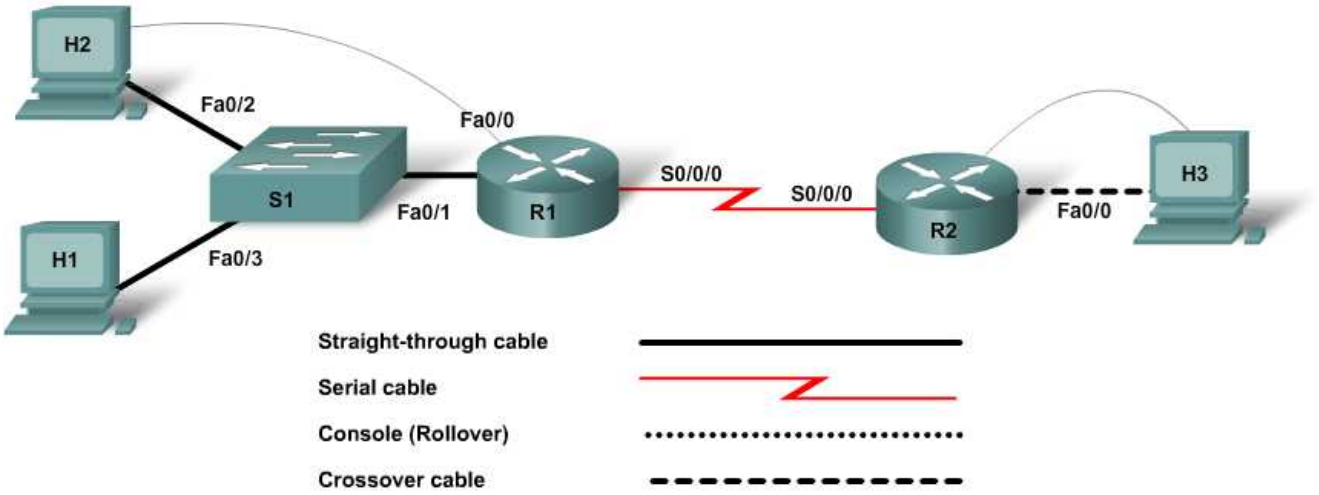
Lab 8.3.4 Planning, Configuring, and Verifying Extended ACLs



Device	Host Name	FastEthernet 0/0 IP Address	Serial 0/0/0/ IP Address	Serial 0/0/0 Interface Type	Default Gateway	Enable Secret Password	Enable, vty, and Console Password
Router 1	R1	192.168.1.1/24	192.168.15.1/30	DCE		class	cisco
Router 2	R2	192.168.5.1/24	192.168.15.2/30	DTE		class	cisco
Switch 1	S1					class	cisco
Host 1	H1	192.168.1.10/24			192.168.1.1		
Host 2	H2	192.168.1.11/24			192.168.1.1		
Host 3	H3	192.168.5.10/24			192.168.5.1		

Objectives

- Configure Extended ACLs to control traffic.
- Verify ACL operation.

Background / Preparation

In this lab you will work with Extended ACLs to control network traffic based on host IP addresses. Any router that meets the interface requirements displayed on the topology diagram may be used. For example, router series 800, 1600, 1700, 1800, 2500, 2600, 2800, or any combination can be used.

The information in this lab applies to 1841 series routers. It also apples to other routers; however, the command syntax may vary. Depending on the router model, the interfaces may differ. For example, on some routers Serial 0 may be Serial 0/0 or Serial 0/0/0 and Ethernet0 may be FastEthernet 0/0. The Cisco Catalyst 2960 switch comes preconfigured and only needs to be assigned basic security information before being connected to a network.

The following resources are required:

- One Cisco 2960 switch or other comparable switch
- Two Cisco 1841 or equivalent routers, each with a serial and an Ethernet interface
- Three Windows-based PCs, at least one with a terminal emulation program, and all set up as hosts
- At least one RJ-45-to-DB-9 connector console cable to configure the routers and switch
- Three straight-through Ethernet cables
- One crossover Ethernet cable
- One 2-part DTE/DCE serial crossover cable

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment

a. Connect the Serial 0/0/0 interface of Router 1 to the Serial 0/0/0 interface of Router 2 using a serial cable.

b. Connect the Fa0/0 interface of Router 1 to the Fa0/1 port of Switch 1 using a straight-through cable.

c. Connect a console cable to each PC to perform configurations on the routers and switch.

d. Connect Host 1 to the Fa0/3 port of Switch 1 using a straight-through cable.

e. Connect Host 2 to the Fa0/2 port of Switch 1 using a straight-through cable.

f. Connect a crossover cable between Host 3 and the Fa0/0 interface of Router 2.

Step 2: Perform basic configuration on Router 1

a. Connect a PC to the console port of the router to perform configurations using a terminal emulation program.

b. On Router 1, configure the hostname, interfaces, passwords, and message-of-the-day banner and disable DNS lookups according to the addressing table and topology diagram. Save the configuration.

Step 3: Perform basic configuration on Router 2

Perform basic configuration on Router 2 and save the configuration.

Step 4: Perform basic configuration on Switch 1

Configure Switch 1 with a hostname, console, Telnet, and privileged passwords according to the addressing table and topology diagram.

Step 5: Configure the hosts with IP address, subnet mask, and default gateway

a. Configure the hosts with IP address, subnet mask, and default gateway according to the addressing table and the topology diagram.

b. Each workstation should be able to ping the attached router. If the pings are not successful, troubleshoot as necessary. Check and verify that the workstation has been assigned a specific IP address and default gateway.

Step 6: Configure RIP routing and verify end to end connectivity in the network

a. On R1, enable the RIP routing protocol and configure it to advertise both connected networks.

b. On R2, enable the RIP routing protocol and configure it to advertise both connected networks.

c. Ping from each host to the other two hosts.

Were the pings successful? _____

If the answer is no, troubleshoot the router and host configurations to find the error. Ping again until they are all successful.

Step 7: Configure Extended ACLs to control traffic

Host 3 in this network contains proprietary information. Security requirements for this network dictate that only certain devices should be allowed access to this machine. Host 1 is the only host that will be allowed to access this computer. All other hosts on this network are used for guest access and should not be allowed access to Host 3. In addition, Host 3 is the only computer in the network that is allowed to access R1 interfaces for remote management. Extended ACLs will be used to control access on this network.

a. Itemize the list of requirements for clarity:

1) Host 1 can access Host 3. All other hosts (on that network only) cannot access Host 3. Any additional hosts added on other networks in the future should be able to access Host 3 because they will not be guest-accessible machines.

2) Host 3 can access the R1 interfaces. All other devices on the network will not have access.

b. Analyze the requirements and determine placement of Extended access control lists.

Based on the requirements, the traffic that needs to be controlled is the traffic traveling out of the R2 Fa0/0 interface and destined for Host 3. Therefore, the access control list should be placed on the R2 Fa0/0 interface.

c. Create an Extended ACL to perform the tasks stated and apply it to R2.

```
R2(config)#access-list 101 permit ip host 192.168.1.10 host
192.168.5.10
R2(config)#access-list 101 deny ip 192.168.1.0 0.0.0.255 host
192.168.5.10
R2(config)#access-list 101 permit ip any any
R2(config)#access-list 101 deny ip any any
```

NOTE: The implicit **deny** at the end of an access control list performs this same function. However, adding the line to the ACL helps document it and is considered good practice. By explicitly adding this statement, the number of packets matching the statement are tallied, and the administrator can see how many packets were denied.

d. Apply the access list on the Fa0/0 interface of R2 in the outbound direction.

```
R2(config)#interface fastethernet 0/0
R2(config-if)#ip access-group 101 out
```

e. Verify the ACL on R2 with the **show access-lists** command.

Does the output of the **show access-lists** command display the ACL that was created?

_____

Does the output of the **show access-lists** command display how the ACL is applied?

_____

f. Use the **show ip interface fa0/0** command on R2 to display the application of the ACL.

What does the output of the **show ip interface** command tell you about the ACL?

_____

Step 8: Test the ACL

a. Ping Host 3 from both Hosts 1 and 2.

Can Host 1 ping Host 3? _____

Can Host 2 ping Host 3? _____

b. To verify that other addresses can ping Host 3, ping Host 3 from R1.

Is the ping successful? _____

c. Display the access control list again with the **show access-lists** command.

What additional information is displayed beyond just the access list statements?

_____

d. Remove this access control list before continuing.

```
R2(config)#interface fastethernet 0/0
R2(config-if)#no ip access-group 101 out
R2(config-if)#exit
R2(config)#no access-list 101
```

Step 9: Configure and test the ACL for the next requirement

a. Host 3 is the only host that should be allowed to connect to R1 for remote management. Create an access control list to meet this requirement. This ACL will need to be placed on R1 because R1 is the destination of the traffic. All other hosts will not be allowed access. This is the only traffic being controlled; all other traffic should be allowed.

```
R1(config)#access-list 101 permit ip host 192.168.5.10 host
192.168.15.1
R1(config)#access-list 101 permit ip host 192.168.5.10 host 192.168.1.1
R1(config)#access-list 101 deny ip any host 192.168.15.1
R1(config)#access-list 101 deny ip any host 192.168.1.1
R1(config)#access-list 101 permit ip any any
R1(config)#access-list 101 deny ip any any
```

b. Because the source traffic could come from any direction, this ACL needs to be applied to both interfaces on R1. The traffic to be controlled would be inbound to the router.

```
R1(config)#interface fastethernet 0/0
R1(config-if)#ip access-group 101 in
R1(config-if)#interface serial 0/0/0
R1(config-if)#ip access-group 101 in
```

c. Now attempt to telnet to R1 from all hosts and R2. Attempt to telnet to both R1 addresses.

Can you telnet to R1 from any of these devices? If yes, which one(s)? _____

d. View the output of the **show access-lists** command on R1.

Does the output of the **show access-lists** command display that the statements are being matched? _____

Step 10: Reflection

a. Why is careful planning and testing of access control lists required?

_____

b. What is an advantage of using Extended ACLs over Standard ACLs?

_____