Lab - Configure Automated Security Features

# Topology



# Addressing Table

| Device | Interface | IP Address | Subnet Mask | Default Gateway | Switch Port |
| --- | --- | --- | --- | --- | --- |
| R1 | G0/0/0 | 10.1.1.1 | 255.255.255.252 | N/A | N/A |
| R1 | G0/0/1 | 192.168.1.1 | 255.255.255.0 | N/A | S1 F0/5 |
| R2 | G0/0/0 | 10.1.1.2 | 255.255.255.252 | N/A | N/A |
| R2 | G0/0/1 | 10.2.2.2 | 255.255.255.252 | N/A | N/A |
| R3 | G0/0/0 | 10.2.2.1 | 255.255.255.252 | N/A | N/A |
| R3 | G0/0/1 | 192.168.3.1 | 255.255.255.0 | N/A | S3 F0/5 |
| PC-A | NIC | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 | S1 F0/6 |
| PC-C | NIC | 192.168.3.3 | 255.255.255.0 | 192.168.3.1 | S3 F0/18 |

Blank Line, No additional information

# Objectives

Part 1: Configure Basic Device Settings

* Cable the network as shown in the topology.
* Configure basic IP addressing for routers and PCs.
* Configure OSPF routing.
* Configure PC hosts.
* Verify connectivity between hosts and routers.

Part 2: Configure Automated Security Features

* Lock down a router using AutoSecure and verify the configuration.
* Contrast using AutoSecure with manually securing a router using the command line.

# Background / Scenario

The router is a critical component in any network. It controls the movement of data into and out of the network and between devices within the network. It is particularly important to protect network routers because the failure of a routing device could make sections of the network, or the entire network, inaccessible. Controlling access to routers and enabling reporting on routers is critical to network security and should be part of a comprehensive security policy.

In this lab, you will build a multi-router network and configure the routers and hosts. You will use automated security features on router R3.

**Note**: The routers used with hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.6 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960+ with Cisco IOS Release 15.2(7) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

**Note**: Before you begin, ensure that the routers and the switches have been erased and have no startup configurations.

# Required Resources

* 3 Routers (Cisco 4221 with Cisco XE Release 16.9.6 universal image or comparable with a Security Technology Package license)
* 2 Switches (Cisco 2960+ with Cisco IOS Release 15.2(7) lanbasek9 image or comparable)
* 2 PCs (Windows OS with a terminal emulation program, such as PuTTY or Tera Term installed)
* Console cables to configure Cisco networking devices
* Ethernet cables as shown in the topology

# Instructions

## Configure Basic Device Settings

In this part, set up the network topology and configure basic settings, such as interface IP addresses.

### Cable the network.

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

### Configure basic settings for each router.

Open configuration window

* + - 1. Console into the router and enable privileged EXEC mode.

Router> **enable**

Router# **configure terminal**

Configure host names as shown in the topology.

R1(config)# **hostname R1**

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

R1(config)# **interface g0/0/0**

R1(config-if)# **ip address 10.1.1.1 255.255.255.252**

R1(config-if)# **no shutdown**

R1(config)# **interface g0/0/1**

R1(config-if)# **ip address 192.168.1.1 255.255.255.0**

R1(config-if)# **no shutdown**

* + - 1. To prevent the router from attempting to translate incorrectly entered commands as though they were host names, disable DNS lookup. R1 is shown here as an example.

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

### Configure OSPF routing on the routers.

* + - 1. Use the **router ospf** command in global configuration mode to enable OSPF on R1.

R1(config)# **router ospf 1**

* + - 1. Configure the **network** statements for the networks on R1. Use an area ID of 0.

R1(config-router)# **network 192.168.1.0 0.0.0.255 area 0**

R1(config-router)# **network 10.1.1.0 0.0.0.3 area 0**

* + - 1. Configure OSPF on R2 and R3.

R2(config)# **router ospf 1**

R2(config-router)# **network 10.1.1.0 0.0.0.3 area 0**

R2(config-router)# **network 10.2.2.0 0.0.0.3 area 0**

R3(config)# **router ospf 1**

R3(config-router)# **network 10.2.2.0 0.0.0.3 area 0**

R3(config-router)# **network 192.168.3.0 0.0.0.255 area 0**

* + - 1. Issue the **passive-interface** command to change the G0/0/1 interface on R1 and R3 to passive.

R1(config)# **router ospf 1**

R1(config-router)# **passive-interface g0/0/1**

R3(config)# **router ospf 1**

R3(config-router)# **passive-interface g0/0/1**

### Verify OSPF neighbors and routing information.

* + - 1. Issue the **show ip ospf neighbor** command to verify that each router lists the other routers in the network as neighbors.

R1# **show ip ospf neighbor**

Neighbor ID Pri State Dead Time Address Interface

10.2.2.2 1 FULL/BDR 00:00:37 10.1.1.2 GigabitEthernet0/0/0

* + - 1. Issue the **show ip route** command to verify that all networks display in the routing table on all routers.

R1# **show ip route**

Codes: L - local, 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, H - NHRP, l - LISP

a - application route

+ - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks

C 10.1.1.0/30 is directly connected, GigabitEthernet0/0/0

L 10.1.1.1/32 is directly connected, GigabitEthernet0/0/0

O 10.2.2.0/30 [110/2] via 10.1.1.2, 00:01:11, GigabitEthernet0/0/0

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.1.0/24 is directly connected, GigabitEthernet0/0/1

L 192.168.1.1/32 is directly connected, GigabitEthernet0/0/1

O 192.168.3.0/24 [110/3] via 10.1.1.2, 00:01:07, GigabitEthernet0/0/0

### Configure PC host IP settings.

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

### Verify connectivity between PC-A and PC-C.

* + - 1. Ping from R1 to R3.

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

* + - 1. Ping from PC-A, on the R1 LAN, to PC-C, on the R3 LAN.

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

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

Close configuration window

## Configure Basic Security Settings on R1

In this part, copy and paste the following commands into R1 to configure basic security settings.

Open configuration window

enable

configure terminal

service password-encryption

security passwords min-length 10

enable algorithm-type scrypt secret cisco12345

ip domain name netsec.com

username user01 algorithm-type scrypt secret user01pass

username admin privilege 15 algorithm-type scrypt secret adminpasswd

banner motd " Unauthorized access is strictly prohibited! "

line con 0

exec-timeout 5 0

login local

logging synchronous

line aux 0

exec-timeout 5 0

login local

line vty 0 4

exec-timeout 5 0

privilege level 15

transport input ssh

login local

crypto key generate rsa general-keys modulus 1024

ip ssh time-out 90

ip ssh authentication-retries 2

ip ssh version 2

close configuration window

## Configure Automated Security Features

In this part, you will do as follows:

* Use AutoSecure to secure R3.
* Review router security configurations with CLI.

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. It can also 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.

### Use the AutoSecure Cisco IOS feature on R3.

* + - 1. Enter privileged EXEC mode using the **enable** command.
      2. Issue the **auto secure** command on R3 to lock down the router. R2 represents an ISP router, so assume that R3 G0/0/0 is connected to the internet when prompted by the AutoSecure questions. Respond to the AutoSecure questions as shown in the following output. The responses are bolded.

Open configuration window

R3# **auto secure**

--- AutoSecure Configuration ---

\*\*\* AutoSecure configuration enhances the security of

the router but it will not make router absolutely secure

from all security attacks \*\*\*

All the configuration done as part of AutoSecure will be

shown here. For more details of why and how this configuration

is useful, and any possible side effects, please refer to Cisco

documentation of AutoSecure.

At any prompt you may enter '?' for help.

Use ctrl-c to abort this session at any prompt.

If this device is being managed by a network management station,

AutoSecure configuration may block network management traffic.

Continue with AutoSecure? [no]: **yes**

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]: **yes**

Enter the number of interfaces facing internet [1]:

Interface IP-Address OK? Method Status Protocol

GigabitEthernet0/0/0 10.2.2.1 YES manual up up

GigabitEthernet0/0/1 192.168.3.1 YES manual up up

Serial0/1/0 unassigned YES unset up up

Serial0/1/1 unassigned YES unset up up

Enter the interface name that is facing internet: **GigabitEthernet0/0/0**

Securing Management plane services..

Disabling service finger

Disabling service pad

Disabling udp & tcp small servers

Enabling service password encryption

Enabling service tcp-keepalives-in

Enabling service tcp-keepalives-out

Disabling the cdp protocol

Disabling the bootp server

Disabling the http server

Disabling the finger service

Disabling source routing

Disabling gratuitous arp

Here is a sample Security Banner to be shown

at every access to device. Modify it to suit your

enterprise requirements.

Authorized Access only

This system is the property of So-&-So-Enterprise.

UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.

You must have explicit permission to access this

device. All activities performed on this device

are logged. Any violations of access policy will result

in disciplinary action.

Enter the security banner {Put the banner between

k and k, where k is any character}:

**# Unauthorized Access Prohibited #**

Enable secret is either not configured or

is the same as the enable password

Enter the new enable secret: **cisco12345**

Confirm the enable secret : **cisco12345**

Enter the new enable password: **12345cisco**

Confirm the enable password: **12345cisco**

Configuration of local user database

Enter the username: **admin**

Enter the password: **adminpasswd**

Confirm the password: **adminpasswd**

Configuring AAA local authentication

Configuring console, Aux and vty lines for

local authentication, exec-timeout, transport

Securing device against Login Attacks

Configure the following parameters

Blocking Period when Login Attack detected: **60**

Maximum Login failures with the device: **2**

Maximum time period for crossing the failed login attempts: **30**

Configure SSH server? [yes]: **[Enter]**

Enter the domain-name: **www.netsec.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

Securing Forwarding plane services..

Enabling unicast rpf on all interfaces connected

to internet

Configure CBAC Firewall feature? [yes/no]: **no**

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

banner motd ^C Unauthorized Access Prohibited ^C

security passwords min-length 6

security authentication failure rate 10 log

enable secret 5 $1$lubv$Rdx4gHUcijbxV7p2z76/71

enable password 7 110A1016141D5D5B5C737B

username admin password 7 02050D4808095E731F1A5C

aaa new-model

aaa authentication login local\_auth local

line console 0

login authentication local\_auth

exec-timeout 5 0

transport output telnet

line aux 0

login authentication local\_auth

exec-timeout 10 0

transport output telnet

line vty 0 4

login authentication local\_auth

transport input telnet

line tty 1

login authentication local\_auth

exec-timeout 15 0

login block-for 60 attempts 2 within 30

ip domain-name www.netsec.com

crypto key generate rsa general-keys modulus 1024

ip ssh time-out 60

ip ssh authentication-retries 2

line vty 0 4

transport input ssh telnet

service timestamps debug datetime msec localtime show-timezone

service timestamps log datetime msec localtime show-timezone

logging facility local2

logging trap debugging

service sequence-numbers

logging console critical

logging buffered

int GigabitEthernet0/0/0

no ip redirects

no ip proxy-arp

no ip unreachables

no ip directed-broadcast

no ip mask-reply

int GigabitEthernet0/0/1

no ip redirects

no ip proxy-arp

no ip unreachables

no ip directed-broadcast

no ip mask-reply

ip access-list extended 100

permit udp any any eq bootpc

interface GigabitEthernet0/0/0

ip verify unicast source reachable-via rx 100

!

end

Apply this configuration to running-config? [yes]: **[Enter]**

Applying the config generated to running-config

WARNING: Command has been added to the configuration using a type 5 password. However, type 5 passwords will soon be deprecated. Migrate to a supported password type

WARNING: Command has been added to the configuration using a type 7 password. However, type 7 passwords will soon be deprecated. Migrate to a supported password type

WARNING: Command has been added to the configuration using a type 7 password. However, type 7 passwords will soon be deprecated. Migrate to a supported password typeThe name for the keys will be: R3.www.netsec.com

% The key modulus size is 1024 bits

% Generating 1024 bit RSA keys, keys will be non-exportable...

[OK] (elapsed time was 0 seconds)

R3#

**Note**: The questions asked and the output may vary depend on the features on the IOS image and device.

### Establish an SSH connection from PC-C to R3.

* + - 1. Start PuTTy or another SSH client, and log in with the **admin** account and password **adminpasswd** created when AutoSecure was run. Enter the IP address of the R3 G0/0/1 interface **192.168.3.1**.
      2. Because SSH was configured using AutoSecure on R3, you will receive a PuTTY security warning. Click **Yes** to connect anyway.
      3. Enter privileged EXEC mode with password **cisco12345**, and verify the R3 configuration using the **show run** command.

### Contrast the AutoSecure-generated configuration of R3 with the manual configuration of R1.

#### Questions:

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

Type your answers here.

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

Type your answers here.

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

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

Services disabled include:

Type your answers here.

For each interface, the following were disabled:

Type your answers here.

* 1. What are some advantages to using AutoSecure?

Type your answers here.

Close configuration window

# Router Interface Summary Table

| Router Model | Ethernet Interface #1 | Ethernet Interface #2 | Serial Interface #1 | Serial Interface #2 |
| --- | --- | --- | --- | --- |
| 1900 | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2900 | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 4221 | Gigabit Ethernet 0/0/0 (G0/0/0) | Gigabit Ethernet 0/0/1 (G0/0/1) | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |
| 4300 | Gigabit Ethernet 0/0/0 (G0/0/0) | Gigabit Ethernet 0/0/1 (G0/0/1) | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |

Blank Line, No additional information

**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.

End of document