Configuration Labs

Part 4: Network Security

Lab 2: Configuring Access Lists I

Objective

The overall objective of this laboratory exercise is to gain experience with configuring access lists on a Cisco router. Your task in this lab is to configure an access control list (ACL) that denies Telnet and web traffic but permits all other traffic. You will then enable that ACL for packets entering R1's S0/0/0 interface. You will test the configuration by sending a ping, which should be allowed, and attempting to telnet, which should be denied.

Topology

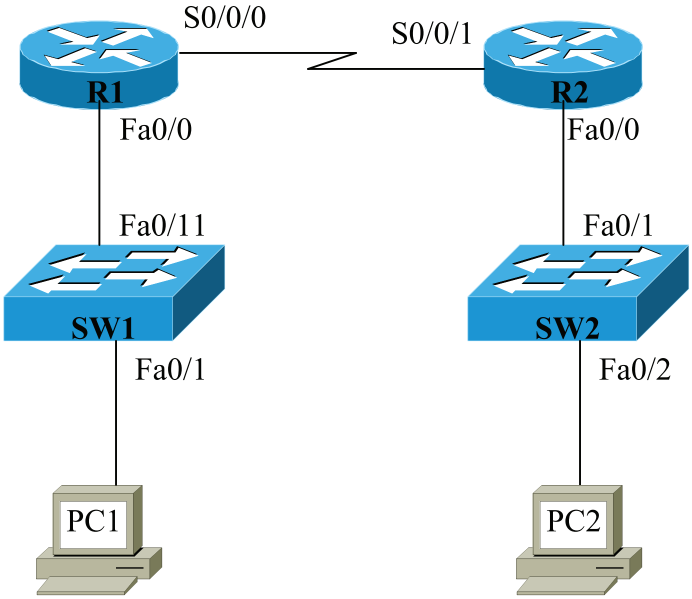

Figure 1 Network Topology for This Lab

Reference

The following simulator exercises provided with the CCNA 640-802 Network Simulator should be reviewed prior to starting this virtual laboratory exercise:

- ACL I–VI
- Named ACL I–III
- ACL Analysis I

Key Concepts

The following concepts, terms, commands, and steps should have been mastered in this exercise:

- The steps for creating an access list.
- There is an implicit deny at the end of an access list.
- The necessity to always place a permit statement at the end of an access list to override the implicit deny.
- Issuing the **access-list** command.
- Applying the access list using the **ip access-group** command.
- Applying the access list to the inbound or outbound direction.
- The steps for creating an access list to deny UDP traffic.
- The steps for creating an access list to deny Telnet traffic.
- The steps for creating an access list to deny by port numbers.
- The features of a standard access list.
- The features of an extended access list.

Reference Tables

Table 1 provides the IP addresses and masks of all necessary interfaces used to complete this lab.

Table 1 Computer IP Addresses, Subnet Masks, and Gateway Addresses for This Lab

Computer/Interface – R1	IP Address	Subnet Mask	Gateway Address
PC1	172.16.160.11	255.255.255.224	172.16.160.1
R1-FA0/0	172.16.160.1	255.255.255.224	—
R1-S0/0/0	172.16.128.5	255.255.255.252	—

Computer/Interface – R2	IP Address	Subnet Mask	Gateway Address
PC1	172.16.192.12	255.255.255.224	172.16.192.1
R2-FA0/0	172.16.192.1	255.255.255.224	—
R2-S0/0/1	172.16.128.6	255.255.255.252	—

Table 2 Settings for Router 1 [R1] and Router 2 [R2]

Setting	Password
enable secret	ciscopress
line vty 0 4	ciscopress
line con 0	ciscopress

Task 1

Configure the network routers (R1 and R2) and computers PC1 and PC2 to operate in the network using the IP addresses, subnet masks, and gateway addresses specified in Table 1. You are to also configure Routing Information Protocol (RIP) routing between the two networks.

Step 1. Configure the IP address and subnet masks for Routers R1 and R2 and PC1 and PC2. List the steps taken to accomplish this task. List the router prompts and commands for each task.

Router R1

```
R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# interface fa0/0
R1(config-if)# ip address 172.16.160.1 255.255.255.224
R1(config-if)# no shut
R1(config-if)#

R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# interface serial 0/0/0
R1(config-if)# ip address 172.16.128.5 255.255.255.252
R1(config-if)# clock rate 128000
R1(config-if)# no shut
R1(config-if)#
```

PC1

```
C:\> ip address 172.16.160.11 255.255.255.224
C:\> gateway 172.16.160.1
```

Router R2

```
R2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)# int fa0/0
R2(config-if)# ip address 172.16.192.1 255.255.255.224
R2(config-if)# no shut
R2(config-if)#

R2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
R2(config)# interface s0/0/1
R2(config-if)# ip address 172.16.128.6 255.255.255.224
R2(config-if)# no shut
R2(config-if)#
```

PC2

```
C:\> ip address 172.16.192.12 255.255.255.224
C:\> gateway 172.16.192.1
```

Step 2. Configure RIPv2 routing for the network. List the router prompts and commands to accomplish this task.

```
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# network 172.16.0.0
R1(config-router)#

R2(config)# router rip
R2(config-router)# version 2
R2(config-router)# network 172.16.0.0
R2(config-router)#
```

Step 3. Verify that the network routing is properly configured. Discuss the steps you took to accomplish this. Make corrections to the network configurations as needed.

```
R2# sh ip route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
R    172.16.160.0/27 [120/1] via 172.16.128.5, 00:22:20, Serial0/0/1
C    172.16.128.4/30 is directly connected, Serial0/0/1
C    172.16.192.0/27 is directly connected, FastEthernet0/0

R2#

R1# sh ip route
Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C    172.16.160.0/27 is directly connected, FastEthernet0/0
C    172.16.128.4/30 is directly connected, Serial0/0/0
R    172.16.192.0/27 [120/1] via 172.16.128.6, 00:24:25, Serial0/0/0

R1#
```

Use the **ping** command to verify connectivity for Routers 1 and 2 and PC1 and PC2. Also use **sh ip int brief** to verify interfaces. Next, verify the settings for PC1 and PC2. The ping was successful from PC1 to PC2. No corrections needed. The **show ip route** command shows that routing has been configured for all the networks.

Step 4. In this step, you will create an ACL on Router R1 that filters all User Datagram Protocol (UDP) traffic coming into the serial 0/0/0 interface on Router R1. You will also allow all other traffic, including Internet Control Message Protocol (ICMP), to enter the network. You can simulate UDP traffic by issuing the **traceroute** command, and you can simulate ICMP traffic by issuing the **ping** command. Given this information, create an access list that meets this requirement. Note that when testing your access list you will issue the **traceroute** and **ping** commands from Router R2 to test your ACL.

Create access list:

```
R1(config)# access-list 100 deny udp any any
R1(config)# access-list 100 permit ip any any
```

Apply access list to the s0/0/0 interface:

```
R1(config)# int s0/0/0
R1(config-if)# ip access-group 100 in

R2# ping 172.16.160.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.160.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round - trip min/avg/max =1/5/16 ms

R2# traceroute 172.16.160.1
Type escape sequence to abort.
Tracing the route to 172.16.160.1
1            *    *    *
2            *    *    *
3
R2#
```

Step 5. Your task now is to create an ACL on Router R1 that will deny Telnet but permit all other traffic, including ICMP. Given this information, write what you think the configuration should be. You will first need to remove the ACL configured in Step 4 and enable a Telnet connection on R1. Next, create the access list on R1 (you don't need to apply it because this was done already for Step 4). Next, you will test your access list by issuing the **telnet** and **ping** commands from Router R2 to test your ACL.

```
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# no access-list 100
R1(config)# line vty 0 4
R1(config-line)# password ciscopress
R1(config-line)# login
R1(config-line)#
```

Create access list:

```
R1(config)# access-list 100 deny tcp any any eq telnet
R1(config)# access-list 100 permit ip any any
```

```
R2#
R2# telnet 172.16.160.1
% Destination unreachable; gateway or host down

But the ping command still works to same interface.
R2# ping 172.16.160.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.160.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round - trip min/avg/max =1/5/16 ms
R2#
```

Step 6. Your next task is to configure on R2's serial 0/0/1 interface an outbound ACL that denies Telnet access for Telnet users in subnet 172.16.192.0/27 (R2's LAN subnet) who try to connect to Telnet servers in subnet 172.16.160.0/27 (R1's LAN subnet). The ACL should also allow other types of traffic between hosts in those same subnets. In this lab, you will use wildcard masks to filter traffic to and from these specific networks. Given this information, write what you think the access list configuration should be. You will need to remove the access list on R1 to be able to test your configuration.

```
R1(config)# no access-list 100
```

Create access list:

```
R2(config)# access-list 100 deny tcp 172.16.192.0 0.0.0.31 172.16.160.0
0.0.0.31  eq telnet
R2(config)# access-list 100 permit ip 172.16.192.0 0.0.0.31 172.16.160.0
0.0.0.31
```

Apply access list to the s0/0/1 interface:

```
R2(config)# int  s0/0/1
R2(config-if)# ip access-group 100 in
```

Task 2: Access List Questions

The following is a partial list of the items displayed when you issue the **show access-lists** command on a router. Your task is to define each item and its purpose. You might need to go to the Cisco website (http://www.cisco.com) and look up what each of these commands means.

What is the purpose/function of the following commands?

1. R1(config)# **access-list 10 permit host 10.10.20.250**

   This access list permits data traffic from 10.10.20.250. The **host** command indicates a wildcard mask of 0.0.0.0.

2. R1(config)# **access-list 100 deny tcp 172.50.12.0 0.0.0.255 172.50.10.0 0.0.0.255 eq 23**

   This access list denies Telnet packets (port 23) from 172.50.12.0 going to 172.50.10.0.

3. R1(config)# **access-list 100 permit ip any any**

   This access list is typically placed at the end of the access list to permit IP traffic from going anywhere. This is added because there is an implicit deny with the access-list.

4. R1(config-if)# **ip access-group 100 in**

   This applies access list 100 on the inbound direction.

5. R1(config)# **access-list 101 permit tcp 0.0.0.0 255.255.255.255 130.120.110.100 0.0.0.0 eq 80**

   This permits any TCP data (web traffic) going to the specific IP address 10.120.110.110.

6. R1(config)# **access-list 101 deny ip any any**

   This statement denies any source to any destination.

7. R1(config-if)# **no ip access-group 100 in**

   Turns off access list 100 on the inbound direction.

8. R1(config)# **access-list 122 permit udp any eq domain host 192.168.1.1 gt 1023**

   This access list permits Domain Name System (DNS) access through your firewall to the DNS server 192.168.1.1.

9. R1(config)# **access-list rate-limit 10 mask 07**

   This assigns packets with an IP Precedence of 0, 1, or 2 to the rate-limit access list 10.

R1

```
R1# sh running-config
Building configuration...
Current configuration : 800 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$KXED$S08d0zG3x3aiaeFjy7nCP
!
no aaa new-model
!
resource policy
!
!
!
ip cef
!
!
!
!
!
!
!
```

```
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address  172.16.160.1 255.255.255.224
!
interface FastEthernet0/1
 no ip address
 shutdown
!
interface Serial0/0/0
 ip address 172.16.128.5 255.255.255.252
 ip access-group 100 in
 clock rate 128000
!
interface Serial0/0/1
 no ip address
 shutdown
!
log-adjacency-changes
router rip
 no auto-summary
 version 2
 network 172.16.0.0
!
!
!
ip http server
no ip http secure-server
!
!
!
access-list 100 deny udp any any
access-list 100 permit ip any any
access-list 100 deny tcp any any eq telnet
access-list 100 permit ip any any
!
!
!
!
control-plane
!
!
!
!
!
!
```

```
!
!
!
!
!
line con 0
  password  ciscopress
  login
line aux 0
login local ciscopress
line vty 0 4
 password ciscopress
 login
!
scheduler allocate 20000 1000
!
end
R1#
```

R2

```
R2# sh running-config
Building configuration...
Current configuration : 800 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$KXED$S08d0zG3x3aiaeFjy7nCP
!
no aaa new-model
!
resource policy
!
!
!
ip cef
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
```

```
!
!
!
!
!
!
interface FastEthernet0/0
 ip address  172.16.192.1 255.255.255.224
 ip access-group 100 in
!
interface FastEthernet0/1
 no ip address
 shutdown
!
interface Serial0/0/0
 no ip address
 shutdown
!
interface Serial0/0/1
 ip address 172.16.128.6 255.255.255.252
!
log-adjacency-changes
router rip
 no auto-summary
 version 2
 network 172.16.0.0
!
!
!
ip http server
no ip http secure-server
!
!
!
access-list 100  deny tcp 172.16.192.0 0.0.0.255 172.16.160.0 0.0.0.255 eq telnet
access-list 100  permit ip 172.16.128.0 0.0.0.255 172.16.160.0 0.0.0.255
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
!
!
line con 0
  password  ciscopress
  login
line aux 0
login local ciscopress
line vty 0 4
 password ciscopress
 login
!
scheduler allocate 20000 1000
!
end
```

R2#