CCNA Security

Chapter 9 Lab A: Security Policy Development and Implementation

Topology

Note: ISR G2 devices have Gigabit Ethernet interfaces instead of Fast Ethernet Interfaces.
### 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 hostnames, 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 CCP to disable unneeded services.
- Configure a CBAC firewall.
- Configure a ZBF firewall.
- Configure intrusion prevention system (IPS) using Cisco IOS and CCP.
- Back up and secure the Cisco IOS image and configuration files.

**Part 4: Secure Network Switches**
- Configure passwords, and a login banner.

### IP Addressing Table

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>Default Gateway</th>
<th>Switch Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>FA0/1</td>
<td>192.168.1.1</td>
<td>255.255.255.0</td>
<td>N/A</td>
<td>S1 FA0/5</td>
</tr>
<tr>
<td></td>
<td>S0/0/0 (DCE)</td>
<td>10.1.1.1</td>
<td>255.255.255.252</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>R2</td>
<td>S0/0/0</td>
<td>10.1.1.2</td>
<td>255.255.255.252</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>S0/0/1 (DCE)</td>
<td>10.2.2.2</td>
<td>255.255.255.252</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>R3</td>
<td>FA0/1</td>
<td>192.168.3.1</td>
<td>255.255.255.0</td>
<td>N/A</td>
<td>S3 FA0/5</td>
</tr>
<tr>
<td></td>
<td>S0/0/1</td>
<td>10.2.2.1</td>
<td>255.255.255.252</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>S1</td>
<td>VLAN 1</td>
<td>192.168.1.11</td>
<td>255.255.255.0</td>
<td>192.168.1.1</td>
<td>N/A</td>
</tr>
<tr>
<td>S2</td>
<td>VLAN 1</td>
<td>192.168.1.12</td>
<td>255.255.255.0</td>
<td>192.168.1.1</td>
<td>N/A</td>
</tr>
<tr>
<td>S3</td>
<td>VLAN 1</td>
<td>192.168.3.11</td>
<td>255.255.255.0</td>
<td>192.168.3.1</td>
<td>N/A</td>
</tr>
<tr>
<td>PC-A</td>
<td>NIC</td>
<td>192.168.1.3</td>
<td>255.255.255.0</td>
<td>192.168.1.1</td>
<td>S1 FA0/6</td>
</tr>
<tr>
<td>PC-B</td>
<td>NIC</td>
<td>192.168.1.2</td>
<td>255.255.255.0</td>
<td>192.168.1.1</td>
<td>S2 FA0/18</td>
</tr>
<tr>
<td>PC-C</td>
<td>NIC</td>
<td>192.168.3.3</td>
<td>255.255.255.0</td>
<td>192.168.3.1</td>
<td>S3 FA0/18</td>
</tr>
</tbody>
</table>
• 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 CCP 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 e-mail, 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 (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 7 with CCP 2.5, RADIUS, TFTP, and syslog servers plus PuTTY and Cisco VPN Client software available
PC-B: Windows XP, Vista, or Windows 7
PC-C: Windows XP, Vista, or Windows 7 with CCP 2.5, RADIUS, TFTP, and syslog servers plus PuTTY software available and SuperScan (optional)
Serial and Ethernet cables as shown in the topology
Rollover cables to configure the routers via the console

**CCP Notes:**
- Refer to Chp 00 Lab A for instructions on how to install and run CCP. Hardware/software recommendations for CCP include Windows XP, Vista, or Windows 7 with Java version 1.6.0_11 up to 1.6.0_21, Internet Explorer 6.0 or above and Flash Player Version 10.0.12.36 and later.
- If the PC on which CCP is installed is running Windows Vista or Windows 7, it may be necessary to right-click on the CCP icon or menu item, and choose Run as administrator.
- In order to run CCP, it may be necessary to temporarily disable antivirus programs and O/S firewalls. Make sure that all pop-up blockers are turned off in the browser.

**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.**


**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.
   a. In the next window, click the SECURITY POLICY INTERVIEW link to begin the interview.
   b. In the first SECURITY POLICY INTERVIEW window, select 51-100 employees for Company Size. Click Next to continue.
   c. 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.
d. For Advanced Technologies, click Yes for the question regarding whether the organization deploys security, VPN, and firewall? Click No for wireless, IP communications (VoIP), and storage. Click Next to continue.

e. For Remote Access, click Yes – For employees only. Click Next to continue.
f. In the SECURITY POLICY RESULTS window, enter your e-mail address and accept the disclaimer. Click Send Security Policy.

Note: The security policy is e-mailed to you as a Word document.

Step 3: Review the basic security policy.

a. 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.
b. What portions of the generated basic SPB policy are related to technical policies?

c. Select a fictitious company name and write it here: ________________________________

d. 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.

e. 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 e-mail 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.
   a. Configure hostnames 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.
   d. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were hostnames.

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.
   a. Configure hostnames as shown in the topology.
   b. Configure the VLAN 1 management addresses as shown in the IP Addressing table.
   c. 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.
   d. Disable DNS lookup to prevent the switches from attempting to translate incorrectly entered commands as though they were hostnames.

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 pass word 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 the pings are 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 the pings are 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.
   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.

   Note: If WinRadius is used on a PC that uses the Microsoft Windows Vista operating system or the Microsoft Windows 7 operating system, ODBC may fail to create successfully because it cannot write to the registry.

   Possible solutions:
   1. Compatibility settings:
      a. Right click on the WinRadius.exe icon and select Properties.
      b. While in the properties dialog box, select the Compatibility tab. In this tab, select the checkbox for Run this program in compatibility mode for. Then in the drop down menu below, choose Windows XP (Service Pack 3) for example, if it is appropriate for your system.
      c. Click OK.
   2. Run as Administrator settings:
      a. Right click on the WinRadius.exe icon and select Properties.
      b. While in the properties dialog box, select the Compatibility tab. In this tab, select the checkbox for Run this program as administrator in the Privilege Level section.
      c. Click OK.
3. **Run as Administration** for each launch:
   a. Right click on the WinRadius.exe icon and select **Run as administrator**.
   b. When WinRadius launches, click **Yes** in the User Account Control dialog box.

**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.**
   a. Clear the log display for the WinRadius server by choosing **Log > Clear**.
   b. Use PuTTY or another terminal emulation client to open an SSH session from PC-A to R1.
   c. At the login prompt, enter the username **RadAdmin** defined on the RADIUS server and the password **RadAdminpa55**.
      Are you able to login to R1? 
   d. Exit the SSH session.
   e. Stop the WinRadius server on PC-A by choosing **Operation > Exit**.
   f. Open an SSH session and attempt to log in again as **RadAdmin**.
      Are you able to login to R1? 
   g. 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 CLI to Disable Unneeded Services on R1 and Secure Against Login Attacks (Chapter 2)

Step 1: Use 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.

a. 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 via CCP. If you want secure access to the router via CCP, you can enable it using the command `ip http secure-server`.

b. For each serial interface, disable the following interface services.

```
ip redirects
ip proxy-arp
ip unreachables
ip directed-broadcast
ip mask-reply
```

c. 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 CCP to Disable Unneeded Services on R3 (Chapter 2)

Step 1: Configure user credentials for HTTP router access prior to starting CCP.
   a. Enable the HTTP server on R3.
      
      R3(config)# ip http server
      
      Or enable the HTTP secure server to connect securely.
   b. Create an admin account on R3 with privilege level 15 for use with AAA and CCP.
      
      R3(config)# username admin privilege 15 password 0 cisco12345
   c. Have CCP use the local database to authenticate web sessions.
      
      R2(config)# ip http authentication local

Step 2: Access CCP and discover R3.
   a. Run the CCP application on PC-C. In the Select/Manage Community window, input the R3 IP address 192.168.3.1 in the first IP Address/Hostname field. Enter admin in the Username field, and cisco12345 in the Password field. Click on the OK button.
   b. At the CCP Dashboard, click the Discovery button to discover and connect to R3. If the discovery process fails, use the Discover Details button to determine the problem in order to resolve the issue.

Step 3: Begin the security audit.
   a. Choose Configure > Security > Security Audit and click the Perform Security Audit button. Click Next at the welcome screen
   b. Choose 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 Close.
   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 (CBAC) 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

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP-Address</th>
<th>OK? Method Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>FastEthernet0/0/0</td>
<td>unassigned</td>
<td>YES unset</td>
<td>administratively down down</td>
</tr>
<tr>
<td>FastEthernet0/1</td>
<td>192.168.1.1</td>
<td>YES manual</td>
<td>up</td>
</tr>
<tr>
<td>Serial0/0/0</td>
<td>10.1.1.1</td>
<td>YES SLARP</td>
<td>up</td>
</tr>
<tr>
<td>Serial0/0/1</td>
<td>unassigned</td>
<td>YES unset</td>
<td>administratively down down</td>
</tr>
</tbody>
</table>

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 autosecInspect cuseeme timeout 3600
ip inspect name autosecInspect ftp timeout 3600
ip inspect name autosecInspect http timeout 3600
ip inspect name autosecInspect rcmd timeout 3600
ip inspect name autosecInspect realtime timeout 3600
ip inspect name autosecInspect smtp timeout 3600
ip inspect name autosecInspect tftp timeout 30
ip inspect name autosecInspect udp timeout 15
ip inspect name autosecInspect 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 autosecInspect out
    ip access-group autosec_firewall_acl in

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.
   a. To which interface is the autosec_inspect name applied and in what direction? ________________
   b. To which interface is the ACL autosec_firewall_acl applied and in which direction? ________________
   c. 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.
   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 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 (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 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 ciscovtypass.

   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: Use CCP to discover R3.

a. Run the CCP application on PC-C. In the Select/Manage Community window, input the R3 IP address 192.168.3.1 in the first IP Address/Hostname field. Enter admin in the Username field, and cisco12345 in the Password field. Click on the OK button.
b. At the CCP Dashboard, click on the Discovery button to discover and connect to R3. If the discovery process fails, use the Discover Details button to determine the problem in order to resolve the issue.

Step 2: Use the CCP Firewall wizard to configure a ZBF on R3.

a. Click the Configure button at the top of the CCP screen, and then click Security > Firewall > Firewall.

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 for Fast Ethernet0/1 and the Outside (untrusted) check box for Serial0/0/1. Click Next. Click OK when the CCP access warning is displayed.

d. Choose 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 attempt 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 ciscovtypass.

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](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-Sxxx-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.

```bash
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 the directory. Remove the files from the directory, and then return to the flash root directory when you are finished.

```bash
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-Sxxx-CLI.pkg`, where `xxx` is the signature file version.
Note: Use the newest signature file available if the router memory can support it. If a signature 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.

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. Allow time for this process to complete. It can take several minutes.

b. Display the contents of the `ipsdir` directory created earlier.

c. 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 CCP (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](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-C. 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-Sxxx-CLI.pkg` signature package file is in a TFTP folder. The `xxx` is the version number and varies depending on which file was downloaded.

   Note: Use the newest signature file available if the router memory can support it. If a signature file is not present, contact your instructor before continuing.

b. Verify that the `realm-cisco.pub.key.txt` file is available and note its location on PC-C. 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-Sxxx-CLI.pkg`, where `xxx` is the signature file version number.

   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: Configure R3 to allow CCP Access and Discovery.

a. Enable the HTTP server on R3.
   Or enable the HTTP secure server to connect securely.

b. Create an admin account on R3 with privilege level 15 and password cisco12345 for use with AAA and CCP.

c. Have CCP use the local database to authenticate web sessions.

d. Run the CCP application on PC-C. In the Select/Manage Community window, input R3 IP address 192.168.3.1 in the first IP Address/Hostname field. Enter admin in the Username field, and cisco12345 in the Password field. Click on the OK button.

e. At the CCP Dashboard, click on the Discover button to discover and connect to R3. If the discovery process fails, use the Discover Details button to determine the problem in order to resolve the issue.

Step 5: Use the CCP IPS wizard to configure IPS.

a. Click the Configure button at the top of the CCP screen and then choose Security > 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 OK.

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 CCP Monitor and SuperScan.

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. 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.

c. 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.

d. 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 CCP logging.

a. From Cisco CCP, choose Monitor > Router > 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?

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.

a. Create a directory for the IOS images on PC-A and PC-C.
b. Start the TFTP server on PC-A and choose the IOS images directory as the default directory.
c. Copy the R1 IOS image to the PC-A TFTP server as a backup in case the current image becomes corrupted.
d. Start the TFTP server on PC-C and choose the IOS images directory as the default directory.
e. 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.

a. Create a directory for configurations on PC-A and PC-C.
b. Start the TFTP server on PC-A and choose the Configs directory as the default directory.
c. 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.
d. Start the TFTP server on PC-C and choose the Configs directory as the default directory.
e. 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 the pings are 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.**

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

b. Launch the client, enter the VLAN 1 IP address, and enter the Admin01 username and password.

c. Close the PuTTY SSH session window with the `exit` or `quit` command.

d. 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.**


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. 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.**

a. Clear the log on the WinRadius server by choosing **Log > Clear**.

b. Use PuTTY or another terminal emulation client to open an SSH session from PC-A to S1.

c. At the login prompt, enter the username **RadAdmin** defined on the RADIUS server and a password of **RadAdminpass**.

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 his or her system as the root bridge in the topology. Alternatively, they can spoof a rogue switch that they added to the network as the root bridge. 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 be added 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.

a. 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.
b. Ports Fa0/1/ and Fa0/18 are used on switch S2. Shut down the remaining Fast Ethernet ports and the two Gigabit Ethernet ports.
c. 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.

a. 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.

b. Add the current active access (non-trunk) ports to the new VLAN.
c. 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.
d. Configure a management VLAN IP address for the VLAN 10 interface on S1 and S2 and enable it.
e. Configure a management VLAN IP address for the VLAN 30 interface on S3 and enable it.

Step 4: Save the running-config to the startup-config.

Part 5: Configuring VPN Remote Access

In Part 5, configure a remote access IPSec VPN. R3 is configured via CCP as an Easy VPN server, 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 CCP VPN Wizard to Configure the Easy VPN Server (Chapter 8)

Step 1: Configure R3 to allow CCP Access and Discovery.

a. Enable the HTTP server on R3.
   Or enable the HTTP secure server to connect securely.
b. Create an admin account on R3 with privilege level 15 for use with AAA and CCP.
c. Have CCP use the local database to authenticate web sessions.
d. Run the CCP application on PC-C. In the Select/Manage Community window, input the R3 IP address 192.168.3.1 in the first IP Address/Hostname field. Enter admin in the Username field, and cisco12345 in the Password field. Click on the OK button.
e. At the CCP Dashboard, click on the Discovery button to discover and connect to R3. If the discovery process fails, click the Discover Details button to determine the problem in order to resolve the issue.

Step 2: Launch the Easy VPN Server wizard.

Click the Configure button at the top of the CCP home screen and choose Security > VPN > Easy VPN Server, and then click Launch Easy VPN Server Wizard. Click Next on the Welcome Screen to continue.

Note: The Easy VPN Server Wizard checks the router configuration to see if AAA is enabled. If AAA was enabled on the router previously.

Step 3: Configure the virtual tunnel interface and authentication.

a. Choose the interface on which the client connections terminate. Click the Unnumbered to radio button, and choose the Serial0/0/1 interface from the drop-down menu.
b. Choose 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 CCP transform set is used. Click Next to accept the default transform set.

Step 6: Specify the group authorization and group policy lookup.

a. In the Group Authorization and Group Policy Lookup window, choose the Local option.
b. 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).**

a. In the User Authentication (XAuth) window, check the **Enable User Authentication** check box and choose **Local Only**.

b. 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? ________________

c. Add the new user **VPNUser1** with a password of **VPNUser1pa55** and click **OK**.

d. 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.

a. Click **Add** to create a group policy.

b. 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**.

c. Click **OK** to accept the entries.

d. A CCP 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.

e. Check the **Configure Idle Timer** check box and enter 1 hour, 0 minutes, and 0 seconds.

f. 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.

g. When the Easy VPN Server Pass-through Configuration window displays, make sure that the **Action Modify** check box is checked. This option allows CCP 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 CCP 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**

a. Start the Cisco VPN Client. Select **Connection Entries > New** or click the **New** icon with the plus sign (+) on it.

b. 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.**

a. Choose the newly created connection **VPN-Corp** and click the **Connect** icon. You can also double-click the connection entry.

b. 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

<table>
<thead>
<tr>
<th>Router Model</th>
<th>Ethernet Interface #1</th>
<th>Ethernet Interface #2</th>
<th>Serial Interface #1</th>
<th>Serial Interface #2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1800</td>
<td>Fast Ethernet 0/0 (Fa0/0)</td>
<td>Fast Ethernet 0/1 (Fa0/1)</td>
<td>Serial 0/0/0 (S0/0/0)</td>
<td>Serial 0/0/1 (S0/0/1)</td>
</tr>
<tr>
<td>1900</td>
<td>Gigabit Ethernet 0/0 (G0/0)</td>
<td>Gigabit Ethernet 0/1 (G0/1)</td>
<td>Serial 0/0/0 (S0/0/0)</td>
<td>Serial 0/0/1 (S0/0/1)</td>
</tr>
<tr>
<td>2800</td>
<td>Fast Ethernet 0/0 (Fa0/0)</td>
<td>Fast Ethernet 0/1 (Fa0/1)</td>
<td>Serial 0/0/0 (S0/0/0)</td>
<td>Serial 0/0/1 (S0/0/1)</td>
</tr>
<tr>
<td>2900</td>
<td>Gigabit Ethernet 0/0 (G0/0)</td>
<td>Gigabit Ethernet 0/1 (G0/1)</td>
<td>Serial 0/0/0 (S0/0/0)</td>
<td>Serial 0/0/1 (S0/0/1)</td>
</tr>
</tbody>
</table>

**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.