Lab 11-01: Basic Security Configuration

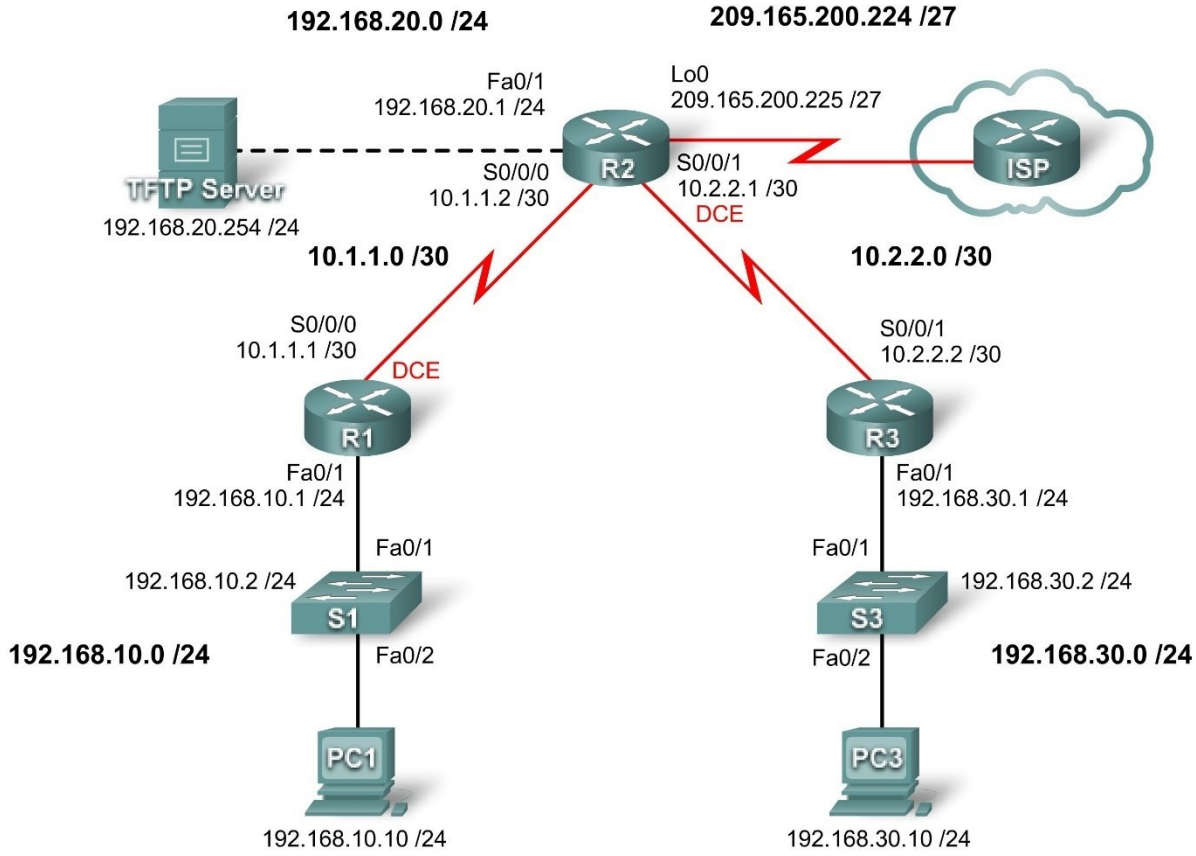
Member list:

1	นายธนพล โรจนะวิชานนท์ 5710503398
2	นายภารุจ สิงหพันธุ์ 5710503495

3 นายเกริกชัย พงศ์ทวีวุฒิ 5710504742

Topology Diagram

4. นายสิทธิชัย ตระกูลมัยผล 5710505765



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	**Fa0/1**	192.168.10.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
R2	**Fa0/1**	192.168.20.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
R3	**Fa0/1**	192.168.30.1	255.255.255.0	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
S1	**VLAN10**	192.168.10.2	255.255.255.0	N/A
S3	**VLAN20**	192.168.30.2	255.255.255.0	N/A
PC1	**NIC**	192.168.10.10	255.255.255.0	192.168.10.1
PC3	**NIC**	192.168.30.10	255.255.255.0	192.168.30.1
TFTP Server	**NIC**	192.168.20.254	255.255.255.0	192.168.20.1

Learning Objectives

Upon completion of this lab, you will be able to:

- Cable a network according to the topology diagram.
- Erase the startup configuration and reload a router to the default state.
- Perform basic configuration tasks on a router.
- Configure basic router security.
- Disable unused Cisco services and interfaces.
- Protect enterprise networks from basic external and internal attacks.
- Understand and manage Cisco IOS configuration files and Cisco file system.
- Configure VLANs on the switches.
- Set up and use Cisco Configuration Professional (CCP) to configure basic router security.

Scenario

In this lab, you will learn how to configure basic network security using the network shown in the topology diagram. You will learn how to configure router security three different ways: using the CLI, the auto-secure feature, and Cisco CCP. You will also learn how to manage Cisco IOS software.

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

You can use any current router in your lab as long as it has the required interfaces shown in the topology.

Note: This lab was developed and tested using 1841 routers. If you use 1700, 2500, or 2600 series routers, the router outputs and interface descriptions might be different.

Step 2: Clear any existing configurations on the routers.

Task 2: Perform Basic Router Configurations

Step 1: Configure routers.

Configure the R1, R2, and R3 routers according to the following guidelines:

- Configure the router hostname according to the topology diagram.
- Disable DNS lookup.
- Configure a message of the day banner.
- Configure IP addresses on R1, R2, and R3.
- Enable RIP version 2 on all routers for all networks.
- Create a loopback interface on R2 to simulate the connection to the Internet.
- Configure a TFTP server on PC2. If you need to download TFTP server software, one option is: http://tftpd32.jounin.net/

Step 2: Configure Ethernet interfaces.

Configure the Ethernet interfaces of PC1, PC3, and TFTP Server with the IP addresses and default gateways from the Addressing Table at the beginning of the lab.

Step 3: Test the PC configuration by pinging the default gateway from each of the PCs and the TFTP server.

Task 3: Secure the Router from Unauthorized Access

Step 1: Configure secure passwords and AAA authentication.

Use a local database on R1 to configure secure passwords. Use **ciscoccna** for all passwords in this lab.

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

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

_____เพื่อป้องกันการถูกโจมตีหรือการพยายามที่จะเข้ามา config router จากผู้ที่ไม่เกี่ยวข้อง_____

_____

_____

The **username** command creates a username and password that is stored locally on the router. The default privilege level of the user is 0 (the least amount of access). You can change the level of access for a user by adding the keyword **privilege** *0-15* before the **password** keyword.

```
R1(config)#username ccna password ciscoccna
```

The **aaa** command enables AAA (authentication, authorization, and accounting) globally on the router. This is used when connecting to the router.


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

You can create an authentication list that is accessed when someone attempts to log in to the device after applying it to vty and console lines. The **local** keyword indicates that the user database is stored locally on the router.

```
R1(config)#aaa authentication login LOCAL_AUTH local
```

Note: LOCAL_AUTH is a case sensitive tag name that must match for all uses.

The following commands tell the router that users attempting to connect to the router should be authenticated using the list you just created.

```
R1(config)#line console 0
R1(config-lin)#login authentication LOCAL_AUTH
R1(config-lin)#line vty 0 4
R1(config-lin)#login authentication LOCAL_AUTH
```

What do you notice that is insecure about the following section of the running configuration:

```
R1#show run
<output omitted>
!
enable secret 5 $1$.DB7$DunHvguQH0EvLqzQCqzfr1
!
aaa new-model
!
aaa authentication login LOCAL_AUTH local
!
username ccna password 0 ciscoccna
!
<output omitted>
!
banner motd ^CUnauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law^C
!
line con 0
 login authentication LOCAL_AUTH
line aux 0
line vty 0 4
 login authentication LOCAL_AUTH
!
```

___เพราะมันบอก password และ usernameหมดเลยโดยที่ไม่ได้ encrypt ไว้_____

_____

_____

To apply simple encryption to the passwords, enter the following command in global config mode:

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

Verify this with the **show run** command.

```
R1#show run
```



```
service password-encryption
!
enable secret 5 $1$.DB7$DunHvguQH0EvLqzQCqzfr1
!
aaa new-model
!
aaa authentication login LOCAL_AUTH local
!
username ccna password 7 0822455D0A1606141C0A
<output omitted>
!
banner motd ^CCUnauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law^C
!
line con 0
 login authentication LOCAL_AUTH
line aux 0
line vty 0 4
 login authentication LOCAL_AUTH
!
```

Step 2: Secure the console and VTY lines.

You can cause the router to log out a line that has been idle for a specified time. If a network engineer was logged into a networking device and was suddenly called away, this command automatically logs the user out after the specified time. The following commands cause the line to log out after 5 minutes.

```
R1(config)#line console 0
R1(config-lin)#exec-timeout 5 0
R1(config-lin)#line vty 0 4
R1(config-lin)#exec-timeout 5 0
```

The following command hampers brute force login attempts. The router blocks login attempts for 5 minutes if someone fails two attempts within 2 minutes. This is set especially low for the purpose of this lab. An additional measure is to log each time this happens.

```
R1(config)#login block-for 300 attempt 2 within 120
R1(config)#security authentication failure rate 2 log
```

To verify this, attempt to connect to R1 from R2 via Telnet with an incorrect username and password.

On R2:

```
R2#telnet 10.1.1.1
Trying 10.1.1.1 ... Open
Unauthorized access strictly prohibited, violators will be prosecuted to the
full extent of the law

User Access Verification

Username: cisco
Password:

% Authentication failed
```



```
User Access Verification

Username: cisco
Password:

% Authentication failed

[Connection to 10.1.1.1 closed by foreign host]
R2#telnet 10.1.1.1
Trying 10.1.1.1 ...
% Connection refused by remote host
```

On R1:

```
*Sep 10 12:40:11.211: %SEC_LOGIN-5-QUIET_MODE_OFF: Quiet Mode is OFF, because
block period timed out at 12:40:11 UTC Mon Sep 10 2007
```

Task 4: Secure Access to the Network

Step 1: Prevent RIP routing update propagation.

Who can receive RIP updates on a network segment where RIP is enabled? Is this the most desirable setup?

_____

_____

_____

The **passive-interface** command prevents routers from sending routing updates to all interfaces except those interfaces configured to participate in routing updates. This command is issued as part of the RIP configuration.

The first command puts all interfaces into passive mode (the interface only receives RIP updates). The second command returns specific interfaces from passive to active mode (both sending and receiving RIP updates).

R1

```
R1(config)#router rip
R1(config-router)#passive-interface default
R1(config-router)#no passive-interface s0/0/0
```

R2

```
R2(config)#router rip
R2(config-router)#passive-interface default
R2(config-router)#no passive-interface s0/0/0
R2(config-router)#no passive-interface s0/0/1
```

R3

```
R3(config)#router rip
R3(config-router)#passive-interface default
R3(config-router)#no passive-interface s0/0/1
```


Step 2: Prevent unauthorized reception of RIP updates.

Preventing unnecessary RIP updates to the whole network is the first step to securing RIP. The next is to have RIP updates password protected. To do this, you must first configure a key to use.

```
R1(config)#key chain RIP_KEY
R1(config-keychain)#key 1
R1(config-keychain-key)#key-string cisco
```

This has to be added to each router that is going to receive RIP updates.

```
R2(config)#key chain RIP_KEY
R2(config-keychain)#key 1
R2(config-keychain-key)#key-string cisco
```

```
R3(config)#key chain RIP_KEY
R3(config-keychain)#key 1
R3(config-keychain-key)#key-string cisco
```

To use the key, each interface participating in RIP updates needs to be configured. These will be the same interfaces that were enabled using the **no passive-interface** command earlier.

R1

```
R1(config)#int s0/0/0
R1(config-if)#ip rip authentication mode md5
R1(config-if)#ip rip authentication key-chain RIP_KEY
```

At this point, R1 is no longer receiving RIP updates from R2, because R2 is not yet configured to use a key for routing updates. You can view this on R1 using the **show ip route** command and confirming that no routes from R2 appear in the routing table.

Clear out IP routes with **clear ip route *** or wait for routes to timeout.

```
R1#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
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, *- candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 1 subnets, 1 masks
C       10.1.1.0/24 is directly connected, Serial0/0/0
C    192.168.10.0 is directly connected, Serial0/0/0
```

Configure R2 and R3 to use routing authentication. Remember that each active interface must be configured.

R2

```
R2(config)#int s0/0/0
R2(config-if)#ip rip authentication mode md5
R2(config-if)#ip rip authentication key-chain RIP_KEY
R2(config)#int s0/0/1
R2(config-if)#ip rip authentication mode md5
R2(config-if)#ip rip authentication key-chain RIP_KEY
```


R3

```
R3(config)#int s0/0/1
R3(config-if)#ip rip authentication mode md5
R3(config-if)#ip rip authentication key-chain RIP_KEY
```

Step 3: Verify that RIP routing still works.

After all three routers have been configured to use routing authentication, the routing tables should repopulate with all RIP routes. R1 should now have all the routes via RIP. Confirm this with the **show ip route** command.

```
R1#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
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, *-candidate default, U-per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

R     192.168.30.0/24 [120/2] via 10.1.1.2, 00:00:16, Serial0/0/0
C     192.168.10.0/24 is directly connected, FastEthernet0/1
R     192.168.20.0/24 [120/1] via 10.1.1.2, 00:00:13, Serial0/0/0
      10.0.0.0/8 is variably subnetted, 2 subnets, 1 masks
R        10.2.2.0/24 [120/1] via 10.1.0.2, 00:00:16, Serial0/0/0
C        10.1.1.0/24 is directly connected, Serial0/0/0
```

Task 5: Logging Activity with SNMP (Simple Network Management Protocol)

Step 1: Configure SNMP logging to the syslog server.

SNMP logging can be useful in monitoring network activity. The captured information can be sent to a syslog server on the network, where it can be analyzed and archived. You should be careful when configuring logging (syslog) on the router. When choosing the designated log host, remember that the log host should be connected to a trusted or protected network or an isolated and dedicated router interface.

In this lab, you will configure PC1 as the syslog server for R1. Use the **logging** command to select the IP address of the device to which SNMP messages are sent. In this example, the IP address of PC1 is used.

```
R1(config)#logging 192.168.10.10
```

Note: PC1 should have syslog software installed and running if you wish to view syslog messages.

In the next step, you will define the level of severity for messages to be sent to the syslog server.

Step 2: Configure the SNMP severity level.

The level of SNMP messages can be adjusted to allow the administrator to determine what kinds of messages are sent to the syslog device. 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. To configure the severity levels, you use the keyword associated with the level, as shown in the table.

Severity Level	Keyword	Description
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

The **logging trap** command sets the severity level. The severity level includes the level specified and anything below it (severity-wise). Set R1 to level 4 to capture messages with severity level 4, 3, 2, and 1.

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

What is the danger of setting the level of severity too high or too low?

__หากความป้องกันต่ำ ก็สามารถถูกโจมตีได้ง่ายๆ แต่หากการป้องกันที่สูงจนเกินไป อาจทำให้ไม่สะดวกในการเข้าถึง หรืออาจ

__ลืมแล้วทำให้ไม่สามรถเข้าถึงได้เลย_____

_____

Note: If you installed syslog software on PC1, generate and look at syslog software for messages.

Task 6: Disabling Unused Cisco Network Services

Step 1: Disable unused interfaces.

Why should you disable unused interfaces on network devices?

__เพื่อป้องกันการต่อผิดพลาดที่อาจก่อให้เกิดความเสียหายกับnetworkได้ รวมไปถึงป้องกันการพยายามโจทตีจากบุคคลอื่นๆด้วย

_____

_____

In the topology diagram, you can see that R1 should only be using interface S0/0/0 and Fa0/1. All other interfaces on R1 should be administratively shut down using the **shutdown** interface configuration command.

```
R1(config)#interface fastethernet0/0
R1(config-if)#shutdown
R1(config-if)# interface s0/0/1
R1(config-if)#shutdown

*Sep 10 13:40:24.887: %LINK-5-CHANGED: Interface FastEthernet0/0, changed
state to administratively down
```



```
*Sep 10 13:40:25.887: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to down
```

To verify that R1 has all inactive interfaces shut down, use the **show ip interface brief** command. Interfaces manually shut down are listed as administratively down.

```
R1#sh ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES unset  administratively down down
FastEthernet0/1        192.168.10.1    YES manual up                    up
Serial0/0/0            10.1.1.1        YES manual up                    up
Serial0/0/1            unassigned      YES unset  administratively down down
```

Step 2: Disable unused global services.

Many services are not needed in most modern networks. Leaving unused services enabled leaves ports open that can be used to compromise a network. Disable each of these services on R1.

```
R1(config)#no service pad
R1(config)#no service finger
R1(config)#no service udp-small-server
R1(config)#no service tcp-small-server
R1(config)#no ip bootp server
R1(config)#no ip http server
R1(config)#no ip finger
R1(config)#no ip source-route
R1(config)#no ip gratuitous-arps
R1(config)#no cdp run
```

Step 3: Disable unused interface services.

These commands are entered at the interface level and should be applied to every interface on R1.

```
R1(config-if)#no ip redirects
R1(config-if)#no ip proxy-arp
R1(config-if)#no ip unreachables
R1(config-if)#no ip directed-broadcast
R1(config-if)#no ip mask-reply
R1(config-if)#no mop enabled
```

Step 4: Use AutoSecure to secure a Cisco router.

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.

Using the AutoSecure feature, you can apply the same security features that you just applied (except for securing RIP) to a router much faster. Because you have already secured R1, use the **auto secure** command on R3.

```
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]: 1

Interface                  IP-Address      OK? Method Status      Protocol
FastEthernet0/0            unassigned      YES unset  down        down
FastEthernet0/1            192.168.30.1    YES manual up          up
Serial0/0/0                unassigned      YES manual down        down
Serial0/0/1                10.2.2.2        YES manual 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
Enable secret is either not configured or
 Is the same as enable password
Enter the new enable password: ciscoccna
Confirm the enable password: ciscoccna
Enter the new enable password: ccnacisco
Confirm the enable password: ccnacisco

Configuration of local user database
Enter the username: ccna
Enter the password: ciscoccna
Confirm the password: ciscoccna
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: 300

Maximum Login failures with the device: 5
```



```
Maximum time period for crossing the failed login attempts: 120

Configure SSH server? Yes
Enter domain-name: cisco.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: 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

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
security passwords min-length 6
security authentication failure rate 10 log
enable password 7 070C285F4D061A061913
username ccna password 7 045802150C2E4F4D0718
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
line tty 192
 login authentication local_auth
 exec-timeout 15 0
login block-for 300 attempts 5 within 120
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 Serial0/1/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
interface Serial0/1/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
```



```
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]:yes

The name for the keys will be: R3.cisco.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R3#
000045: *Nov 16 15:39:10.991 UTC: %AUTOSEC-1-MODIFIED: AutoSecure
configuration has been Modified on this device
```

As you can see, the AutoSecure feature is much faster than line by line configuration. However, there are advantages to doing it manually, as you will see in the troubleshooting lab. When you use AutoSecure, you may disable a service you need. Always use caution and think about the services that you require before using AutoSecure.

Task 7: Managing Cisco IOS and Configuration Files

Step 1: Show Cisco IOS files.

Cisco IOS is the software that routers use to operate. Your router may have enough memory to store multiple Cisco IOS images. It is important to know which files are stored on your router.

Issue the **show flash** command to view the contents of the flash memory of your router.

Caution: Be very careful when issuing commands that involve the flash memory. Mistyping a command could result in the deletion of the Cisco IOS image.

```
R1#show flash
-#- --length-- -----date/time------ path
1     13937472 May 05 2007 21:25:14 +00:00 c1841-ipbase-mz.124-1c.bin
2         1821 May 05 2007 21:40:28 +00:00 sdmconfig-18xx.cfg
3      4734464 May 05 2007 21:41:02 +00:00 sdm.tar
4       833024 May 05 2007 21:41:24 +00:00 es.tar
5      1052160 May 05 2007 21:41:48 +00:00 common.tar

8679424 bytes available (23252992 bytes used)
```

Just by looking at this list, we can determine the following:

- The image is for an 1841 router (c**1841**-ipbase-mz.124-1c.bin).
- The router is using IP base image (c1841**-ipbase**-mz.124-1c.bin).
- The Cisco IOS is version 12.4(1c) (c1841-ipbase-mz.**124-1c**.bin).
- SDM is installed on this device (**sdm**config-18xx.cfg, **sdm**.tar).

You can use the **dir all** command to show all files on the router.

```
R1#dir all
Directory of archive:/

No files in directory

No space information available
Directory of system:/

 3  dr-x           0                    <no date>  memory
 1  -rw-         979                    <no date>  running-config
 2  dr-x           0                    <no date>  vfiles

No space information available
Directory of nvram:/

 189  -rw-         979                      <no date>  startup-config
 190  ----           5                      <no date>  private-config
 191  -rw-         979                      <no date>  underlying-config
   1  -rw-           0                      <no date>  ifIndex-table

196600 bytes total (194540 bytes free)
Directory of flash:/

 1 -rw- 13937472  May 05 2007 20:08:50 +00:00  c1841-ipbase-mz.124-1c.bin
 2 -rw-     1821  May 05 2007 20:25:00 +00:00  sdmconfig-18xx.cfg
 3 -rw-  4734464  May 05 2007 20:25:38 +00:00  sdm.tar
 4 -rw-   833024  May 05 2007 20:26:02 +00:00  es.tar
 5 -rw-  1052160  May 05 2007 20:26:30 +00:00  common.tar
 6 -rw-     1038  May 05 2007 20:26:56 +00:00  home.shtml
 7 -rw-   102400  May 05 2007 20:27:20 +00:00  home.tar
 8 -rw-   491213  May 05 2007 20:27:50 +00:00  128MB.sdf
 9 –rw-   398305  May 05 2007 20:29:08 +00:00  sslclient-win-1.1.0.154.pkg
 10 -rw- 1684577  May 05 2007 20:28:32 +00:00  securedesktop-ios-3.1.1.27-
k9.pkg

31932416 bytes total (8679424 bytes free)
```

Step 2: Transfer files with TFTP.

TFTP is used when archiving and updating the Cisco IOS software of a device. In this lab, however, we do not use actual Cisco IOS files because any mistakes made in entering the commands could lead to erasing the Cisco IOS image of the device. At the end of this section, there is an example of what a Cisco IOS TFTP transfer looks like.

Why is it important to have an updated version of Cisco IOS software?

__เพื่อให้อุปกรณ์ทันต่อโลกภายนอกเพื่อที่จะป้องกันการโจมตีใหม่ๆที่อาจเพิ่มเข้ามาภายหลังได้มิฉะนั้นหากไม่ทำการ update__

__ก็อาจจะถูกโจมตีจากการโจมตีใหม่ๆที่ยังไม่ได้ updateโจมตีได้_____

_____

When transferring files via TFTP, it is important to ensure that the TFTP server and the router can communicate. One way to test this is to ping between these devices.

To begin transfer of the Cisco IOS software, create a file on the TFTP server called **test** in the TFTP root folder. Each TFTP program differs in where files are stored. Consult your TFTP server help file to determine the root folder.

From R1, retrieve the file and save it to the flash memory.

```
R1#copy tftp flash
Address or name of remote host []? 192.168.20.254 (IP address of the TFTP server)
Source filename []? Test (name of the file you created and saved to TFTP server)
Destination filename [test]? test-server (An arbitrary name for the file when saved to the
router)
Accessing tftp://192.168.20.254/test...
Loading test from 192.168.20.254 (via FastEthernet0/1): !
[OK - 1192 bytes]

1192 bytes copied in 0.424 secs (2811 bytes/sec)
```

Verify the file's existence in the flash with the **show flash** command.

```
R1#show flash
-#- --length-- -----date/time------ path
1     13937472 May 05 2007 21:13:20 +00:00 c1841-ipbase-mz.124-1c.bin
2         1821 May 05 2007 21:29:36 +00:00 sdmconfig-18xx.cfg
3      4734464 May 05 2007 21:30:14 +00:00 sdm.tar
4       833024 May 05 2007 21:30:42 +00:00 es.tar
5      1052160 May 05 2007 21:31:10 +00:00 common.tar
6         1038 May 05 2007 21:31:36 +00:00 home.shtml
7       102400 May 05 2007 21:32:02 +00:00 home.tar
8       491213 May 05 2007 21:32:30 +00:00 128MB.sdf
9      1684577 May 05 2007 21:33:16 +00:00 securedesktop-ios-3.1.1.27-k9.pkg
10      398305 May 05 2007 21:33:50 +00:00 sslclient-win-1.1.0.154.pkg
11        1192 Sep 12 2007 07:38:18 +00:00 test-server

8675328 bytes available (23257088 bytes used)
```

Routers can also act as TFTP servers. This can be useful if there is a device that needs an image and you have one that is already using that image. We will make R2 a TFTP server for R1. Remember that Cisco IOS images are specific to router platforms and memory requirements. Use caution when transferring a Cisco IOS image from one router to another.

The command syntax is: **tftp-server nvram:** [*filename1* [**alias** *filename2*]

The command below configures R2 as a TFTP server. R2 supplies its startup config file to devices requesting it via TFTP (we are using the startup config for the sake of simplicity and ease). The **alias** keyword allows devices to request the file using the alias **test** instead of the full filename.

```
R2(config)#tftp-server nvram:startup-config alias test
```

Now we can request the file from R2 using R1.

```
R1#copy tftp flash
Address or name of remote host []? 10.1.1.2
Source filename []? test
Destination filename []? test-router
Accessing tftp://10.1.1.2/test...
Loading test from 10.1.1.2 (via Serial0/0/0): !
[OK - 1192 bytes]
```



```
1192 bytes copied in 0.452 secs (2637 bytes/sec)
```

Again, verify that the file **test** has been successfully copied with the **show flash** command

```
R1#show flash
-#- --length-- -----date/time------ path
1     13937472 May 05 2007 21:13:20 +00:00 c1841-ipbase-mz.124-1c.bin
2         1821 May 05 2007 21:29:36 +00:00 sdmconfig-18xx.cfg
3      4734464 May 05 2007 21:30:14 +00:00 sdm.tar
4       833024 May 05 2007 21:30:42 +00:00 es.tar
5      1052160 May 05 2007 21:31:10 +00:00 common.tar
6         1038 May 05 2007 21:31:36 +00:00 home.shtml
7       102400 May 05 2007 21:32:02 +00:00 home.tar
8       491213 May 05 2007 21:32:30 +00:00 128MB.sdf
9      1684577 May 05 2007 21:33:16 +00:00 securedesktop-ios-3.1.1.27-k9.pkg
10      398305 May 05 2007 21:33:50 +00:00 sslclient-win-1.1.0.154.pkg
11        1192 Sep 12 2007 07:38:18 +00:00 test-server
12        1192 Sep 12 2007 07:51:04 +00:00 test-router

8671232 bytes available (23261184 bytes used)
```

Because you do not want unused files occupying precious memory space, delete them now from the flash memory of R1. **Be very careful when doing this!** Accidentally erasing flash memory will mean that you have to re-install the entire IOS image for the router. If the router prompts you to **erase flash**, something is very wrong. You rarely want to erase the entire flash. The only legitimate time this will happen is when you are upgrading the IOS to a large IOS image. If you see the **erase flash** prompt as in the example, STOP IMMEDIATELY. Do NOT hit enter. IMMEDIATELY ask for assistance from your instructor.

```
Erase flash: ?[confirm] no
```

```
R1#delete flash:test-server
Delete filename [test-server]?
Delete flash:test? [confirm]
R1#delete flash:test-router
Delete filename [test-router]?
Delete flash:test-router? [confirm]
```

Verify that the files have been deleted by issuing the **show flash** command.

```
R1#show flash
-#- --length-- -----date/time------ path
1     13937472 May 05 2007 21:13:20 +00:00 c1841-ipbase-mz.124-1c.bin
2         1821 May 05 2007 21:29:36 +00:00 sdmconfig-18xx.cfg
3      4734464 May 05 2007 21:30:14 +00:00 sdm.tar
4       833024 May 05 2007 21:30:42 +00:00 es.tar
5      1052160 May 05 2007 21:31:10 +00:00 common.tar
6         1038 May 05 2007 21:31:36 +00:00 home.shtml
7       102400 May 05 2007 21:32:02 +00:00 home.tar
8       491213 May 05 2007 21:32:30 +00:00 128MB.sdf
9      1684577 May 05 2007 21:33:16 +00:00 securedesktop-ios-3.1.1.27-k9.pkg
10      398305 May 05 2007 21:33:50 +00:00 sslclient-win-1.1.0.154.pkg

8679424 bytes available (23252992 bytes used)
```


The following is an example of a TFTP transfer of a Cisco IOS image file.

Do NOT complete on your routers. Only read it.

```
R1#copy tftp flash
Address or name of remote host []? 10.1.1.2
Source filename []? c1841-ipbase-mz.124-1c.bin
Destination filename []? flash:c1841-ipbase-mz.124-1c.bin
Accessing tftp://10.1.1.2/c1841-ipbase-mz.124-1c.bin...
Loading c1841-ipbase-mz.124-1c.bin from 10.1.1.2 (via
Serial0/0/0): !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!
<output omitted>
!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 13937472 bytes]

13937472 bytes copied in 1113.948 secs (12512 bytes/sec)
```

Step 3: Recover a password using ROMmon.

If for some reason you can no longer access a device because you do not know, have lost, or have forgotten a password, you can still gain access by changing the configuration register. The configuration register tells the router which configuration to load on bootup. In the configuration register, you can instruct the router to boot from a blank configuration that is not password protected.

The first step in changing the configuration register is to view the current setting using the **show version** command. These steps are performed on R3.

```
R3#show version
Cisco IOS Software, 1841 Software (C1841-IPBASE-M), Version 12.4(1c), RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Tue 25-Oct-05 17:10 by evmiller

ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)

R3 uptime is 25 minutes
System returned to ROM by reload at 08:56:50 UTC Wed Sep 12 2007
System image file is "flash:c1841-ipbase-mz.124-1c.bin"

Cisco 1841 (revision 7.0) with 114688K/16384K bytes of memory.
Processor board ID FTX1118X0BN
2 FastEthernet interfaces
2 Low-speed serial(sync/async) interfaces
DRAM configuration is 64 bits wide with parity disabled.
191K bytes of NVRAM.
31360K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2102
```

Next, reload the router and send a break during the boot up. The **Break** key is different on different computers. Frequently, it is in the upper right hand corner of the keyboard. A break causes the device to enter a mode called ROMmon. This mode does not require the device to have access to a Cisco IOS image file.

Note: Hyperterminal require a Ctrl-Break sequence. For other terminal emulation software, check the standard Break Key sequence combinations.

```
R3#reload
Proceed with reload? [confirm]

*Sep 12 08:27:28.670: %SYS-5-RELOAD: Reload requested by console. Reload
Reason: Reload command.
System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2006 by cisco Systems, Inc.
PLD version 0x10
GIO ASIC version 0x127
c1841 platform with 131072 Kbytes of main memory
Main memory is configured to 64 bit mode with parity disabled

Readonly ROMMON initialized
rommon 1 >
```

Change the configuration register to a value that loads the initial configuration of the router. This configuration does not have a password configured, but supports Cisco IOS commands. Change the value of the configuration register to 0x2142.

```
rommon 1 > confreg 0x2142
```

Now that this is changed we can boot the device with the **reset** command.

```
rommon 2 > reset
program load complete, entry point: 0x8000f000, size: 0xcb80
program load complete, entry point: 0x8000f000, size: 0xcb80

program load complete, entry point: 0x8000f000, size: 0xd4a9a0
Self decompressing the image :
############################################################
################################################################################
# [OK]

<output omitted>


         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no


Press RETURN to get started!
```

Step 4: Restore the router.

Now we copy the startup configuration to the running configuration, restore the configuration, and then change the configuration register back to the default (0x2102).

To copy the startup configuration from NVRAM to running memory, type **copy startup-config running-config**. Be careful! Do *not* type `copy running-config startup-config` or you will erase your startup configuration.


```
Router#copy startup-config running-config
Destination filename [running-config]? {enter}

2261 bytes copied in 0.576 secs (3925 bytes/sec)

R3#:show running-config
<output omitted>
enable secret 5 $1$31P/$cyPgoxc0R9y93Ps/N3/kg.
!
<output omitted>
!
key chain RIP_KEY
 key 1
  key-string 7 01100F175804
username ccna password 7 094F471A1A0A1411050D
!
interface FastEthernet0/1
 ip address 192.168.30.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 shutdown
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
!
<output omitted>
!
line con 0
 exec-timeout 5 0
 logging synchronous
 login authentication
 transport output telnet
line aux 0
 exec-timeout 15 0
 logging synchronous
 login authentication local_auth
 transport output telnet
line vty 0 4
 exec-timeout 15 0
 logging synchronous
 login authentication local_auth
 transport input telnet
!
end
```


In this configuration, the **shutdown** command appears under all interfaces because all the interfaces are currently shut down. Most important, you can now see the passwords (enable password, enable secret, VTY, console passwords) in either an encrypted or unencrypted format. You can reuse unencrypted passwords. You must change encrypted passwords to a new password.

```
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#enable secret ciscoccna
R3(config)#username ccna password ciscoccna
```

Issue the **no shutdown** command on every interface that you want to use.

```
R3(config)#interface FastEthernet0/1
R3(config-if)#no shutdown
R3(config)#interface Serial0/0/1
R3(config-if)#no shutdown
```

You can issue a **show ip interface brief** command to confirm that your interface configuration is correct. Every interface that you want to use should display up up.

```
R3#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES NVRAM  administratively down down
FastEthernet0/1        192.168.30.1    YES NVRAM  up                    up
Serial0/0/1            unassigned      YES NVRAM  administratively down down
Serial0/0/0            10.2.2.2        YES NVRAM  up                    up
```

Type **config-register** *configuration register value*. The variable *configuration register value* is either the value you recorded in Step 3 or 0x2102. Save the running configuration.

```
R3(config)#config-register 0x2102
R3(config)#end
R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

What are the downsides to password recovery?

__อาจถูกผู้โจตีมาทำการขอ recovery password จนสามารถเข้ามาจัดการ อุปกรณ์ของเราได้_____

_____

_____

Task 8: Using CCP to Secure a Router

In this task, you will use CCP, the GUI interface, to secure router R2. SDM is faster than typing each command and gives you more control than the AutoSecure feature.

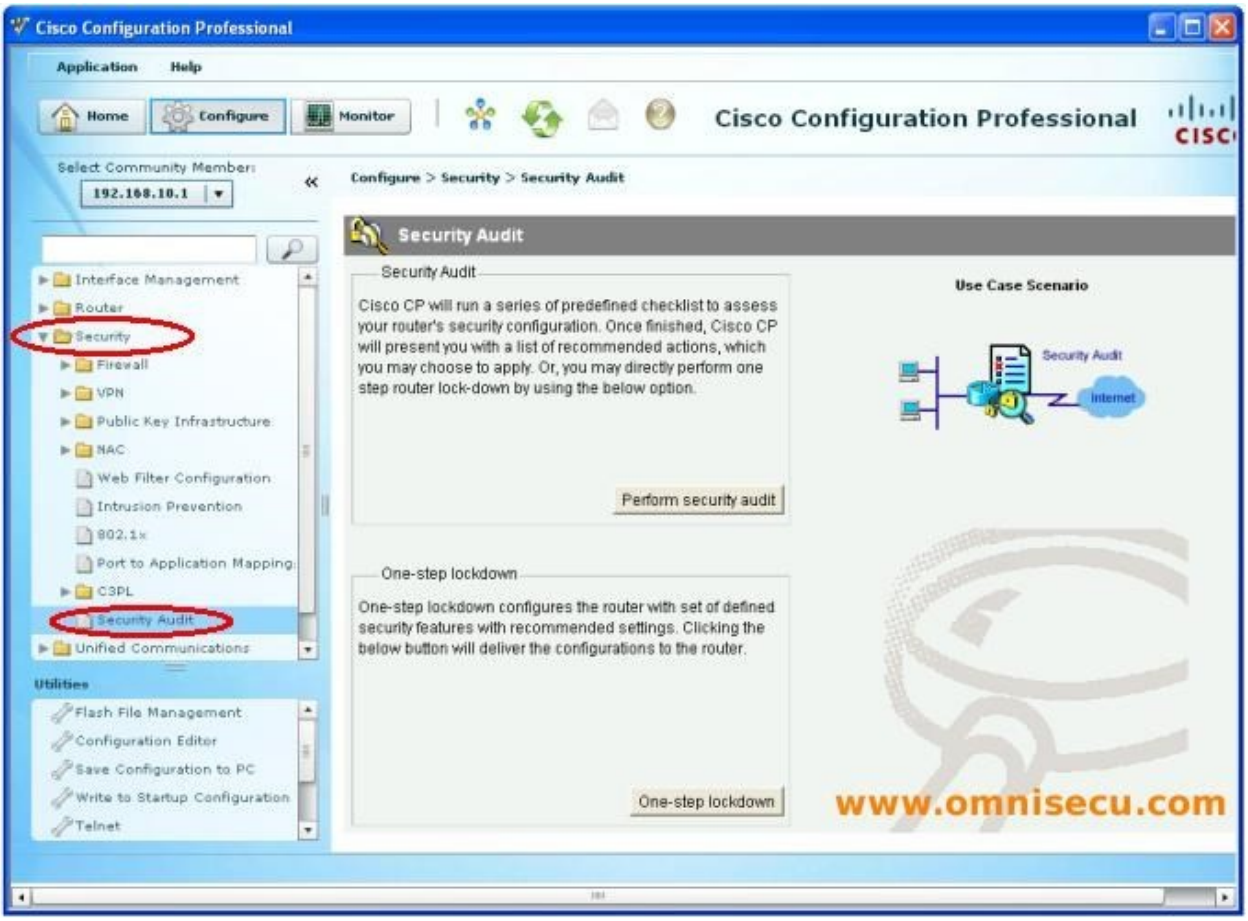
If CCP is NOT installed on your pc, it must be installed to continue. Please consult the instruction file: *"Lab11-0X: Configuring Devices for Use with Cisco Configuration"* for directions to setup on router R2.

After CCP is done starting, a new window opens for CCP.

Step 2: Navigate to the Security Audit feature.

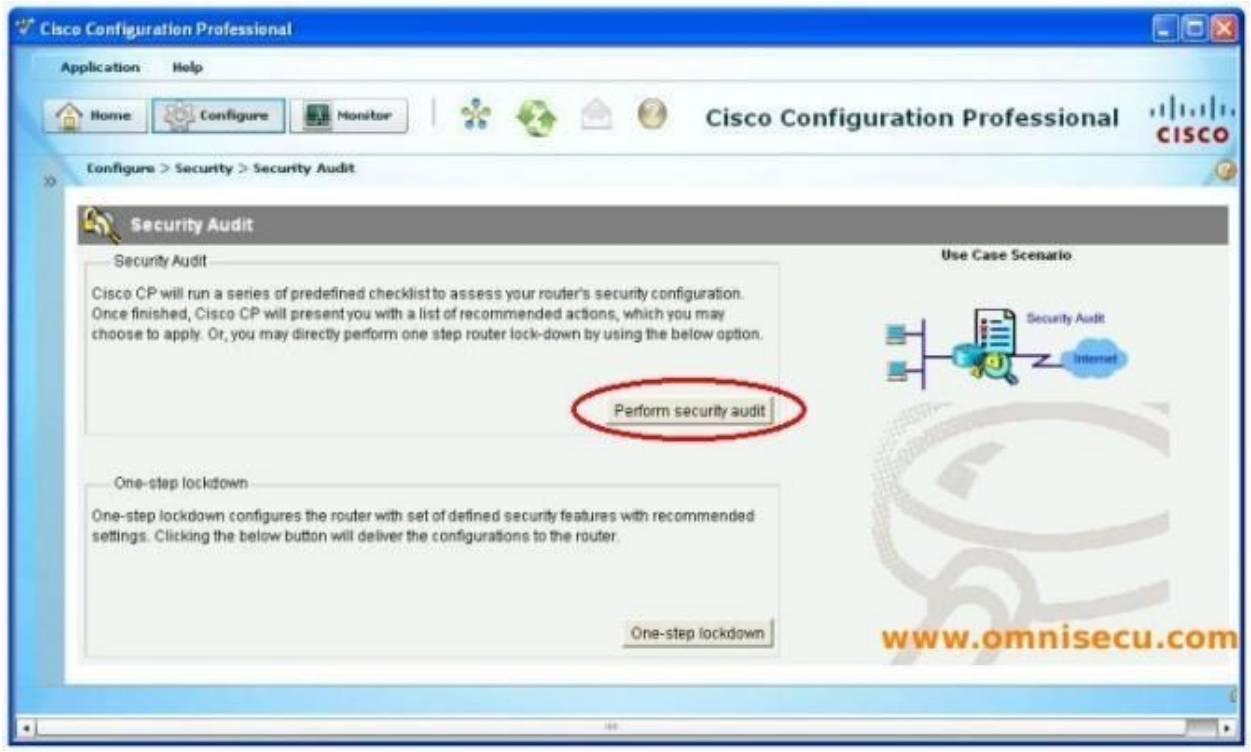
Click the **Security** panel in the left side of the window.

Now navigate down the left panel to **Security Audit** and click on it.

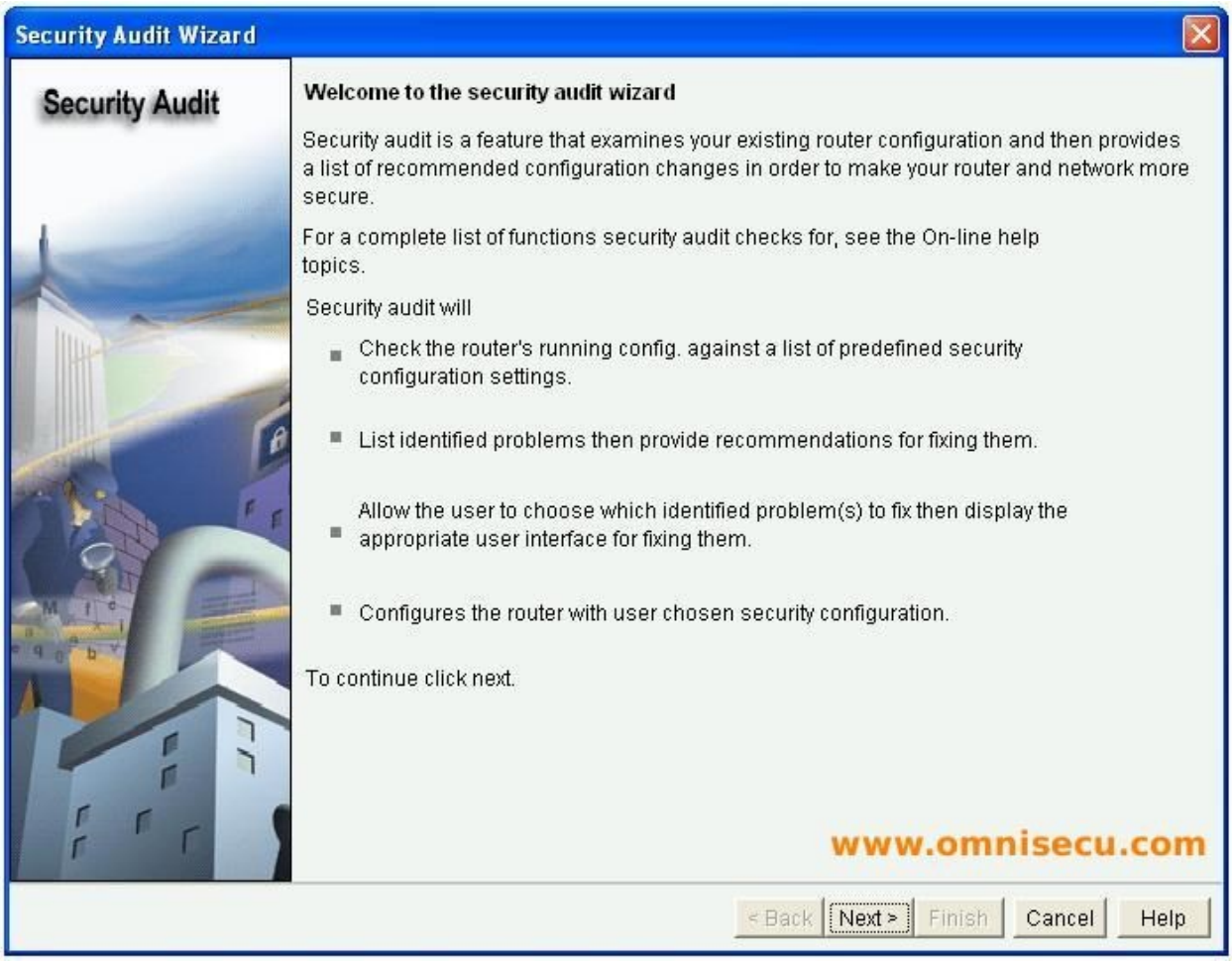


Now navigate down the left panel to **Security Audit** and click on it.

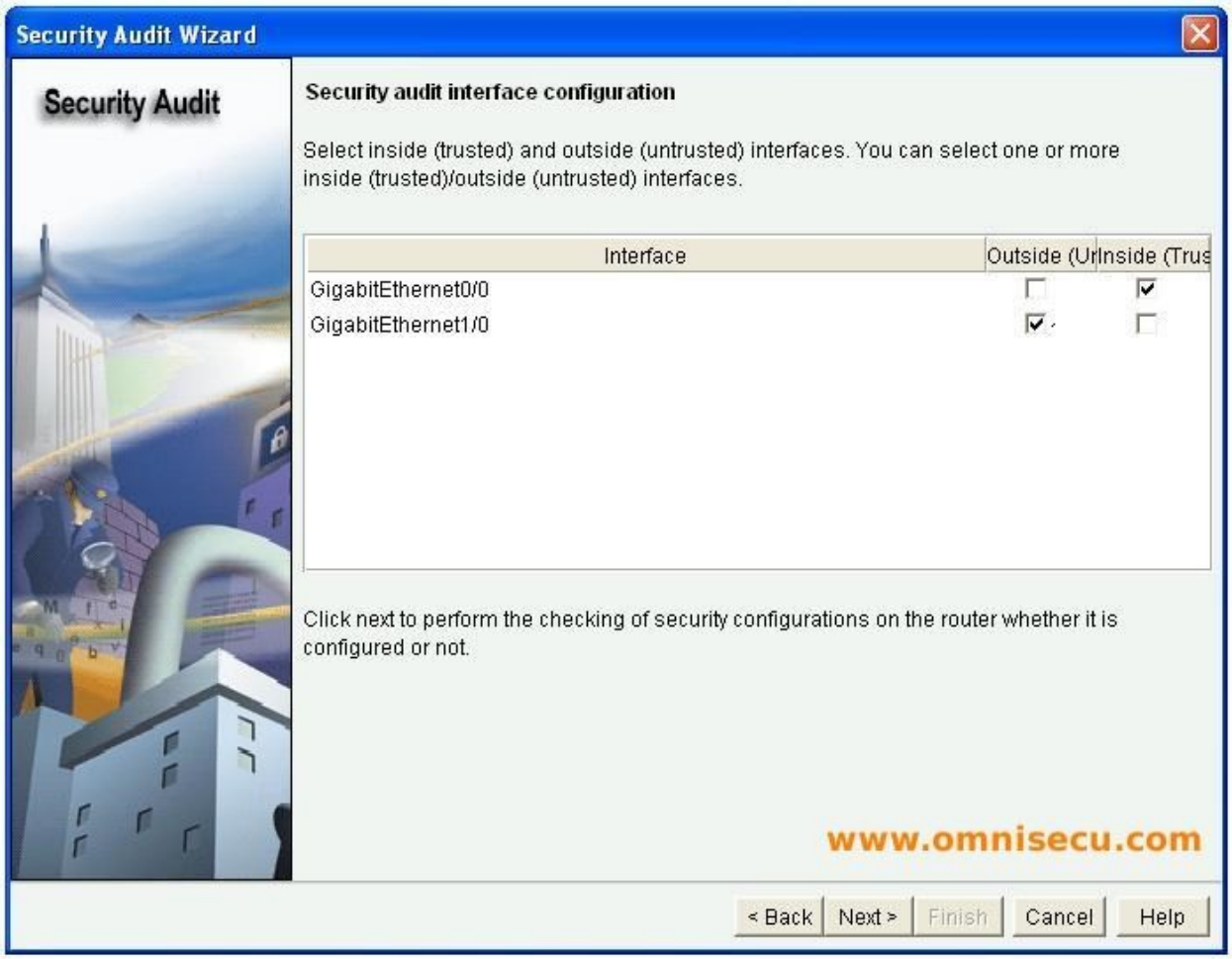
When you click on **Perform security audit,** another window opens.



Step 3: Perform a Security Audit.

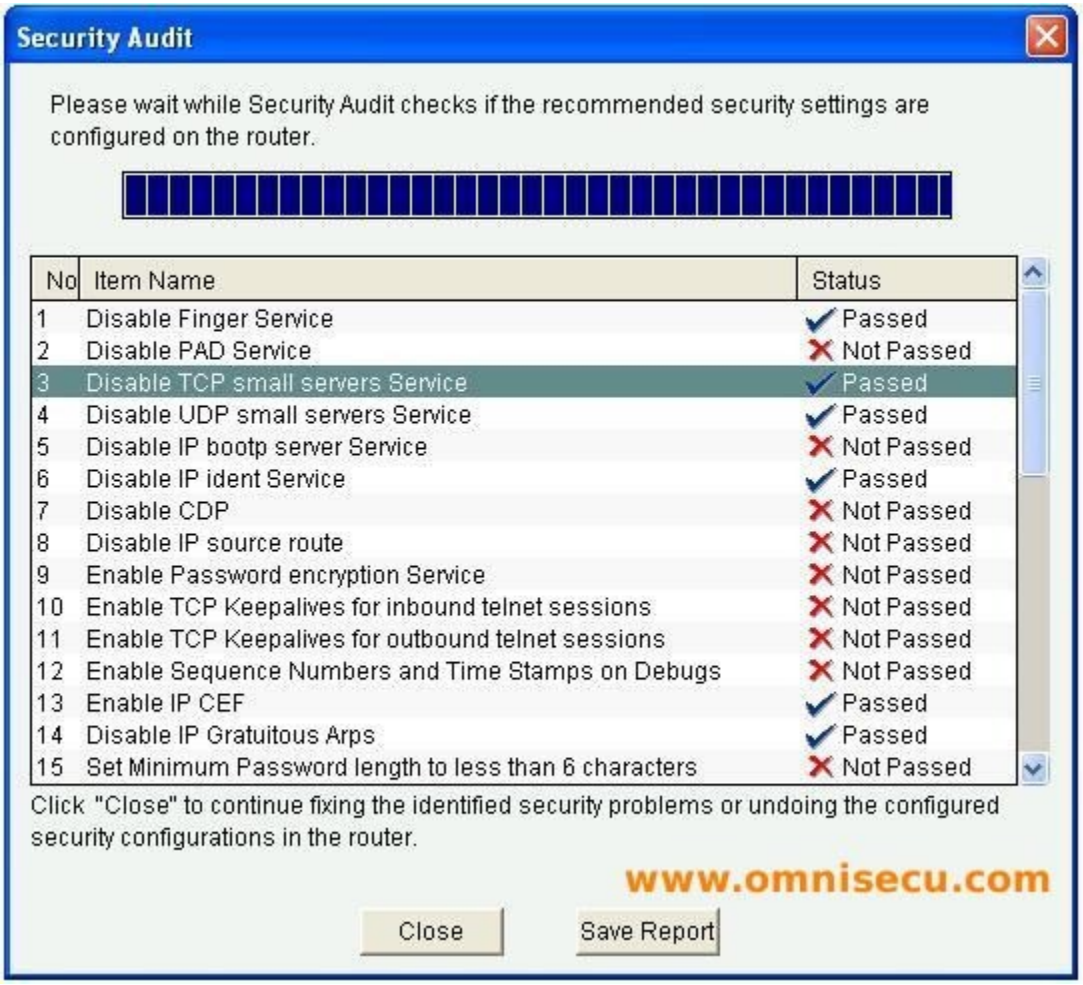


This gives a brief explanation of what the Security Audit feature does. Click on **Next** to open the Security Audit Interface configuration window.



An interface should be classified as outside (untrusted) if you cannot be sure of the legitimacy of the traffic coming into the interface. In this example, a GigabitEthernet0/1 is untrusted because GigabitEthernet0/1 is facing the Internet. A GigabitEthernet0/0 is trusted because it is the private LAN that is used inside the company.

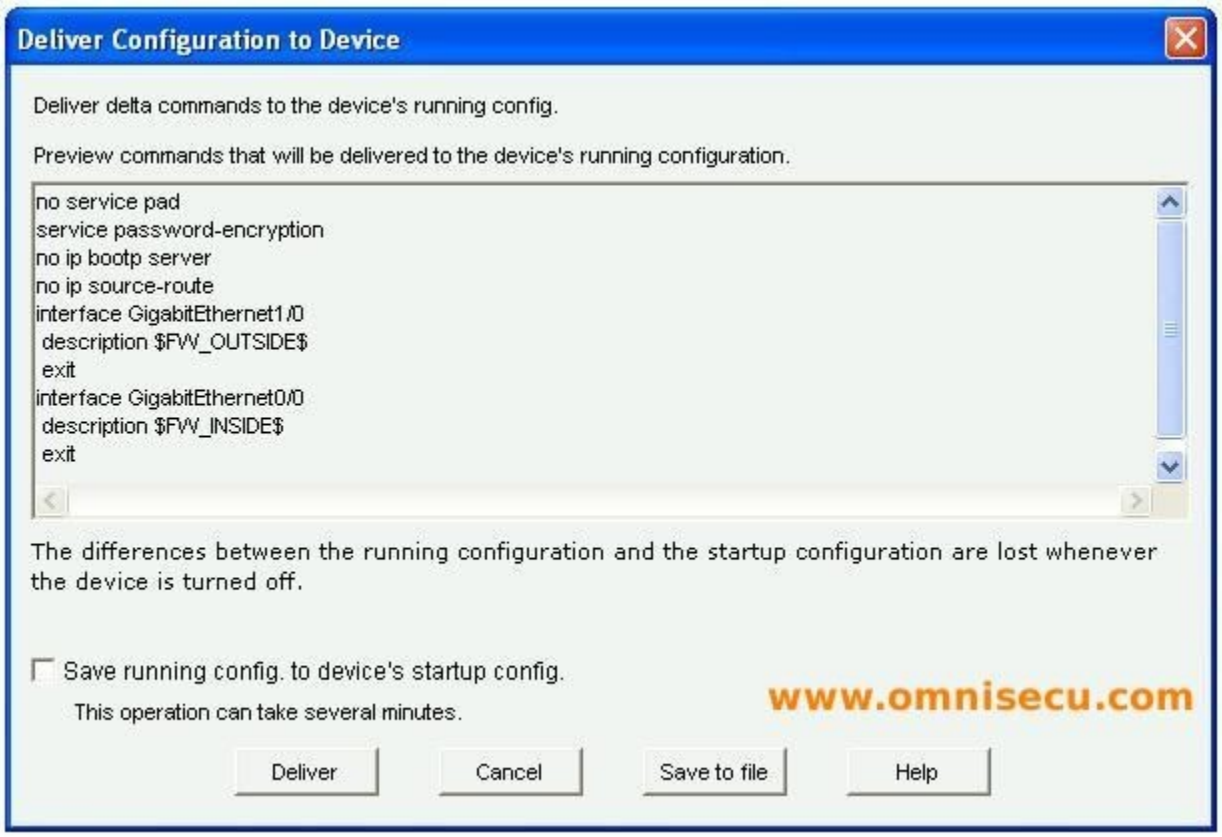
After selecting outside and inside interfaces, click **Next**. A new window opens indicating that CCP is conducting a security audit.



As you can see, the default configuration is unsecure. Click the **Close** button to continue.

Step 4: Apply settings to the router.

Click the **Fix All** button to make all the suggested security changes. Then click the **Next** button.



The CCP will now display "Deliver Configuration to Device" dialog box. Click "Deliver" to deliver the IOS commands to the Router

Task 9: Document the Router Configurations

On each router, issue the **`show run`** command and capture the configurations.

Task 10: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

