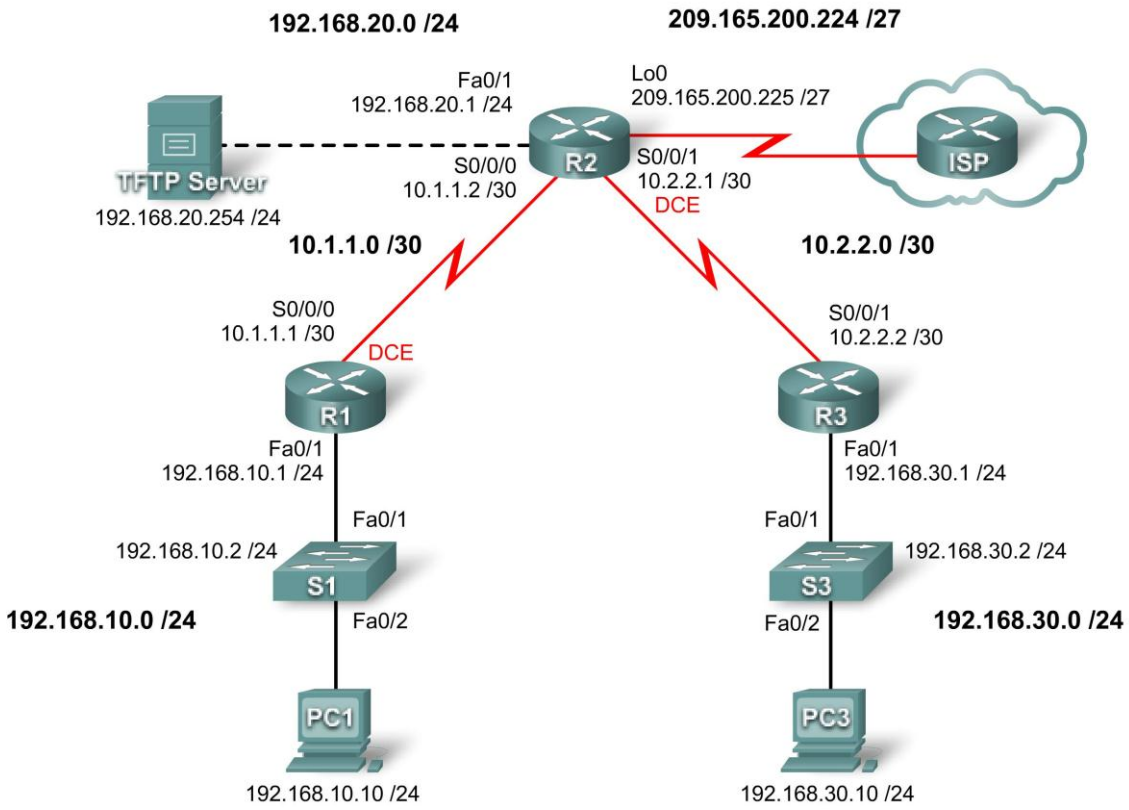
Lab: Basic Security Configuration

Topology Diagram



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

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 SDM.

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.

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 to configure secure passwords. Use **ciscoccna** for all passwords in this lab.

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

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

_____

_____

_____

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.

```
R(config)#username ccna privilege 15 password ciscoccna
R(config)#username kasutaja privilege 1 password parool123

Test the login with both usernames afterwards!
```

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

```
R(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.

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

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

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

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

```
R#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
 logging synchronous
 login authentication LOCAL_AUTH
line aux 0
line vty 0 4
 login authentication LOCAL_AUTH
!
```


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

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

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

```
R#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
 logging synchronous
 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 five 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 5 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: Configuring Secure Shell Virtual Terminal Access (SSH)

Step 1: As a requirement to generate an RSA general-usage key you'll need to change the hostname to a hostname other then the default "Router" hostname.

Step 2. Another requirement prior to generating an RSA certificate on the Cisco device is to set a domain name. For the purposes of this lab, the domain name will be set to **cnap.ut.ee** as shown below;

```
R(config)#ip domain-name cnap.ut.ee
```

Step 3. Now you're ready to generate the RSA certificate. To generate the RSA certification you'll execute the **crypto key generate rsa modulus** command followed by the modulus keysize which ranges between [360-2048]. As shown below, an RSA certificate is generated using a 2048 bit modulus key.

```
R1(config)#crypto key generate rsa modulus 2048
```

You'll notice that immediately after the rsa general keys are generated, SSH v1.99 is enabled.

Once SSH v1.99 is enabled you can connect to the Cisco device remotely using the SSH v2 protocol found in Putty, SecureCRT and other terminal emulators; excluding HyperTerminal as it does not support cryptographic connectivity.

Task 5: 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 6: 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 your PC as the syslog server for your router. Run KiWi Syslog Server application for that.. 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: PC 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, 5, 6, and 7.

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

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

_____

_____

_____

Note: G enerate and look at syslog software for messages.

Task 7: Disabling Unused Cisco Network Services

Step 1: Disable unused interfaces.

Why should you disable unused interfaces on network devices?

_____

_____

_____

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            10.1.0.1        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
```

What kind of attack does disabling IP redirects, IP unreachables, and IP directed broadcasts mitigate?

_____

_____

_____

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 8: Using SDM to Secure a Router

In this task, you will use Security Device Manager (SDM), the GUI interface, to secure router R. SDM is faster than typing each command and gives you more control than the AutoSecure feature.

Step 1: Configuring SDM prerequisites.

Create a username and password for your router

```
R(config)#username ccna privilege 15 password ciscoccna
```

Enable the http secure server on R and authenticate it to a local user database.

```
R(config)#ip http server
R(config)#ip http secure-server
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R(config)#
*Nov 16 16:01:07.763: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Nov 16 16:01:08.731: %PKI-4-NOAUTOSAVE: Configuration was modified.  Issue
"write memory" to save new certificate
R(config)#ip http authentication local
```

Configure the VTY lines 0 through 4 to authenticate using the local database and accept incoming connections using TELNET or SSH only.

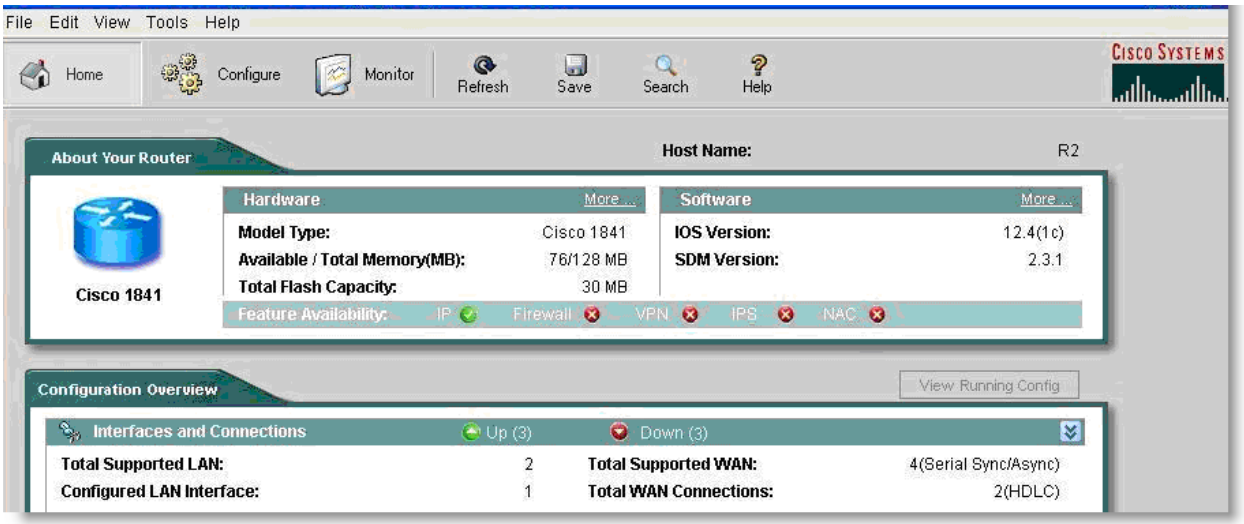
```
R(config)#line vty 0 4
R(config-line)#login local
R(config-line)#transport input telnet ssh
R(config-line)#end

R#copy run start
```

From your PC, execute SDM application, connect to your router and login with the previously configured username and password:

Also make sure that JAVA is installed and updated.

After it is done loading, a new window opens for SDM.



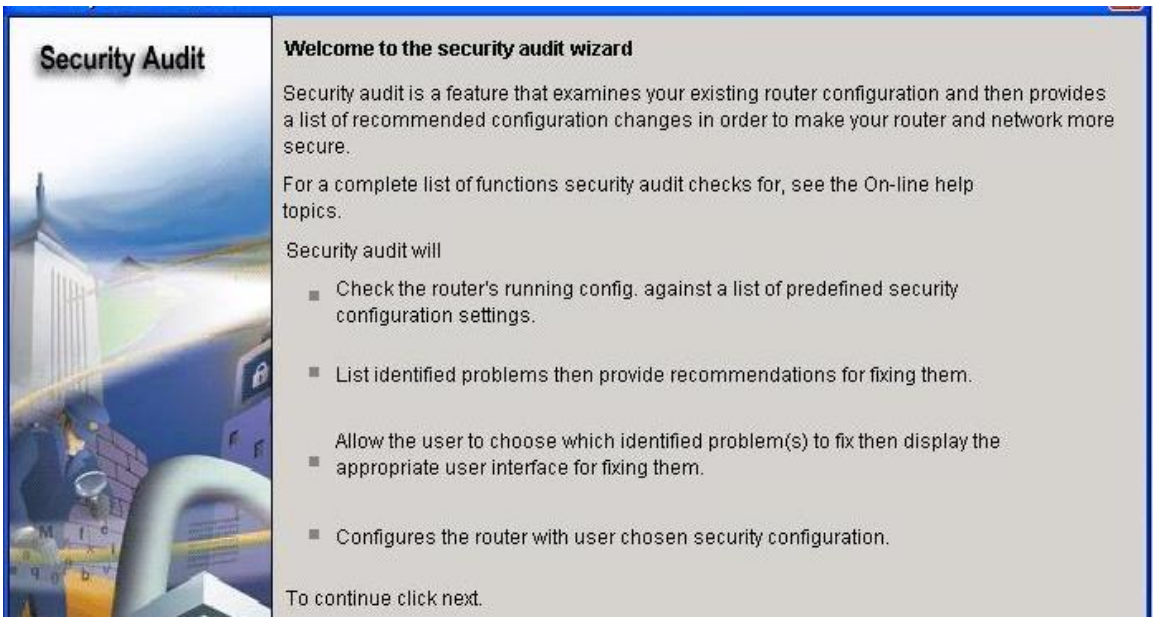
Step 2: Navigate to the Security Audit feature.

Click the **Configure** button in the top left side of the window.

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

When you click on **Security Audit,** another window opens.

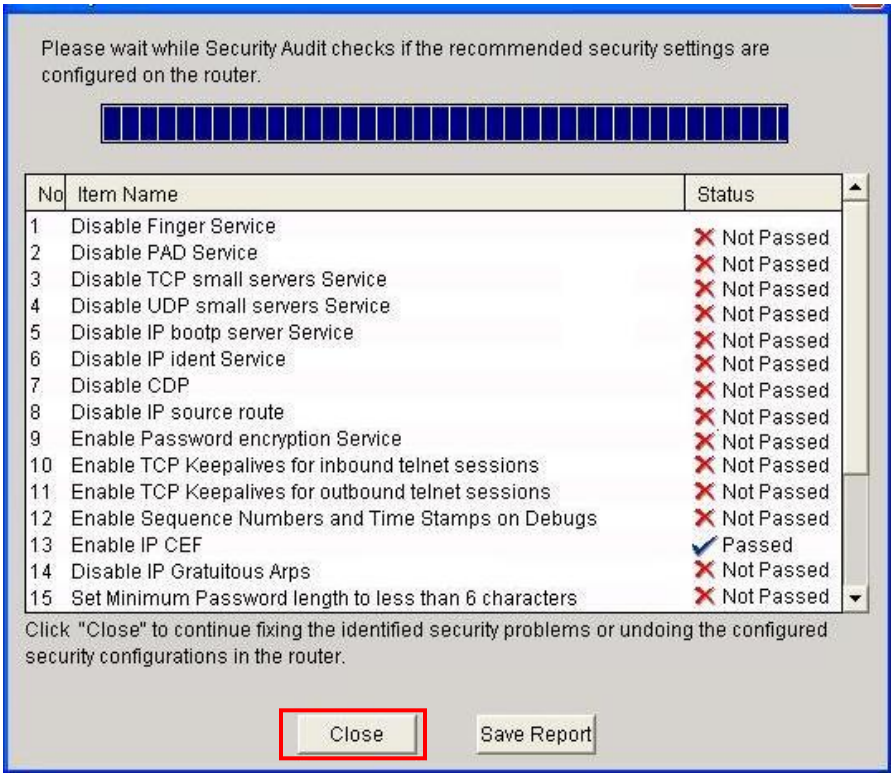
Step 3: Perform a Security Audit.



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

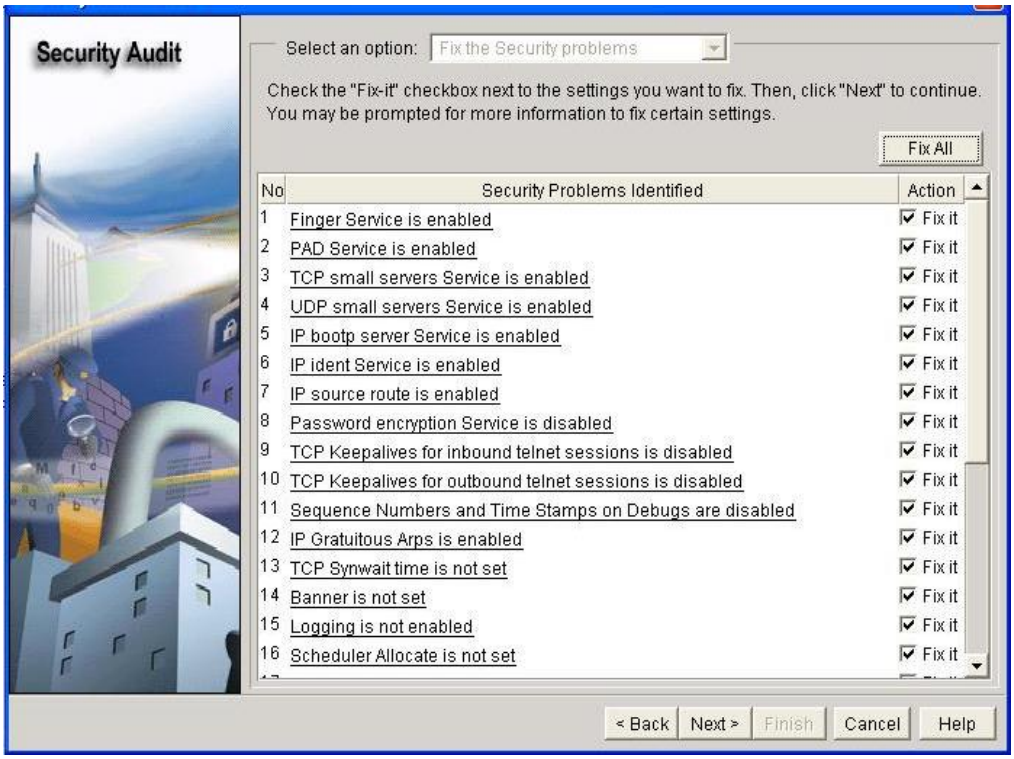
An interface should be classified as outside (untrusted) if you cannot be sure of the legitimacy of the traffic coming into the interface. In this example, both FastEthernet0/1 and Serial0/1/0 are untrusted because Serial0/1/0 is facing the Internet, and Fastethernet0/1 is facing the access part of the network and illegitimate traffic could be generated.

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

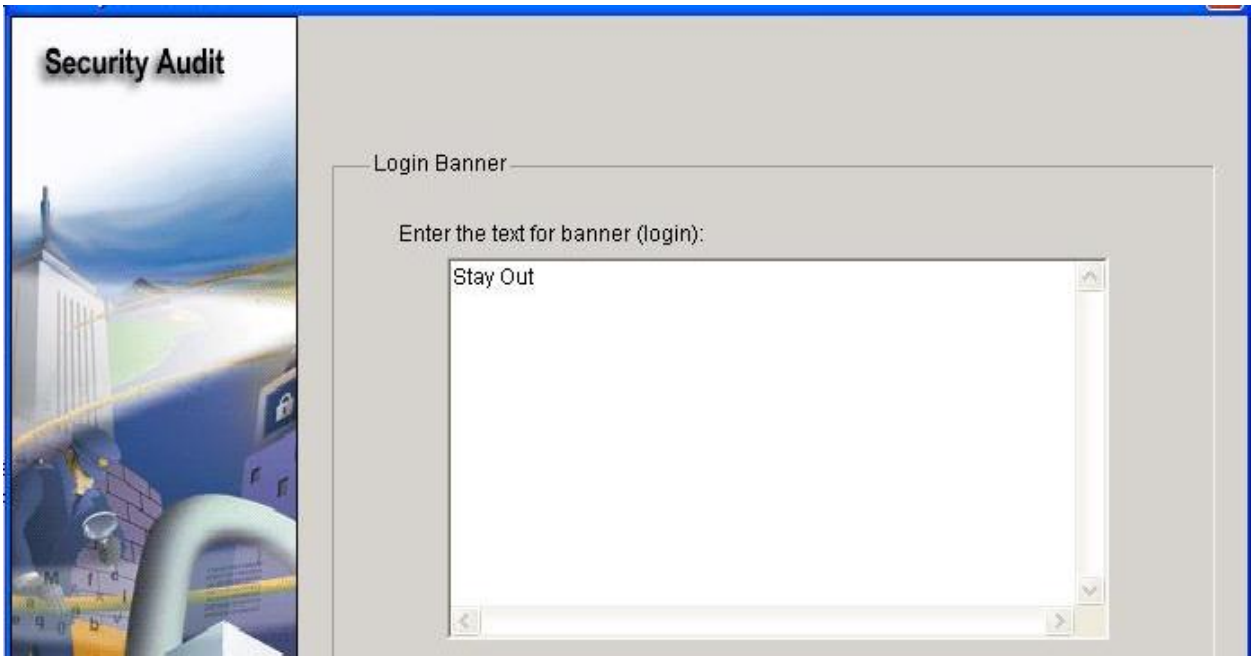


As you can see, the default configuration is unsecure. Click the **Close** button to continue.

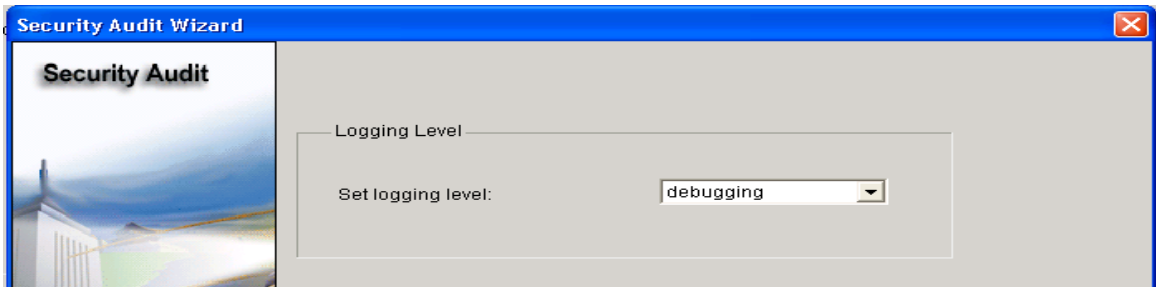
Step 4: Apply settings to the router.



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

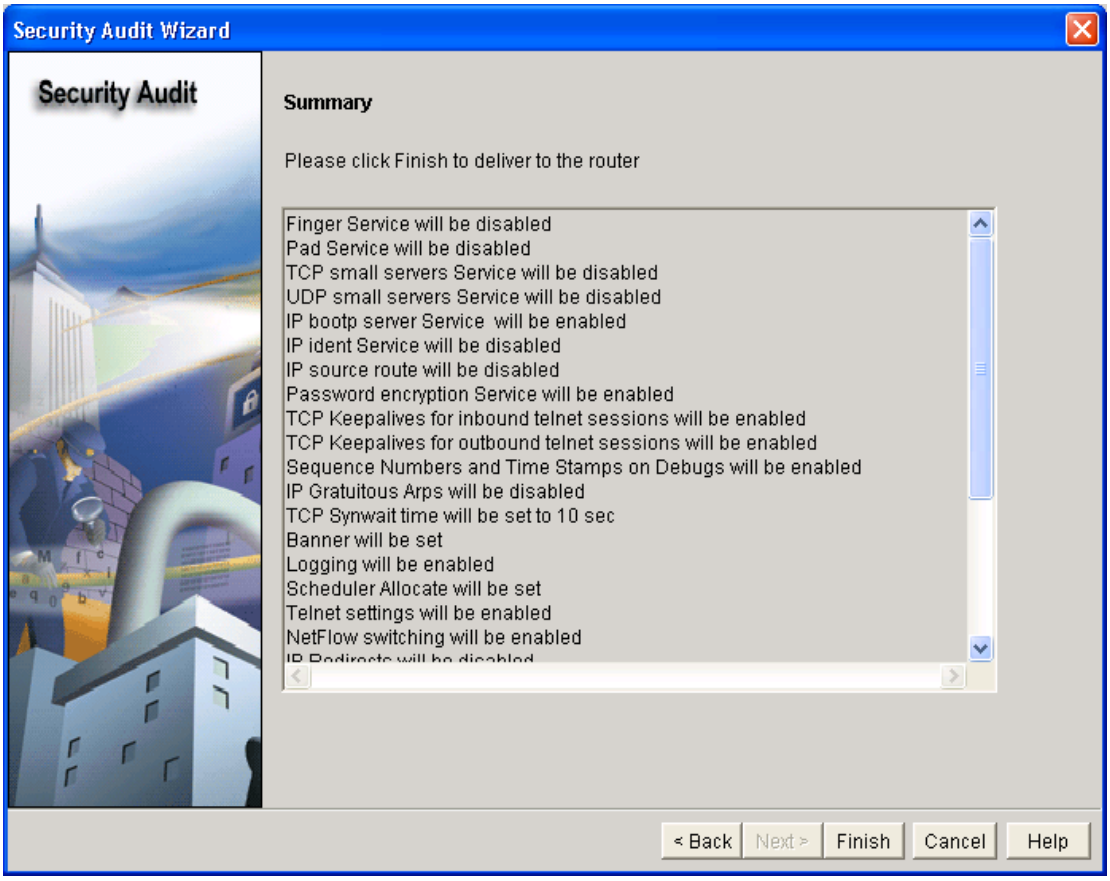


Enter a banner message to use as the message of the day for the router, and then click **Next**.

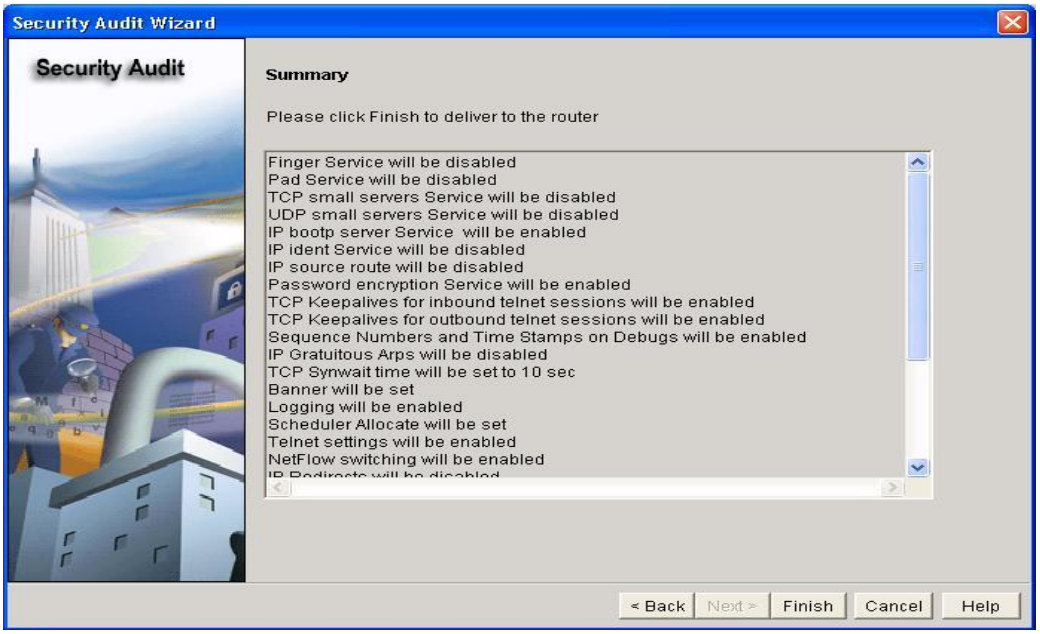


Next, set the level of severity of log traps that you want the router to send to the syslog server. The severity level is set to debugging for this scenario. Click **Next** to view a summary of the changes about to be made to the router.

Step 5: Commit the configuration to the router.



After reviewing the changes about to be committed, click **Finish**.



Click **OK** and exit SDM.

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.

