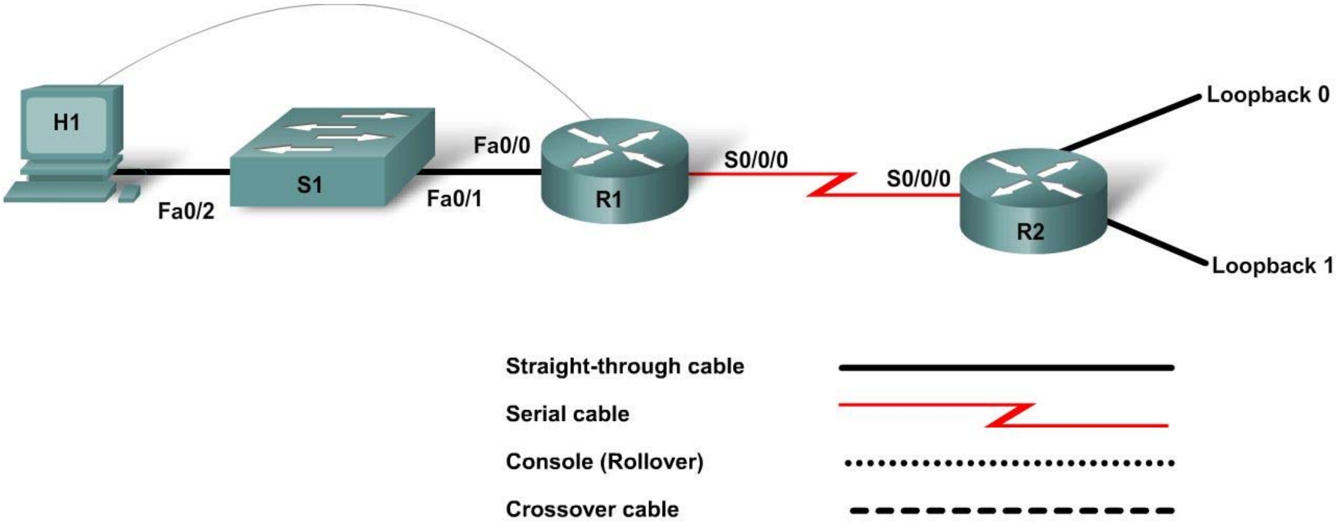
Lab 8.3.3 Configuring and Verifying Standard ACLs



Device	Host Name	FastEthernet 0/0 IP Address	Serial 0/0/0 IP Address	Serial 0/0/0 Interface Type	Loopback Interface Addresses	Enable Secret Password	Enable, vty, and Console Password
Router 1	R1	192.168.200.1/24	192.168.100.1/30	DCE	n/a	class	cisco
Router 2	R2	n/a	192.168.100.2/30	DTE	Lo0 192.168.1.1/32 Lo1 192.168.2.1/32	class	cisco
Switch 1	S1	n/a	n/a	n/a	n/a	class	cisco

Objectives

- Configure standard ACLs to limit traffic.
- Verify ACL operation.

Background / Preparation

In this lab you will work with Standard ACLs to control network traffic based on host IP addresses. Any router that meets the interface requirements displayed on the above 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 is based on the 1841 series router. Other routers may be used; however, 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 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 series routers or equivalent, each with a serial and an Ethernet interface
- One Windows-based PC with a terminal emulation program and set up as a host
- At least one RJ-45-to-DB-9 console cable to configure the routers and switch
- Two straight-through Ethernet cables
- 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 the PC to perform configurations on the routers and switch.

d. Connect H1 to the Fa0/2 port of Switch 1 using a straight-through cable.

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 and passwords according to the addressing table and topology diagram.

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

a. Configure the host with the proper IP address, subnet mask, and default gateway. The host should be assigned the address 192.168.200.10/24 and the default gateway of 192.168.200.1.

b. The workstation should be able to ping the attached router. 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.

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

a. On Router 1, enable the RIP routing protocol and configure it to advertise both connected networks.

b. On Router 2, enable the RIP routing protocol and configure it to advertise all three connected networks.

c. Ping from Host 1 to the two loopback interfaces on Router 2.

Were the pings from Host 1 successful? __________

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

Step 7: Configure and test a standard ACL

In this lab topology, the loopback interfaces on R2 simulate two Class C networks connected to the router. ACLs will be used to control access to these subnets. The loopback 0 interface will represent a network of management workstations, and the loopback 1 interface will represent a limited-access engineering network.

In this network, it is necessary to have at least one management workstation on the 192.168.200.0/24 subnet along with other user workstations. The management workstation is assigned a static IP address of 192.168.200.10. The user workstations consume the rest of the IP addresses on the network.

The ACL should allow the management workstation access to the networks attached to R2, but not allow access to these networks from the other hosts on the 192.168.200.0 network.

A Standard ACL is being used and will be placed on R2, because R2 is closest to the destination.

a. Create a Standard ACL on R2 to be used for access to the attached networks. This ACL will allow the 192.168.200.10 host access and deny all others.

```
R2(config)#access-list 1 permit 192.168.200.10
R2(config)#access-list 1 deny 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.

b. After the ACL has been created, it must be applied to an interface on the router. Use the Serial 0/0/0 interface to allow control to both the 192.168.1.0 and 192.168.2.0 networks. Potential traffic would be flowing into the interface; therefore, apply the ACL in the inbound direction.

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip access-group 1 in
```

c. Now that the ACL has been created and applied, use the **`show access-lists`** command on R2 to view the ACL.

Are there any matches for either ACL statement? __________

```
R2#show access-lists
Standard IP access list 1
    10 permit 192.168.200.10
    20 deny   any
```

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?

____

d. Use the **`show ip interface s0/0/0`** command 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. From Host 1, ping the 192.168.1.1 loopback address.

Is the ping successful? __________

b. From Host 1, ping the 192.168.2.1 loopback address.

Is the ping successful? __________

c. Issue the **`show access-list`** command again.

How many matches are there for the first ACL statement (`permit`)? __________

```
R2#show access-lists
Standard IP access list 1
    permit 192.168.200.10 (16 matches)
    deny   any
```

How many matches are there for the second ACL statement (`deny`)? __________

d. View the routing table on R2 using the **`show ip route command`**.

What route is missing from the routing table? ____

The route is missing from the routing table because the ACL only permits packets from 192.168.200.10. RIP update packets from R1 are sourced from the router Serial 0/0/0 interface 192.168.100.1 and are denied by the ACL. Because R1 RIP updates advertising the 192.168.200.0 network are blocked by the ACL, R2 has no knowledge of the 192.168.200.0 network. The pings that were done earlier were not blocked by the ACL. They failed because R2 could not return the echo reply; R2 did not know how to get to the 192.168.200.0 network.

This example shows why ACLs must be programmed carefully and tested thoroughly for functionality.

e. Recreate the ACL on R2 to allow for routing updates to be received from R1.

```
R2(config)#no access-list 1
R2(config)#access-list 1 permit 192.168.200.10
R2(config)#access-list 1 permit 192.168.100.1
R2(config)#access-list 1 deny any
```

f. Ping 192.168.1.1 and 192.168.2.1 from Host 1.

Are the pings now successful? ___________

g. Change the IP address on Host 1 to 192.168.200.11.

h. Again ping 192.168.1.1 and 192.168.2.1 from Host 1.

Are the pings successful? __________

Display the ACL again using the **`show access-lists`** command.

Are there matches for the 192.168.100.1 ACL statement? __________

NOTE: You can clear the ACL counters using the **`clear ip access-list counters`** command from the privileged EXEC prompt.

Step 9: Reflection

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

____

b. What is the main limitation of standard ACLs?

____