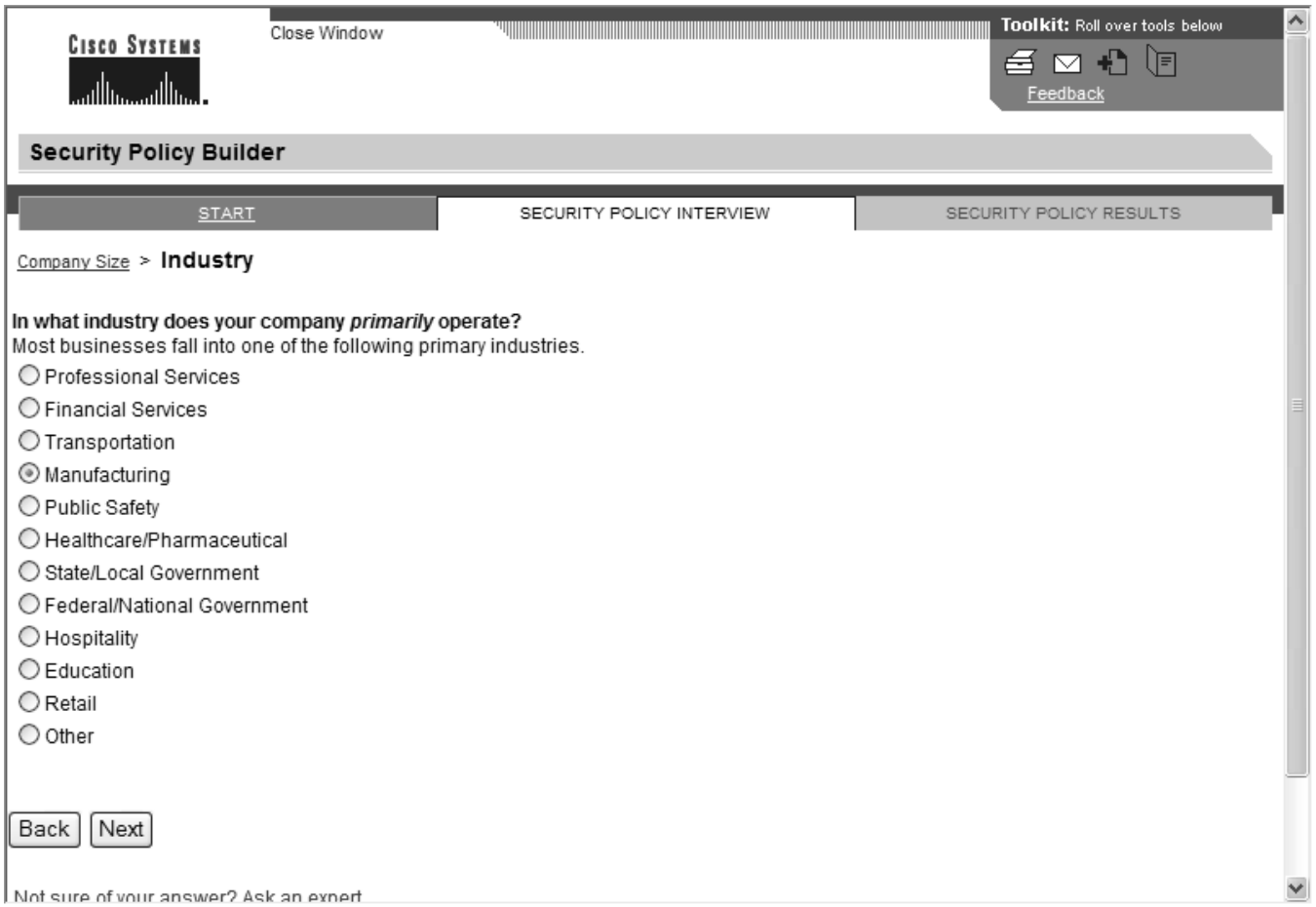
b. Read through the introduction screen to get an overview of what SPB does and then click the **Launch Security Policy Builder** link.

Step 2: Create a basic security policy.

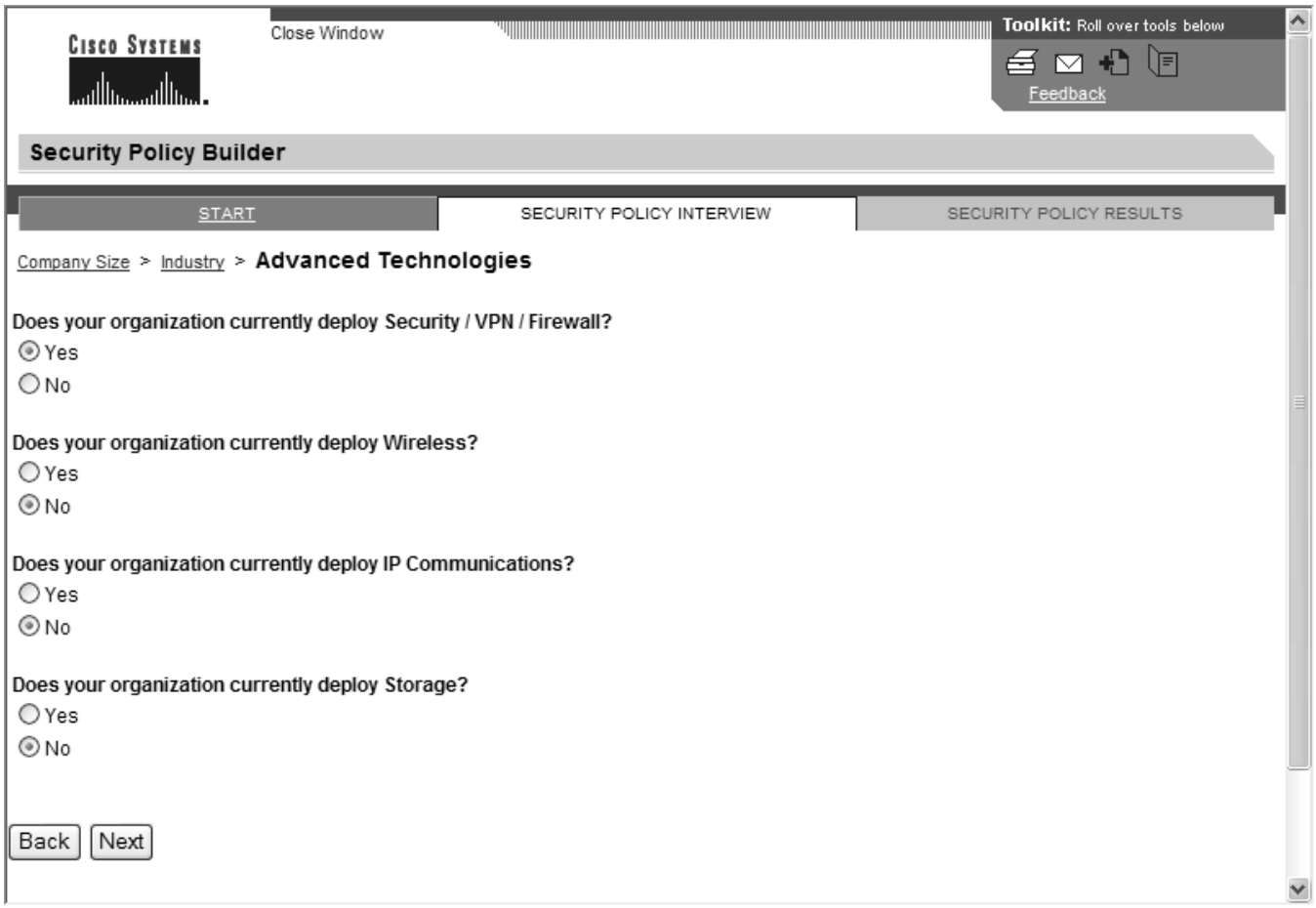
In the next window, click the **SECURITY POLICY INTERVIEW** link to begin the interview.

a. In the first SECURITY POLICY INTERVIEW window, select 51-100 employees for **Company Size**. Click **Next** to continue.

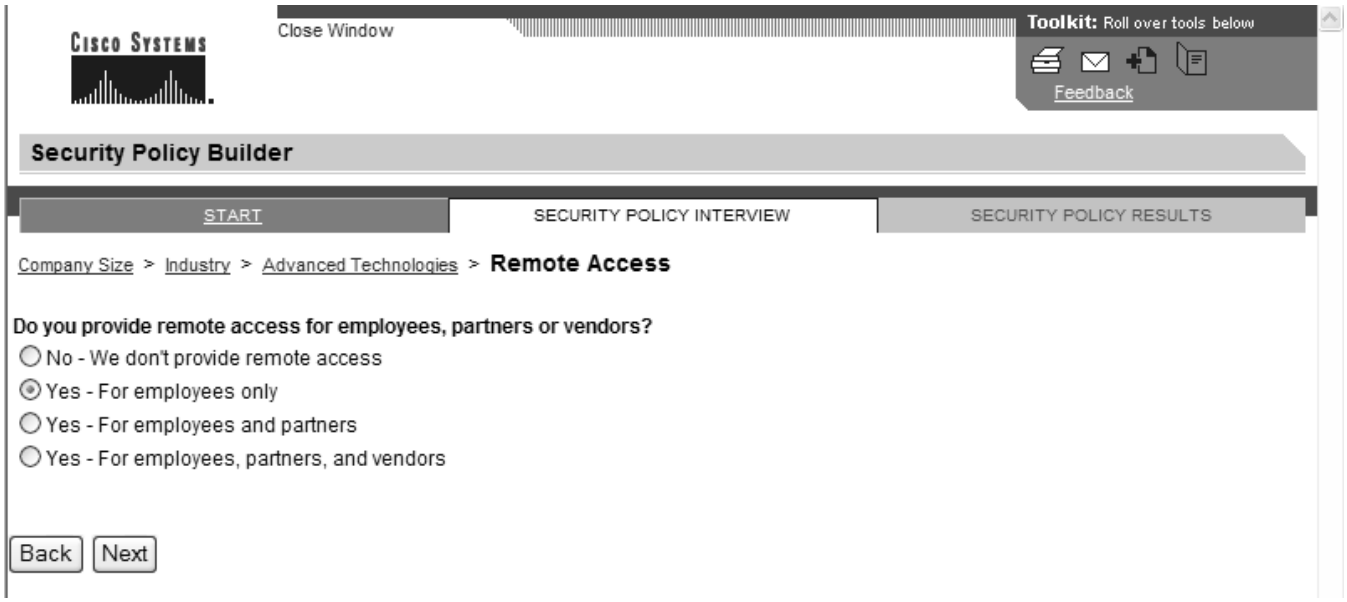
b. For **Industry**, select the industry in which your company primarily operates. You may choose any of the industries listed. In this example, the manufacturing industry is selected. Click **Next** to continue.



c. For **Advanced Technologies**, select **Yes** for the question regarding whether the organization deploys security, VPN, and firewall? Select **No** for wireless, IP communications (VoIP), and storage. Click **Next** to continue.



d. For **Remote Access**, select **Yes – For Employees only**. Click **Next** to continue.



e. In the SECURITY POLICY RESULTS window, enter your email address and accept the disclaimer. Click **Send Security Policy**.

Note: The security policy is emailed to you as a Word document.

Step 3: Review the basic security policy.

The security policy generated by Cisco SPB is approximately 20 pages. Review the major sections of the policy and list them in the space provided below.

Note: These sections change based on your answers to the security policy interview in Step 2, especially those related to the advanced technologies employed.

_____
_____
_____
_____
_____

What portions of the generated basic SPB policy are related to technical policies?

a. Select a fictitious company name and write it here: _____

b. Read through the policy to identify generic text to be replaced. Use find and replace to replace the text with the company name that you selected.

c. Replace the generic text in the basic security policy document, such as < YOUR COMPANY NAME HERE >, with the name of your fictitious company.

Task 2. Create Network Equipment Security Guidelines to Supplement the Basic Security Policy (Chapter 9)

Step 1: Review the objectives for previous CCNA Security labs.

a. Open each of the previous labs completed from chapters one through eight and review the objectives listed for each one.

b. Copy them to a separate document for use as a starting point. Focus mainly on those objectives that involve security practices and device configuration.

Step 2: Create a Network Device Security Guidelines document for router and switch security.

Create a high-level list of tasks to include for network device security. This document reinforces and supplements the information presented in the basic Security Policy document created in Task 1. It is based on the content of previous CCNA Security labs and on the networking devices present in the course lab topology. Construct the document so that the topic headings and wording are similar to that found in the Security Policy document.

Note: The Network Device Security Guidelines document is no more than two pages and is the basis for the equipment configuration in the remaining parts of the lab.

Step 3: Submit the basic Security Policy and Network Device Security Guidelines to your instructor.

Provide the edited basic Security Policy and Network Device Security Guidelines documents to your instructor for review before starting Part 2 of the lab. You can send them as email attachments or put them on removable storage media, such as a flash drive, floppy disc, or CD.

Note: These security documents are over 20 pages. Do not print them out.

Part 2. Basic Network Device Configuration (Chapters 2 and 6)

In Part 2, you set up the network topology and configure basic settings, such as the interface IP addresses and static routing. Perform steps on routers and switches as indicated.

Step 1: Cable the network as shown in the topology.

Attach the devices shown in the topology diagram, and cable as necessary.

Step 2: Configure basic settings for all routers.

Configure host names as shown in the topology.

a. Configure the interface IP addresses as shown in the IP addressing table.

b. Configure a clock rate for the routers with a DCE serial cable attached to their serial interface.

c. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

Step 3: Configure static default routes on R1 and R3.

Configure a static default route from R1 to R2 and from R3 to R2.

Step 4: Configure static routes on R2.

Configure a static route from R2 to the R1 LAN and from R2 to the R3 LAN.

Step 5: Configure basic settings for each switch.

Configure host names as shown in the topology.

a. Configure the VLAN 1 management addresses as shown in the IP Addressing table.

b. Configure the IP default gateway for each of the three switches. The gateway for the S2 and S3 switches is the R1 Fa0/1 interface IP address. The gateway for the S3 switch is the R3 Fa0/1 interface IP address.

c. Disable DNS lookup to prevent the switches from attempting to translate incorrectly entered commands as though they were host names.

Step 6: Configure PC host IP settings.

Configure a static IP address, subnet mask, and default gateway for PC-A, PC-B, and PC-C, as shown in the IP addressing table.

Step 7: Verify connectivity between PC-A and PC-C.

Step 8: Save the basic running configuration for each router.

Part 3. Secure Network Routers

In Part 3, you configure device access, passwords, firewalls, and intrusion prevention. Perform steps on routers as indicated.

Task 1. Configure Passwords and a Login Banner (Chapter 2)

Step 1: Configure a minimum password length of 10 characters on all routers.

Step 2: Configure the enable secret password on all routers.

Use an enable secret password of **cisco12345.**

Step 3: Encrypt plaintext passwords.

Step 4: Configure the console lines on all routers.

Configure a console password of **ciscoconpass** and enable login. Set the `exec-timeout` to log out after 5 minutes of inactivity. Prevent console messages from interrupting command entry.

Step 5: Configure the vty lines on R2.

Configure a vty lines password of **ciscovtypass** and enable login. Set the `exec-timeout` to log out after 5 minutes of inactivity.

Note: The vty lines for R1 and R3 are configured for SSH in Task 2.

Step 6: Configure a login warning banner on routers R1 and R3.

Configure a warning to unauthorized users with a message-of-the-day (MOTD) banner that says "`Unauthorized access strictly prohibited and prosecuted to the full extent of the law`".

Task 2. Configure the SSH Server on Routers R1 and R3 (Chapter 2)

Step 1: Configure a privileged user for login from the SSH client.

Create the user `Admin01` account with a privilege level of 15 and a secret password of `Admin01pa55`.

Step 2: Configure the domain name ccnasecurity.com.

Step 3: Configure the incoming vty lines.

Specify a privilege level of 15 so that a user with the highest privilege level (15) will default to privileged EXEC mode when accessing the vty lines. Other users will default to user EXEC mode. Specify local user accounts for mandatory login and validation, and accept only SSH connections.

Step 4: Generate the RSA encryption key pair for the router.

Configure the RSA keys with 1024 for the number of modulus bits.

Step 5: Verify SSH connectivity to R1 from PC-A.

a. If the SSH client is not already installed, download either TeraTerm or PuTTY.

b. Launch the SSH client, enter the Fa0/1 IP address, and enter the **Admin01** username and password **Admin01pa55**.

Task 3. Configure a Synchronized Time Source Using NTP (Chapter 2)

Step 1: Set up the NTP master using Cisco IOS commands.

R2 will be the master NTP server. All other routers and switches learn their time from it, either directly or indirectly.

a. Ensure that R2 has the correct coordinated universal time. Set the time if it is not correct.

b. Configure R2 as the NTP master with a stratum number of 3.

Step 2: Configure R1 and R3 as NTP clients.

a. Configure R1 and R3 to become NTP clients of R2.

b. Verify that R1 and R3 have made an association with R2 using the **`show ntp associations`** command.

Task 4. Configure Router Syslog Support (Chapter 2)

Step 1: (Optional) Install the syslog server on PC-A and PC-C.

If a syslog server is not currently installed on the host, download the latest version of Kiwi from http://www.kiwisyslog.com or Tftpd32 from http://tftpd32.jounin.net and install it on your desktop. If it is already installed, go to Step 2.

Step 2: Configure R1 to log messages to the PC-A syslog server.

a. Verify that you have connectivity between R1 and host PC-A by pinging the R1 Fa0/1 interface IP address 192.168.1.1 from PC-A. If it is not successful, troubleshoot as necessary before continuing.

b. Configure logging on the router to send syslog messages to the syslog server.

Step 3: Configure R3 to log messages to the PC-C syslog server.

a. Verify that you have connectivity between R3 and the host PC-C by pinging the R3 Fa0/1 interface IP address 192.168.3.1 from PC-C. If it is not successful, troubleshoot as necessary before continuing.

b. Configure logging on the router to send syslog messages to the syslog server.

Task 5. Configure Authentication Using AAA and RADIUS (Chapter 3)

PC-A will serve as the local RADIUS server for the remote site, and R1 accesses the external RADIUS server for user authentication. The freeware RADIUS server WinRadius is used for this section of the lab.

Step 1: (Optional) Download and configure the WinRadius software.

a. If WinRadius is not currently installed on R1, download the latest version from http://www.suggestsoft.com/soft/itconsult2000/winradius/. There is no installation setup. The extracted WinRadius.exe file is executable.

b. Start the WinRadius.exe application. If the application is being started for the first time, follow the instructions to configure the WinRadius server database.

Step 2: Configure users and passwords on the WinRadius server.

a. Add username **RadAdmin** with a password of **RadAdminpa55.**

b. Add username **RadUser** with a password of **RadUserpa55**.

Step 3: Enable AAA on R1.

Use the **`aaa new-model`** command to enable AAA.

Step 4: Configure the default login authentication list.

Configure the list to first use **radius** for the authentication service and then **local** to allow access based on the local router database if a RADIUS server cannot be reached.

Step 5: Verify connectivity between R1 and the PC-A RADIUS server.

Ping from R1 to PC-A.

If the pings are not successful, troubleshoot the PC and router configuration before continuing.

Step 6: Specify a RADIUS server on R1.

Configure the router to access the RADIUS server at the PC-A IP address. Specify port numbers 1812 and 1813, along with the default secret key of WinRadius for the RADIUS server.

Step 7: Test your configuration by logging into the console on R1.

a. Exit to the initial router screen that displays the following: R1 con0 is now available.

b. Log in with the username RadAdmin and password RadAdminpa55. Are you able to login with minimal delay? _____

Note: If you close the WinRadius server and restart it, you must recreate the user accounts from Step 2.

Step 8: Test your configuration by connecting to R1 with SSH.

Clear the log display for the WinRadius server by selecting **Log > Clear**.

a. Use PuTTY or another terminal emulation client to open an SSH session from PC-A to R1.

b. At the login prompt, enter the username **RadAdmin** defined on the RADIUS server and the password **RadAdminpa55**.

Are you able to login to R1? _____

c. Exit the SSH session.

d. Stop the WinRadius server on PC-A by selecting **Operation > Exit**.

e. Open an SSH session and attempt to log in again as RadAdmin.

Are you able to login to R1? _____

f. Close the SSH client and open another SSH session to R1 and attempt to log in as Admin01 with a password of Admin01pa55.

With the WinRadius server unavailable, are you able to log in to R1? Why or why not?

_____

_____

Step 9: Configure RADIUS support on R3.

Repeat steps 1 through 6 to configure R3 to access PC-C as a RADIUS server.

Task 6. Use the CLI to Disable Unneeded Services on R1 and Secure Against Login Attacks (Chapter 2)

Step 1: Use the CLI to disable common IP services that can be exploited for network attacks.

Tip: You can issue the **`auto secure management`** command to see the management related commands that would be generated. When prompted with "Apply this configuration to running-config? [yes]:" respond **NO** and then selectively copy the desired commands to a text file for editing and application to the router.

Disable the following global services on the router.

```
Service finger
service pad
service udp-small-servers
service tcp-small-servers
cdp run
ip bootp server
ip http server
ip finger
ip source-route
ip gratuitous-arps
ip identd
```

Note: Disabling the HTTP server prevents web-based access to the router using SDM. If you want to have secure access to the router using SDM, you can enable it using the command **`ip http secure-server`**.

a. For each serial interface, disable the following interface services.

```
Ip redirects
ip proxy-arp
ip unreachables
ip directed-broadcast
ip mask-reply
```

b. For each Fast Ethernet interface, disable the following interface services.

```
Ip redirects
ip proxy-arp
ip unreachables
ip directed-broadcast
ip mask-reply
mop enabled
```

Step 2: Secure against login attacks on R1 and R3.

Configure the following parameters:

- Blocking period when login attack detected: 60
- Maximum login failures with the device: 2

- Maximum time period for crossing the failed login attempts: 30

Step 3: Save the running configuration to the startup configuration for R1 and R3.

Task 7. Use SDM to Disable Unneeded Services on R3 (Chapter 2)

Step 1: Configure secure HTTP router access prior to starting SDM.

Enable the HTTP secure server on R3.

Step 2: Access SDM and set command delivery preferences.

a. Start the SDM application, or open a browser on PC-C and start SDM by entering the R3 IP address at **https://192.168.3.1** in the address field. Be sure to use HTTPS as the protocol.

b. At the security certificate warning, click **Continue to this website**.

c. Log in with no username and the enable secret password cisco12345.

d. If the Warning – Security window pops up stating that the website's certificate cannot be verified, check the **Always trust content from this publisher** check box and then click **Yes** to continue.

e. In the Authentication Required dialog box, do not enter a username but enter the enable secret password **cisco12345.**

f. In the IOS IPS Login dialog box, do not enter a username but enter the enable secret password **cisco12345.**

g. Set the user preferences to allow preview of commands before delivering them to the router.

Step 3. Begin the security audit.

a. Select **Configure > Security Audit** and click the **Perform Security Audit** button.

b, Select **FastEthernet 0/1** as the Inside Trusted interface and **Serial 0/0/1** as the Outside Untrusted interface

c. View the Security Audit report and note which services did not pass. Click **Next**.

d. In the Fix It window, click **Fix it** to disable the following global and interface services:

```
Global services to disable:
service pad
cdp run
ip bootp server
ip source-route

Per-interface service to disable:
ip redirects
ip unreachables
mop enabled
```

Note: Do not fix (disable) Proxy ARP because this disables ARP on all R3 interfaces and causes a problem, specifically with interface Fa0/1, and pings to the R3 VPN server LAN. The VPN server is configured in Part 5 of the lab.

e. Click **Next** to view a summary of the problems that will be fixed. Click **Finish** to deliver the commands to the router.

Task 8. Configure a CBAC Firewall on R1 (Chapter 4)

Step 1: Use the Cisco IOS AutoSecure feature to enable a CBAC firewall on R1.

a. To configure only the Context Based Access Control (CABC) firewall on R1, use the **auto secure** command and specify the **firewall** option. Respond as shown in the following AutoSecure output to the AutoSecure questions and prompts. The responses are in bold.

```
R1#auto secure firewall
                --- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security of the router, but it will
not make it absolutely resistant to all security attacks ***

AutoSecure will modify the configuration of your device. All configuration
changes will be shown. For a detailed explanation of how the configuration
changes enhance security and any possible side effects, please refer to
Cisco.com for
Autosecure documentation.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]:  yes

   Enter the number of interfaces facing the internet [1]: 1

   Interface         IP-Address    OK? Method Status                Protocol
   FastEthernet0/0   unassigned    YES unset  administratively down down

   FastEthernet0/1   192.168.1.1   YES manual up                    up

   Serial0/0/0       10.1.1.1      YES SLARP  up                    up

   Serial0/0/1       unassigned    YES unset  administratively down down


   Enter the interface name that is facing the internet: serial0/0/0

   Configure CBAC Firewall feature? [yes/no]: yes

   This is the configuration generated:

   ip inspect audit-trail
   ip inspect dns-timeout 7
   ip inspect tcp idle-time 14400
   ip inspect udp idle-time 1800
   ip inspect name autosec_inspect cuseeme timeout 3600
   ip inspect name autosec_inspect ftp timeout 3600
   ip inspect name autosec_inspect http timeout 3600
```

```
ip inspect name autosec_inspect rcmd timeout 3600
ip inspect name autosec_inspect realaudio timeout 3600
ip inspect name autosec_inspect smtp timeout 3600
ip inspect name autosec_inspect tftp timeout 30
ip inspect name autosec_inspect udp timeout 15
ip inspect name autosec_inspect tcp timeout 3600
ip access-list extended autosec_firewall_acl
 permit udp any any eq bootpc
 deny ip any any
interface Serial0/0/0
 ip inspect autosec_inspect out
 ip access-group autosec_firewall_acl in
!
end

Apply this configuration to running-config? [yes]: yes

Applying the config generated to running-config

R1#
Feb 12 18:34:58.040: %AUTOSEC-5-ENABLED: AutoSecure is configured on the
device
```

Step 2: Review the AutoSecure CBAC configuration.

To which interface is the autosec_inspect name applied and in what direction? _____

a. To which interface is the ACL autosec_firewall_acl applied and in which direction? _____

b. What is the purpose of the ACL autosec_firewall_acl?

_____

Step 3: From PC-A, ping the R2 external WAN interface.

a. From PC-A, ping the R2 interface S0/0/0 at IP address 10.1.1.2.

b. Are the pings successful? Why or why not?

_____

Step 4: Add ICMP to the autosec_inspect list.

Configure R1 to inspect ICMP and allow ICMP echo replies from outside hosts with a timeout of 60 seconds.

Step 5: From PC-A, ping the R2 external WAN interface.

From PC-A, ping the R2 interface S0/0/0 at IP address 10.1.1.2.

Are the pings successful? Why or why not?

_____

Step 6: From R2, ping PC-A.

From R2 ping PC-A. Are the pings successful? Why or why not?

_____

Step 7: Test SSH access from PC-C to R1.

From external host PC-C, start a PuTTY session to R1.

Is the SSH session connection successful? Why or why not?

_____

Step 8: Configure the R1 firewall to allow SSH access from external hosts on the 192.168.3.0/24 network.

a. Display the Extended ACL named autosec_firewall_acl that is applied to S0/0/0 inbound.

```
R1#show access-list autosec_firewall_acl
Extended IP access list autosec_firewall_acl
    10 permit udp any any eq bootpc
    20 deny ip any any (57 matches)
```

b. Configure R1 to allow SSH access by adding a statement to the Extended ACL autosec_firewall_acl that permits the SSH TCP port 22.

```
R1(config)#ip access-list extended autosec_firewall_acl
R1(config-ext-nacl)#13 permit tcp 192.168.3.0 0.0.0.255 any eq 22
R1(config-ext-nacl)#end
```

c. From external host PC-C, start a PuTTY SSH session to R1 at IP address 10.1.1.1 and log in as RADIUS user RadAdmin with a password of RadAdminpa55.

d. From the SSH session on R1, display the modified Extended ACL autosec_firewall_acl.

```
R1#show access-list autosec_firewall_acl
Extended IP access list autosec_firewall_acl
    10 permit udp any any eq bootpc
    13 permit tcp 192.168.3.0 0.0.0.255 any eq 22 (16 matches)
    20 deny ip any any (60 matches)
```

Step 9: Configure the R1 firewall to allow NTP and VPN traffic.

a. Configure R1 to allow Network Time Protocol (NTP) updates from R2 by adding a statement to the Extended ACL autosec_firewall_acl that permits the NTP (UDP port 123).

```
R1(config)#ip access-list extended autosec_firewall_acl
R1(config-ext-nacl)#15 permit udp host 10.1.1.2 host 10.1.1.1 eq ntp
```

b. Configure R1 to allow IPsec VPN traffic between PC-A and R3 by adding a statement to the Extended ACL autosec_firewall_acl that permits the Ipsec Encapsulating Security Protocol (ESP).

Note: In Part 5 of the lab, R3 will be configured as a VPN server, and PC-A will be the remote client.

```
R1(config-ext-nacl)#18 permit esp any any
R1(config-ext-nacl)#end
```

c. Display the modified extended ACL autosec_firewall_acl.

```
R1#show access-list autosec_firewall_acl
Extended IP access list autosec_firewall_acl
    10 permit udp any any eq bootpc
    13 permit tcp 192.168.3.0 0.0.0.255 any eq 22 (67 matches)
    15 permit udp host 10.1.1.2 host 10.1.1.1 eq ntp (3 matches)
    18 permit esp any any
    20 deny ip any any (21 matches)
```

Step 10: Test Telnet access from internal PC-A to external router R2.

a. From PC-A, telnet to R2 at IP address 10.1.1.2 using the vty line password Cisc0vtypa55.

C:\>**telnet** `10.1.1.2`

Is the telnet attempt successful? Why or why not?

_____

b. Leave the Telnet session open.

Step 11: Display CBAC inspection sessions.

Display the IP inspect session to see the active Telnet session from PC-A to R2.

Task 9. Configure a ZBF Firewall on R3 (Chapter 4)

Step 1: Access SDM using HTTPS.

a. Start the SDM application or open a browser on PC-C and start SDM by entering the R3 IP address at **https://192.168.3.1** in the address field. Be sure to use HTTPS as the protocol.

b. At the security certificate warning, click **Continue to this website**.

c. Log in with no username and the enable secret password cisco12345.

d. In the Authentication Required dialog box and IOS IPS Login dialog box, do not enter a username but enter the enable secret password **cisco12345.**

Step 2: Use the SDM Firewall wizard to configure a ZBF on R3.

a. Click the **Configure** button at the top of the SDM screen, and then click **Firewall and ACL.**

b. Select **Basic Firewall** and click the **Launch the selected task** button. On the Basic Firewall Configuration wizard screen, click **Next**.

c. Check the **Inside (trusted)** check box fo**r FastEthernet0/1** and the **Outside (untrusted)** check box fo**r Serial0/0/1.** Click **Next**. Click **OK** when the SDM access warning is displayed.

d. Select **Low Security** and click **Next**. In the Summary window, click **Finish**.

e. Click **OK** in the Commands Delivery Status window.

Step 3: Verify ZBF functionality.

a. From PC-C, ping the R2 interface S0/0/1 at IP address 10.2.2.2.

Are the pings successful? Why or why not?

_____

b. From external router R2, ping PC-C at IP address 192.168.3.3

Are the pings successful? Why or why not? _____

c. From router R2, telnet to R3 at IP address 10.2.2.1.

Is the telnet successful? Why or why not? _____

d. From PC-C on the R3 internal LAN, telnet to R2 at IP address 10.2.2.2 and use password Cisc0vtypa55.

e. With the Telnet session open from PC-C to R2, issue the command **show policy-map type inspect zone-pair session** on R3. Continue pressing enter until you see an Inspect Established session section toward the end.

Step 4: Save the running configuration to the startup configuration.

Task 10. Configure Intrusion Prevention System (IPS) on R1 Using Cisco IOS (Chapter 5)

Step 1: (Optional) Install the TFTP server on PC-A.

If a TFTP server is not currently installed on PC-A, download Tftpd32 from http://tftpd32.jounin.net and install it on your desktop. If it is already installed, go to Step 2.

Step 2: Prepare the router and TFTP server.

To configure Cisco IOS IPS 5.x, the IOS IPS Signature package file and public crypto key files must be available on PC-A. Check with your instructor if these files are not on the PC. These files can be downloaded from Cisco.com with a valid user account that has proper authorization.

a. Verify that the IOS-S*xxx*-CLI.pkg signature package file is in a TFTP folder. The *xxx* is the version number and varies depending on which file was downloaded.

b. Verify that the realm-cisco.pub.key.txt file is available and note its location on PC-A. This is the public crypto key used by IOS IPS.

c. Verify or create the IPS directory in router flash on R1. From the R1 CLI, display the content of flash memory using the **show flash** command. Check whether the ipsdir directory exists and if it has files in it.

d. If the **ipsdir** directory is not listed, create it.

```
R1#mkdir ipsdir
Create directory filename [ipsdir]? Press Enter
Created dir flash:ipsdir
```

e. If the ipsdir directory exists and the signature files are in it, you must remove the files to perform this part of the lab. Switch to the ipsdir directory and verify that you are in it. Remove the files from the directory, and then return to the flash root directory when you are finished.

```
R1#cd ipsdir

R1#pwd
flash:/ipsdir/

R1#delete R1*
Delete filename [/ipsdir/R1*]?
Delete flash:/ipsdir/R1-sigdef-typedef.xml? [confirm]
```

```
Delete flash:/ipsdir/R1-sigdef-category.xml? [confirm]
Delete flash:/ipsdir/R1-sigdef-default.xml? [confirm]
Delete flash:/ipsdir/R1-sigdef-delta.xml? [confirm]
Delete flash:/ipsdir/R1-seap-delta.xml? [confirm]
Delete flash:/ipsdir/R1-seap-typedef.xml? [confirm]

R1#cd flash:/
R1#pwd
flash:/
```

Step 3: Open the IPS crypto key file and copy the contents to the router.

On PC-A, locate the crypto key file named realm-cisco.pub.key.txt and open it using Notepad or another text editor. On R1, enter global config mode, copy the contents of the file, and paste the contents to the router.

Step 4: Create an IPS rule.

On R1, create an IPS rule named **iosips**. This rule will be used later on an interface to enable IPS.

Step 5: Configure the IPS signature storage location in router flash memory.

Specify the location **flash:ipsdir** where the signature files will be stored.

Step 6: Configure Cisco IOS IPS to use a pre-defined signature category.

Retire all signatures in the “all” category and then unretire the ios_ips basic category.

Step 7: Apply the IPS rule to interfaces S0/0/0 and Fa0/1.

a. Apply the iosips rule that you created on the S0/0/0 interface in the inbound direction.

b. Apply the IPS rule to the R1 Fa0/1 interface in the inbound direction.

Step 8: Verify the IOS IPS signature package location and TFTP server setup.

a. Verify connectivity between R1 and PC-A, the TFTP server.

b. Verify that the PC has the IPS signature package file in a directory on the TFTP server. This file is typically named IOS-S*xxx*-CLI.pkg, where *xxx* is the signature file version.

Note: If this file is not present, contact your instructor before continuing.

c. Start the TFTP server and set the default directory to the one that contains the IPS signature package.

Step 9: Copy the signature package from the TFTP server to the router.

Use the **copy tftp** command to retrieve the signature file. Be sure to use the **idconf** keyword at the end of the **copy** command.

Note: Immediately after the signature package is loaded to the router, signature compiling begins. Allow time for this process to complete. It can take several minutes.

a. Display the contents of the ipsdir directory created earlier.

b. Use the **`show ip ips all`** command to see an IPS configuration status summary. To which interfaces and in which direction is the iosips rule applied? _____

Step 10: Save the running configuration to the startup configuration.

Task 11. Configure IPS on R3 Using SDM (Chapter 5)

Step 1: (Optional) Install the TFTP server on PC-C.

If a TFTP server is not currently installed on PC-C, download Tftpd32 from http://tftpd32.jounin.net and install it on your desktop. If it is already installed, go to Step 2.

Step 2: Prepare the router and TFTP server.

To configure Cisco IOS IPS 5.x, the IOS IPS signature package file and public crypto key files must be available on PC-A. Check with your instructor if these files are not on the PC. These files can be downloaded from Cisco.com with a valid user account that has proper authorization.

a. Verify that the IOS-S*xxx*-CLI.pkg signature package file is in a TFTP folder. The *xxx* is the version number and varies depending on which file was downloaded.

b. Verify that the realm-cisco.pub.key.txt file is available and note its location on PC-A. This is the public crypto key used by Cisco IOS IPS.

c. Verify or create the IPS directory in router flash on R1. From the R1 CLI, display the content of flash memory and check to see if the ipsdir directory exists.

d. If the ipsdir directory is not listed, create it in privileged EXEC mode.

Step 3: Verify the IOS IPS signature package and TFTP server setup.

a. Verify connectivity between R3 and PC-C, the TFTP server, using the **`ping`** command.

b. Verify that the PC has the IPS signature package file in a directory on the TFTP server. This file is typically named IOS-S*xxx*-CLI.pkg, where *xxx* is the signature file version.

Note: If this file is not present, contact your instructor before continuing.

c. Start Tftpd32 or another TFTP server and set the default directory to the one with the IPS signature package in it. Take note of the filename for use in the next step.

Step 4: Access SDM using HTTPS.

a. Start the SDM application or open a browser on PC-C and start SDM by entering the R3 IP address at **https://192.168.3.1** in the address field. Be sure to use HTTPS as the protocol.

b. At the security certificate warning, click **Continue to this website**.

c. Log in with no username and the enable secret password cisco12345.

d. In the Authentication Required dialog box and IOS IPS Login dialog box, do not enter a username but enter the enable secret password **cisco12345.**

Step 5: Use the SDM IPS Wizard to configure IPS.

a. Click the **Configure** button at the top of the SDM screen and then select **Intrusion Prevention > Create IPS**. Click the **Launch IPS Rule Wizard** button to begin the IPS configuration. If prompted regarding SDEE notification, click **OK**. Click **Next** at the welcome screen.

b. Apply the IPS rule in the inbound direction for FastEthernet0/1 and Serial0/0/1. Click **Next**.

c. In the Signature File and Public Key window, specify the signature file with a URL and use TFTP to retrieve the file from PC-C. Enter the IP address of the PC-C TFTP server and the filename. Click **OK**.

d. In the Signature File and Public Key window, enter the name of the public key file realm-cisco.pub.

e. Open the public key file and copy the text that is between the phrase “key-string” and the word “quit.” Paste the text into the **Key** field in the Configure Public Key section. Click **Next**.

f. In the Config Location and Category window, specify **flash:/ipsdir** as the location to store the signature information. Click **OK**.

g. In the **Choose Category** field of the Config Location and Category window, choose **basic**.

h.Click **Next** to display the Summary window, and click **Finish** to deliver the commands to the router. Click **OK**.

Note: Allow the signature configuration process to complete. This can take several minutes.

Step 6: (Optional) Verify IPS functionality with SDM Monitor and SuperScan.

If SuperScan is not on PC-C, download the SuperScan 4.0 tool from the Scanning Tools group at http://www.foundstone.com.

a. Start SuperScan on PC-C. Click the **Host and Service Discovery** tab. Check the **Timestamp Request** check box, and uncheck the **Echo Request** check box. Scroll the UDP and TCP port selection lists and notice the range of ports that will be scanned.

b. Click the **Scan** tab and enter the IP address of R2 S0/0/1 (10.2.2.2) in the **Hostname/IP** field.

Note: You can also specify an address range, such as 10.1.1.1 to 10.1.1.254, by entering an address in the **Start IP** and **End IP** fields. The program scans all hosts with addresses in the range specified.

c**.** Click the button with the blue arrow in the lower left corner of the screen to start the scan.

Step 7: Check the results with SDM logging.

a. From Cisco SDM, choose **Monitor > Logging**.

b. Click the **Update** button. You will see that Cisco IOS IPS has been logging the port scans generated by SuperScan.

c. What syslog messages did you see? You should see syslog messages on R3 and entries in the SDM Monitor Log with descriptions that include one of these phrases: “Invalid DHCP Packet” or “DNS Version Request.”

Step 8: Save the running configuration to the startup configuration.

Task 12. Back Up and Secure the Cisco Router IOS Image and Configuration Files (Chapter 2)

Note: The procedures described here can also be used to back up the switch IOS images and configuration files.

Step 1: Back up the IOS Image from R1 and R3 to a TFTP server.

Create a directory for the IOS images on PC-A and PC-C.

a. Start the TFTP server on PC-A and select the IOS images directory as the default directory.

b. Copy the R1 IOS image to the PC-A TFTP server as a backup in case the current image becomes corrupted.

c. Start the TFTP server on PC-C and select the IOS images directory as the default directory.

d. Copy the R3 IOS image to the TFTP server as a backup in case the current image becomes corrupted.

Note: The IOS image on R1 should be the same as the one for R3, so a single backup could suffice for both routers.

Step 2: Back up the configuration files from R1 and R3 to a TFTP server.

Create a directory for configurations on PC-A and PC-C.

a. Start the TFTP server on PC-A and select the Configs directory as the default directory.

b. Copy the R1 startup-config file to the PC-A TFTP server as a backup.

Note: If changes have been made to the running config, you can save them to the startup config before backing up the config file.

c. Start the TFTP server on PC-C and select the Configs directory as the default directory.

d. Copy the R3 startup-config file to the PC-C TFTP server as a backup.

Step 3: Secure the Cisco IOS image and archive a copy of the running configuration for R1 and R3.

a. Secure the IOS boot image to enable Cisco IOS image resilience and hide the file from **`dir`** and **`show`** commands.

b. Secure the router running configuration and securely archive it in persistent storage (flash).

Step 4: Verify that the image and configuration are secured.

Display the status of configuration resilience and the primary bootset filename.

Part 4. Secure Network Switches (Chapter 6)

Task 1: Configure Passwords and a Login Banner on All Switches (Chapter 2)

Step 1: Configure the enable secret password.

Use an enable secret password of cisco12345.

Step 2: Encrypt a plaintext password.

Step 3: Configure the console line.

Configure a console password of ciscoconpass and enable login. Set the `exec-timeout` to log out after 5 minutes of inactivity. Prevent console messages from interrupting command entry.

Note: The vty lines for the switches are configured for SSH in Task 2.

Step 4: Configure a login warning banner.

Configure a warning to unauthorized users with a message-of-the-day (MOTD) banner that says "`Unauthorized access strictly prohibited and prosecuted to the full extent of the law`".

Step 5: Disable HTTP access.

HTTP access to the switch is enabled by default. To prevent HTTP access, disable the HTTP server and HTTP secure server.

Task 2. Configure Switches as NTP Clients (Chapter 2)

Note: Router R2 is the master NTP server. All other routers and switches learn their time from it, either directly or indirectly.

Step 1: Configure S1, S2, and S3 to become NTP clients of R2.

Step 2: Verify that S1 has made an association with R2.

Task 3. Configure Syslog Support on All Switches (Chapter 2)

Step 1: (Optional) Install the syslog server on PC-A and PC-C.

If a syslog server is not currently installed on the host, download the latest version of Kiwi from http://www.kiwisyslog.com or Tftpd32 from http://tftpd32.jounin.net and install it on your desktop. If it is already installed, go to Step 2.

Step 2: Configure S1 to log messages to the PC-A syslog server.

a. Verify that you have connectivity between S1 and host PC-A by pinging the S1 VLAN 1 interface IP address 192.168.1.11 from PC-A. If it is not successful, troubleshoot as necessary before continuing.

b. Configure the syslog service on the switch to send syslog messages to the syslog server.

Task 4. Configure the SSH Server on All Switches (Chapter 2)

Step 1: Configure a domain name.

Enter global configuration mode and set the domain name.

Step 2: Configure a privileged user for login from the SSH client.

Use the **username** command to create the user ID with the highest possible privilege level and a secret password.

Step 3: Configure the incoming vty lines.

a. Configure vty access on lines 0 through 4. Specify that a privilege level of 15 is required to access the vty lines, use the local user accounts for mandatory login and validation, and accept only SSH connections.

b. Disable login for switch vty lines 5 through 15.

Step 4: Generate the RSA encryption key pair.

The switch uses the RSA key pair for authentication and encryption of transmitted SSH data. Configure the RSA keys with 1024 for the number of modulus bits.

Step 5: Verify SSH connectivity to S1 from the SSH client PC-A.

If the SSH client is not already installed, download either TeraTerm or PuTTY.

a. Launch the client, enter the VLAN 1 IP address, and enter the Admin01 username and password.

b. Close the PuTTY SSH session window with the **exit** or **quit** command.

c. Try to open a Telnet session to switch S1 from PC-A. Are you able to open the Telnet session? Why or why not? _____

Task 5. Configure Authentication Using AAA and RADIUS on All Switches (Chapter 3)

Step 1: (Optional) Download and configure the WinRadius software.

a. If WinRadius is not currently installed on PC-A and PC-C, download the latest version from http://www.suggestsoft.com/soft/itconsult2000/winradius/. There is no installation setup. The extracted WinRadius.exe file is executable.

b. Start the WinRadius.exe application. If the application is being started for the first time, follow the instructions to configure the WinRadius server database.

Step 2: Configure users and passwords on the WinRadius server.

Note: If the RADIUS user accounts were previously configured, you can skip this step. If the RADIUS server has been shut down and restarted, you must recreate the user accounts.

a**.** Add username **RadAdmin** with a password of **RadAdminpa55.**

b. Add username **RadUser** with a password of **RadUserpa55**.

Step 3: Enable AAA.

Create a AAA new model to enable AAA.

Step 4: Configure the default login authentication list.

Configure the list to first use RADIUS for the authentication service and then local**,** to allow access based on the local switch database if a RADIUS server cannot be reached.

Step 5: Verify connectivity between S1 and the PC-A RADIUS server.

Ping from S1 to PC-A.

If the pings are not successful, troubleshoot the PC and switch configuration before continuing.

Step 6: Specify a RADIUS server.

Configure the switch to access the RADIUS server at PC-A. Specify auth-port 1812 and acct-port 1813, along with the IP address and secret key of WinRadius for the RADIUS server.

Step 7: Test the RADIUS configuration by logging in to the console on S1.

a. Exit to the initial router screen that displays the following: R1 con0 is now available, Press RETURN to get started.

b. Log in with the username RadAdmin and password RadAdminpass. Can you log in with minimal delay?

_____

Note: If you exit the WinRadius server and restart it, you must recreate the user accounts from Step 2.

Step 8: Test your configuration by connecting to S1 with SSH.

Clear the log on the WinRadius server by selecting **Log > Clear**.

a. Use PuTTY or another terminal emulation client to open an SSH session from PC-A to S1.

b. At the login prompt, enter the username RadAdmin defined on the RADIUS server and a password of RadAdminpa55.

Are you able to login to R1? _____

Task 6. Secure Trunk Ports (Chapter 6)

Step 1: Configure trunk ports on S1 and S2.

a. Configure port Fa0/1 on S1 as a trunk port.

b. Configure port Fa0/1 on S2 as a trunk port.

c. Verify that S1 port Fa0/1 is in trunking mode.

Step 2: Change the native VLAN for the trunk ports on S1 and S2.

Changing the native VLAN for trunk ports to an unused VLAN helps prevent VLAN hopping attacks.

a. Set the native VLAN on the S1 Fa0/1 trunk interface to an unused VLAN 99.

b. Set the native VLAN on the S2 Fa0/1 trunk interface to VLAN 99.

Step 3: Prevent the use of DTP on S1 and S2.

Set the trunk ports on S1 and S2 so that they do not negotiate by turning off the generation of DTP frames.

Step 4: Verify the trunking configuration on port Fa0/1.

Step 5: Enable storm control for broadcasts.

Enable storm control for broadcasts on the trunk port with a 50 percent rising suppression level using the **`storm-control broadcast`** command.

Step 6: Verify the configuration with the show run command.

Task 7. Secure Access Ports (Chapter 6)

By manipulating the STP root bridge parameters, network attackers hope to spoof their system, or a rogue switch that they add to the network, as the root bridge in the topology. If a port that is configured with PortFast receives a BPDU, STP can put the port into the blocking state by using a feature called BPDU guard.

Step 1: Disable trunking on S1, S2, and S3 access ports.

a. On S1, configure ports Fa0/5 and F0/6 as access mode only.

b. On S2, configure Fa0/18 as access mode only.

c. On S3, configure ports Fa0/5 and Fa0/18 as access mode only.

Task 8. Protect Against STP Attacks (Chapter 6)

The topology has only two switches and no redundant paths, but STP is still active. In this step, you enable some switch security features that can help reduce the possibility of an attacker manipulating switches via STP-related methods.

Step 1: Enable PortFast on S1, S2, and S3 access ports.

PortFast is configured on access ports that connect to a single workstation or server to enable them to become active more quickly.

a. Enable PortFast on the S1 Fa0/5 and Fa0/6 access ports.

b. Enable PortFast on the S2 Fa0/18 access port.

c. Enable PortFast on the S3 Fa0/5 and Fa0/18 access port.

Step 2: Enable BPDU guard on the S1, S2, and S3 access ports.

BPDU guard is a feature that can help prevent rogue switches and spoofing on access ports. Enable BPDU guard on the switch ports previously configured as access only.

Task 9. Configure Port Security and Disable Unused Ports (Chapter 6)

Step 1: Configure basic port security.

Shut down all end-user access ports that are in use and enable basic default port security. This sets the maximum MAC addresses to 1 and the violation action to shutdown. Reissue the port security command using the **`sticky`** option to allow the secure MAC address that is dynamically learned on a port to the switch running configuration. Re-enable each access port to which port security was applied.

Step 2: Disable unused ports on S1 and S2.

As a further security measure, disable any ports not being used on the switch.

Ports Fa0/1, Fa0/5, and Fa0/6 are used on switch S1. Shut down the remaining Fast Ethernet ports and the two Gigabit Ethernet ports.

Ports Fa01/ and Fa0/18 are used on switch S2. Shut down the remaining Fast Ethernet ports and the two Gigabit Ethernet ports.

Ports Fa0/5 and Fa0/18 are used on switch S3. Shut down the remaining Fast Ethernet ports and the two Gigabit Ethernet ports.

Step 3: (Optional) Move active ports to another VLAN and change the management VLAN.

As a further security measure, you can move all active end-user and router ports to a VLAN other than the default VLAN 1 on the switches. You can also change the management VLAN from VLAN 1 to another VLAN, but you must have at least one end-user host port in that VLAN to manage the switch remotely using Telnet, SSH, or HTTP.

Note: The following configuration allows you to manage either switch remotely from either PC-A or PC-B. You can only access the switches remotely using SSH, because Telnet and HTTP have been disabled. The procedure for switch S3 is also shown.

Configure a new VLAN for users on each switch using the following commands.

Note: You could also configure VLAN 10 on switch S3, but it would not communicate with VLAN 10 on switches S1 and S2.

```
S1(config)#vlan 10
S1(config-vlan)#name Users

S2(config)#vlan 10
S2(config-vlan)#name Users

S3(config)#vlan 30
S3(config-vlan)#name Users
```

a. Add the current active access (non-trunk) ports to the new VLAN.

```
S1(config)#interface range fa0/5 – 6
S1(config-if)#switchport access vlan 10

S2(config)#interface fa0/18
S2(config-if)#switchport access vlan 10

S3(config)#interface fa0/5
S3(config-if)#switchport access vlan 30

S3(config)#interface fa0/18
S3(config-if)#switchport access vlan 30
```

b. On each switch, remove the management VLAN IP address from VLAN 1 (configured in Part 1 of the lab) and shut it down. The following example is for switch S1.

```
S1(config)#interface vlan 1
S1(config-if)#no ip address
S1(config-if)#shutdown
```

c. Configure a management VLAN IP address for the VLAN 10 interface on S1 and S2 and enable it.

```
S1(config)#interface vlan 10
S1(config-if)#ip address 192.168.1.11 255.255.255.0
S1(config-if)#no shutdown

S2(config)#interface vlan 10
S2(config-if)#ip address 192.168.1.12 255.255.255.0
S2(config-if)#no shutdown
```

d. Configure a management VLAN IP address for the VLAN 30 interface on S3 and enable it.

```
S3(config)#interface vlan 30
S3(config-if)#ip address 192.168.3.11 255.255.255.0
S3(config-if)#no shutdown
```

Step 4: Save the running-config to the startup-config.

Part 5. Configuring VPN Remote Access

In Part 5, you configure a remote access IPsec VPN. R3 is configured as an Easy VPN server using SDM, and the Cisco VPN Client is configured on PC-A. The PC-A host simulates an employee connecting from home or a remote office over the Internet. Router R2 simulates an Internet ISP router.

Task 1. Use the SDM VPN Wizard to Configure the Easy VPN Server (Chapter 8)

Step 1: Access SDM using HTTPS.

a. Start the SDM application or open a browser on PC-C and start SDM by entering the R3 IP address at https://192.168.3.1 in the address field. Be sure to use HTTPS as the protocol.

b. At the security certificate warning, click **Continue to this website**.

c. Log in with no username and the enable secret password cisco12345.

d. In the Authentication Required dialog box and IOS IPS Login dialog box, do not enter a username, but enter enable secret password **cisco12345.**

Step 2: Launch the Easy VPN Server Wizard.

a. Click the **Configure** button at the top of the SDM home screen and click the **VPN** task button to view the VPN configuration page.

b. Select **Easy VPN Server** from the main VPN window, and then click **Launch Easy VPN Server Wizard**.

Note: The Easy VPN Server Wizard checks the router configuration to see if AAA is enabled. If AAA is not enabled, the Enable AAA window displays. AAA was enabled on the router previously.

Step 3: Configure the virtual tunnel interface and authentication.

Select the interface on which the client connections terminate. Click the **Unnumbered to** radio button, and select the **Serial0/0/1** interface from the pull-down menu.

Select **Pre-shared Keys** for the authentication type and click **Next** to continue.

Step 4: Select an IKE proposal.

In the Internet Key Exchange (IKE) Proposals window, the default IKE proposal is used for R3. Click **Next** to accept the default IKE policy.

Step 5: Select the transform set.

In the Transform Sets window, the default SDM transform set is used. Click **Next** to accept the default transform set.

Step 6: Specify the group authorization and group policy lookup.

In the Group Authorization and Group Policy Lookup window, select the **Local** option.

Click **Next** to create a new AAA method list for group policy lookup that uses the local router database.

Step 7: Configure user authentication (XAuth).

In the User Authentication (Xauth) window, check the **Enable User Authentication** check box and select **Local Only**.

a. Click the **Add User Credentials** button. In the User Accounts window, you can view currently defined local users or add new users. Which user account is currently defined locally? _____

b. Add the new user **VPNUser1** with a password of **VPNUser1pa55** and click **OK**.

c. Click **OK** to close the User Accounts window. Click **Next**.

Step 8: Specify group authorization and user group policies.

In the Group Authorization and User Group Policies window, you must create at least one group policy for the VPN server.

Click **Add** to create a group policy.

a. In the Add Group Policy window, enter **VPN-Access** in the **Name of This Group** field. Enter a new pre-shared key of **cisco12345** and then re-enter it. Leave the **Pool Information** box checked. Enter a starting address of **192.168.3.200**, an ending address of **192.168.3.250**, and a subnet mask of **255.255.255.0**.

b. Click **OK** to accept the entries.

c. An SDM warning message displays indicating that the IP address pool and the Fast Ethernet 0/1 address are in the same subnet. Click **Yes** to continue.

d. Check the **Configure Idle Timer** check box and enter 1 hour, 0 minutes, and 0 seconds.

e. When the Cisco Tunneling Control Protocol (cTCP) window displays, do not enable cTCP. Click **OK** if a firewall warning message displays. Click **Next** to continue.

f. When the Easy VPN Server Pass-through Configuration window displays, make sure that the **Action Modify** check box is checked. This option allows SDM to modify the firewall on S0/0/1 to allow IPsec VPN traffic to reach the internal LAN.

Step 9: Review the configuration summary and deliver the commands.

Scroll through the commands that SDM will send to the router. Click **Finish**.

Step 10: Test the VPN Server

You are returned to the main VPN window with the Edit VPN Server tab selected. Click the **Test VPN Server** button in the lower right corner of the screen. In the VPN Troubleshooting window, click the **Start** button. Click **Close** to exit the VPN Troubleshooting window.

Task 2. Use the Cisco VPN Client to Test the Remote Access VPN (Chapter 8)

Step 1: (Optional) Install the Cisco VPN client.

If the Cisco VPN Client software is not already installed on host PC-A, install it now. If you do not have the Cisco VPN Client software or are unsure of the process, contact your instructor.

Step 2: Configure PC-A as a VPN client to access the R3 VPN server.

Start the Cisco VPN Client. Select **Connection Entries > New** or click the **New** icon with the plus sign (+) on it.

Enter the following information to define the new connection entry. Click **Save** when you are finished.

Connection Entry: **VPN-Corp**

Description: **Connection to R3 corporate network**

Host: **10.2.2.1** (IP address of the R3 S0/0/1 interface)

Group Authentication Name: **VPN-Access** (specifies the address pool configured in Task 2)

Password: **cisco12345** (pre-shared key configured in Task 2)

Confirm Password: **cisco12345**

Note: The group authentication name and password are case-sensitive and must match the ones created on the VPN Server.

Step 3: Test access from PC-A without a VPN connection.

Note: In the previous step, you created a VPN connection entry on the VPN client computer PC-A, but have not activated it yet.

Open a command prompt on PC-A and ping the PC-C IP address at 192.168.3.3 on the R3 LAN. Are the pings successful? Why or why not?

_____

_____

Step 4: Establish a VPN connection and login.

Select the newly created connection **VPN-Corp** and click the **Connect** icon. You can also double-click the connection entry.

a. When the VPN Client User Authentication dialog box displays, enter the username **VPNUser1** created previously on the VPN router R3, and enter the password of **VPNUser1pa55**. Click **OK** to continue. The VPN Client window minimizes to a lock icon in the tools tray of the taskbar. When the lock is closed, the VPN tunnel is up. When it is open, the VPN connection is down.

Step 5: Test access from the client with the VPN connection.

With the VPN connection from computer PC-A to router R3 activated, open a command prompt on PC-A and ping the R3 default gateway at 192.168.3.1. Then ping the PC-C IP address at 192.168.3.3 on the R3 LAN. Are the pings successful? Why or why not?

_____

_____

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1700	Fast Ethernet 0 (FA0)	Fast Ethernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2600	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
2800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Router Interface Summary
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.