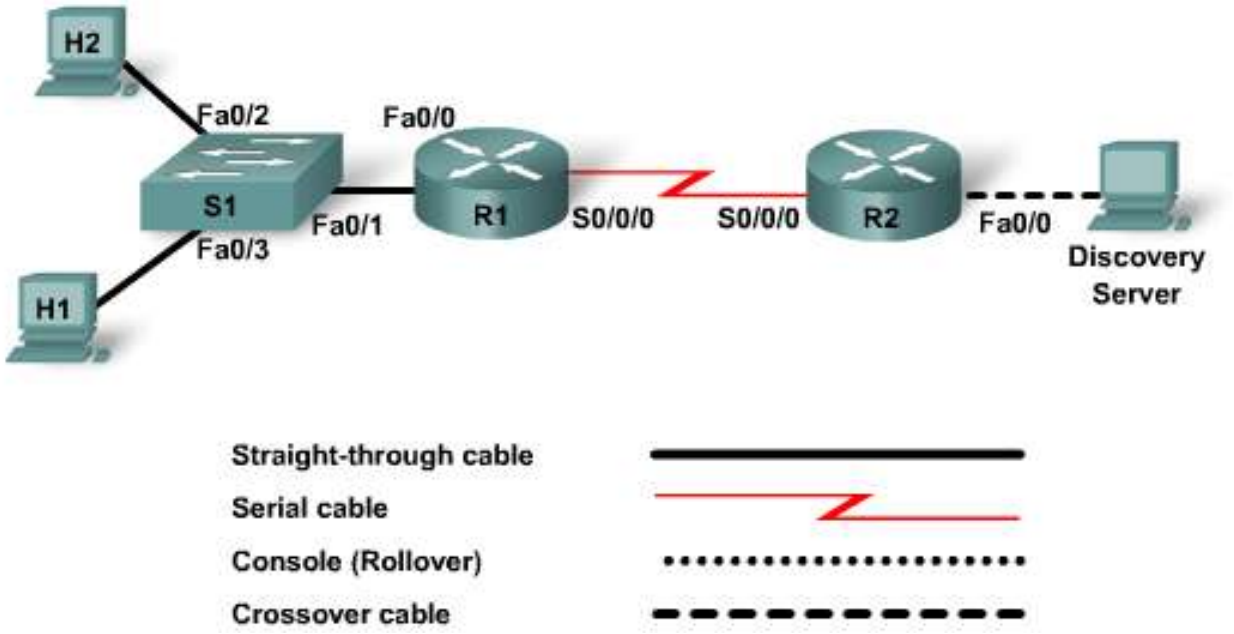
Lab 8.5.1 Configuring ACLs and Verifying with Console Logging



Device	Host Name	FastEthernet 0/0 Interface IP Address	Serial 0/0/0 IP Address	Serial 0/0/0 Interface Type	Network Statements	Enable Secret Password	Enable, vty, and Console Password
Router 1	R1	192.168.1.1/24	192.168.5.1/30	DCE	192.168.1.0 192.168. 5.0	class	cisco
Router 2	R2	172.17.0.1/16	192.168.5.2/30	DTE	192.168. 5.0 172.17.0.0	class	cisco
Switch 1	S1					class	cisco
Host 1	Host 1	192.168.1.5/24 GW=192.168.1.1					
Host 2	Host 2	192.168.1.6/24 GW=192.168.1.1					
Discovery Server	Server	172.17.1.1/16 GW=172.17.0.1					

Objectives

- Configure and verify ACLs to control traffic.
- Verify ACLs using the logging capabilities of the router.

Background / Preparation

Cable a network similar to the one shown in the topology diagram. Any router that meets the interface requirements displayed in the above diagram may be used. For example, router series 800, 1600, 1700, 1800, 2500, 2600, 2800, or any combination can be used.

The command syntax given in the lab may vary. For example, the interfaces may differ due to the router model. On some routers Serial 0 may be Serial 0/0 or Serial 0/0/0 and Ethernet 0 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, both with a Serial connection and an Ethernet interface
- Two Windows-based PCs, each with a terminal emulation program and set up as a host
- One PC to act as the Discovery Server
- One Discovery Live CD for the server
- 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 DTE/DCE serial 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.

NOTE: This lab makes use of the Discovery Server Live CD. For detailed instructions on the installation and configuration of the Discovery Server Live CD, please refer to the lab manual that is located on Academy Connection in the Tools Section.

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 on Switch 1 using a straight-through cable.

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

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

e. Connect the Discovery Server to the Fa0/0 interface of Router 2 using a crossover cable.

Step 2: Perform basic configuration on Router 1

Step 3: Perform basic configuration on Router 2

Step 4: Perform basic configuration on Switch 1

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

a. Configure each host with the proper IP address, subnet mask, and default gateway.

   1) Host 1 should be assigned 192.168.1.5 /24 and the default gateway of 192.168.1.1.

   2) Host 2 should be assigned 192.168.1.6 /24 and the default gateway of 192.168.1.1.

   3) The server should be assigned 172.17.1.1 and a default gateway of 172.17.0.1.

b. Each host should be able to ping the other hosts. If the ping is not successful, troubleshoot as necessary. Check and verify that the workstation has been assigned a specific IP address and default gateway. Do not configure ACLs until each host can ping the other hosts.

Step 6: Configure and apply ACLs

ACLs will be configured to control what services Hosts 1 and 2 can access from the server. An ACL will be created that allows Host 1 web (HTTP) and FTP access to the server but denies Host 2. Host 2 will be allowed to telnet to the server, but this service is denied to Host 1. These ACLs will be configured and verified with **show** commands and logging.

a. Create an ACL based on the requirements previously outlined. This ACL is applied to R1.

```
R1(config)#access-list 110 remark Allow Host 1 web access to server
R1(config)#access-list 110 permit tcp host 192.168.1.5 host 172.17.1.1
eq www
R1(config)#access-list 110 remark Allow Host 1 FTP access to server
R1(config)#access-list 110 permit tcp host 192.168.1.5 host 172.17.1.1
eq ftp
R1(config)#access-list 110 remark Allow Host 2 Telnet access to server
R1(config)#access-list 110 permit tcp host 192.168.1.6 host 172.17.1.1
eq telnet
R1(config)#access-list 110 remark Deny all other traffic
R1(config)#access-list 110 deny ip any any
```

b. Apply the ACL to the FastEthernet 0/0 interface on R1 in the inbound direction.

```
R1(config)#interface fastethernet 0/0
R1(config-if)#ip access-group 110 in
```

c. From Host 1, open a web browser and attempt to connect to the web and FTP services on the server. In the web browser address textbox, enter **http://172.17.1.1**.

   Is the web connection from Host 1 successful? Yes

d. In the web browser address textbox, enter **ftp://172.17.1.1**.

   Is the FTP connection from Host 1 successful? No however using Command Prompt FTP works.

e. Attempt to connect to the web and FTP services on the server from Host 2.

   Are you able to connect from Host 2? No

f. Attempt to telnet to the server from Host 1 and Host 2?

   Is the Telnet connection from Host 1 successful? No server does not have telnet services

   Is the Telnet connection from Host 2 successful? No server does not have telnet services

g. Use the command **show access-lists** to display the access control list and associated statistics.

What information can be obtained from the command output?

The attempts made for that rule

```
R1#show access-lists
Extended IP access list 110
    10 permit tcp host 192.168.1.5 host 172.17.1.1 eq www (3 matches)
    20 permit tcp host 192.168.1.5 host 172.17.1.1 eq ftp (9 matches)
    30 permit tcp host 192.168.1.6 host 172.17.1.1 eq telnet (3 matches)
    40 deny ip any any (92 matches)
```

The output of the **show access-lists** command displays the number of times each `access-list` line was matched. In many troubleshooting scenarios, however, this is not enough information. For example, the output shown above indicates that the **deny ip any any** line had 92 matches. But it does not tell you what type of traffic was sent and from what sources the traffic was denied. If there is an error in an access control list that is blocking traffic to or from a destination that the ACL was not meant to block, more information is necessary. Logging can be useful in this type of environment.

The same ACL will be configured on R1; this time, the logging option will be enabled.

NOTE: Turning on the logging option of an access control list is similar to using a **debug** command. In a production network, this option can place a heavy load on router resources and slow down the network or even cause it to fail. In a production network this feature must be used with caution.

h. Remove the ACL on R1 and recreate it with the logging option.

```
R1(config)#no access-list 110

R1(config)#access-list 110 remark Allow Host 1 web access to server
R1(config)#access-list 110 permit tcp host 192.168.1.5 host 172.17.1.1
eq www log
R1(config)#access-list 110 remark Allow Host 1 FTP access to server
R1(config)#access-list 110 permit tcp host 192.168.1.5 host 172.17.1.1
eq ftp log
R1(config)#access-list 110 remark Allow Host 2 Telnet access to server
R1(config)#access-list 110 permit tcp host 192.168.1.6 host 172.17.1.1
eq telnet log
R1(config)#access-list 110 remark Deny all other traffic
R1(config)#access-list 110 deny ip any any log
```

i. Attempt to telnet from Host 1 to the server.

After verifying that Host 1 is unable to make the connection, view the output from the console connection on R1. The output should look similar to this sample:

```
*Oct 18 01:10:57.466: %SEC-6-IPACCESSLOGP: list 110 denied tcp
192.168.1.5(1097) -> 172.17.1.1(23), 1 packet
```

The line displayed is the result of adding the **log** option to an `access-list` line. It displays a date and a time (`01:10:57.466`), the process that generated the console message (`%SEC-6-IPACCESSLOGP`), and detailed information about the message (`list 110 denied tcp 192.168.1.5(1097) -> 172.17.1.1(23), 1 packet`).

In this example, the logging option indicates that an access-list line had a match, and it also indicates the exact source and destination of the matched packet.

j. Attempt to ping as well as use Telnet, web, and FTP connections from Host 1 and Host 2 to the Discovery Server.

Is a log message created each time a connection is attempted? No not supported in Packet Tracer

Do the console messages indicate which packets are allowed by the ACL as well as those that are denied? Logging options unavailable in Packet Tracer

If you attempt connections very rapidly, a message similar to this one may appear:

```
*Oct 18 01:26:39.638: %SEC-6-IPACCESSLOGRL: access-list logging rate-
limited or missed 1 packet
```

This message indicates that the IOS sensed either that a console rate was too high or that the console was too busy to process all the packets. In this example, it indicates that it missed one packet. To avoid this situation in a production network, limit the number of `access-list` lines for which logging is enabled.

Step 7: Reflection

a. What is an advantage of using the logging option on an ACL versus the information provided by the **`show access-lists`** command?

more detailed information

b. What is a major concern of enabling the logging feature of an access control list?

Space used/memory

c. Would you normally log more than one line? Why or why not?

Depends on the specific needs of troubleshooting

d. If the network is not performing as expected (e.g. routing updates not occurring, name resolution not occurring) which ACL statement would you log? DNS