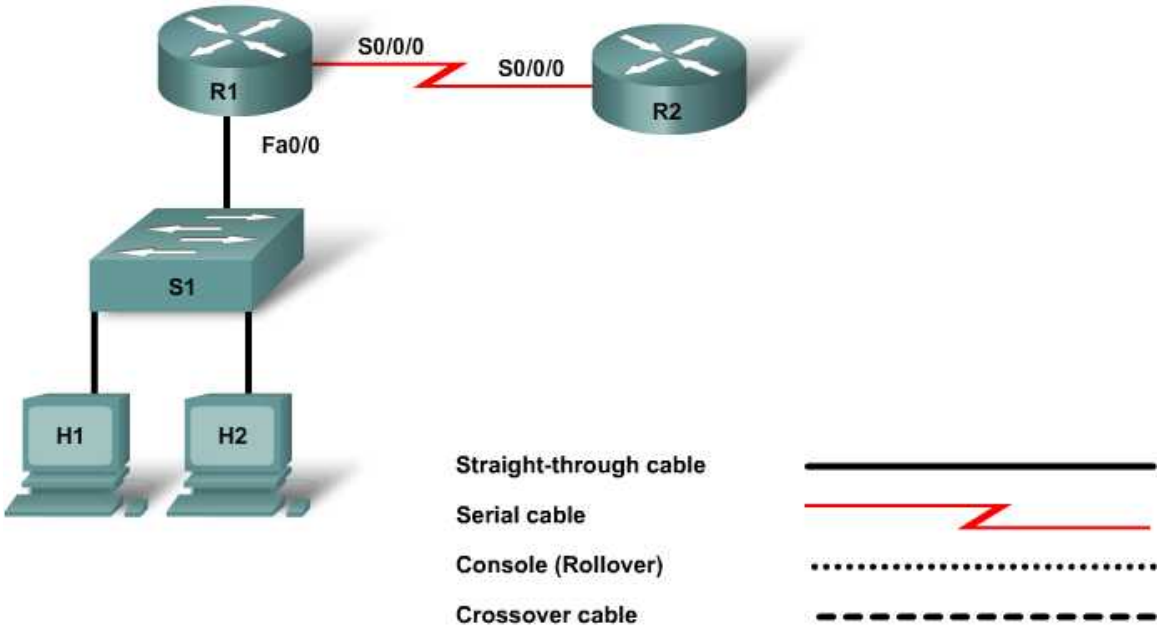
Lab 8.3.5 Configuring and Verifying Extended Named ACLs



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	192.168.15.1/24	209.165.201.1/30	DTE		class	cisco
Router 2	R2		209.165.201.2/30	DCE		class	cisco
Switch 1	S1					class	cisco
Host 1	H1	192.168.15.2/24			192.168.15.1		
Host 2	H2	192.168.15.3/24			192.168.15.1		

Objectives

- Create Standard and Extended Named ACLs.
- Test the ACLs to determine whether they achieve the desired results.
- Edit a Named ACL.

Background / Preparation

In this lab you will work with Named Standard and 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 routers. Other routers may be used; 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 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 comparable routers, each with a serial connection and an Ethernet interface
- Two Windows-based PCs, both with a terminal emulation program, and both 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 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 as shown in the diagram and addressing table.

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

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

d. Connect Host 2 to the Fa0/3 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

a. Perform basic configuration on Router 2 according to the addressing table and topology table. Save the configuration.

Step 4: Perform basic configuration on Switch 1

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

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

a. Configure the hosts IP address, subnet mask, and default gateway according to the addressing table and the topology diagram.
b. Each workstation should be able to ping R1 and each other. 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: Verify that the network is functioning

a. From the attached hosts, ping the FastEthernet interface of the default gateway router.

   Was the ping from Host 1 successful? _____

   Was the ping from Host 2 successful? _____

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

b. Use the command **`show ip interface brief`** and check the status of each interface.

   What is the state of the interfaces on each router?

   R1:

   FastEthernet 0/0: _____

   Serial 0/0/0: _____

   Serial 0/0/1: _____

   R2:

   FastEthernet 0/0: _____

   Serial 0/0/0: _____

   Serial 0/0/1: _____

c. Ping from the Serial 0/0/0 interface of Router 1 to the Serial 0/0/0 interface of Router 2.

   Was the ping successful? _____

   If the answer is no, troubleshoot the router configurations to find the error. Ping again until successful.

Step 7: Configure static and default routing on the routers.

a. Configure a default route on R1. Use the next hop interface on R2 as the path.

   ```
   R1(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.2
   ```

b. From one of the host PCs on R1, ping R2.

   Why is the ping unsuccessful?

   _____

c. Configure a static route on R2 to the R1 192.168.15.0 network. Use the next hop interface on R1 as the path.

   ```
   R2(config)#ip route 192.168.15.0 255.255.255.0 209.165.201.1
   ```

d. From one of the host PCs on R1, ping R2.

   Did the ping succeed? _____

   If the ping did not succeed, troubleshoot the static and default routes.

Step 8: Configure and test a simple Named Standard ACL

a. Create a Named ACL that allows H2 to reach other hosts on the local network but does not allow H2 to access remote networks. At the configuration prompt, use this command sequence:

```
R1(config)#ip access-list standard H2_no_access
R1(config-std-nacl)#deny host 192.168.15.3
R1(config-std-nacl)#permit any
```

Why do you need the third statement? _____

b. Apply the ACL to the interface.

```
R1(config)#interface fastethernet0/0
R1(config-if)#ip access-group H2_no_access in
```

Describe how you should test this ACL: _____

_____

c. Conduct the tests to verify that this ACL achieves its goals. If it does not, troubleshoot by viewing the output of a **show running-config** command to verify that the ACL is present and applied to the correct interface.

Step 9: Create and test a Named Extended ACL

a. Create a Named ACL that does not allow H1 to ping R2 but allows H1 to reach the local network and R1.

```
R1(config)#ip access-list extended H1_limit_access
R1(config-ext-nacl)#deny ip host 198.168.15.2 host 209.165.201.2
R1(config-ext-nacl)#permit ip any any
```

b. Apply the ACL to the interface.

```
R1(config)#interface s0/0/0
R1(config-if)#ip access-group H1_limit_access out
```

Describe how you would test this ACL: _____

_____

c. Conduct the tests to verify that this ACL achieves its goals. If it does not, troubleshoot by viewing the output of a **show running-config** command to verify that the ACL is present and applied to the correct interface.

Step 10: Edit a Named Standard ACL

a. You have decided to edit the Named Standard ACL. In privileged EXEC mode, view the access list statements.

```
R1#show access-lists
Standard IP access list H2_no_access
    10 deny host 192.168.15.3
    20 permit any
```

b. Add a line to this Named Standard ACL to block H1 from reaching R1, but still permit H1 and H2 to reach each other.

Enter configuration commands, one per line. End with **CNTL/Z**.

```
R1(config)#ip access-list standard H2_no_access
R1(config-std-nacl)#15 deny host 192.168.15.2
```

c. View the edited ACL to verify that all statements are present.

```
R1#show access-lists
```

```
Standard IP access list H2_no_access
    10 deny host 192.168.15.3
    15 deny host 192.168.15.2
    20 permit any
```

If you added a new PC to the topology, attached it to S1, and gave it the IP address 192.168.15.4/24, would it be able to reach R1? _____

Step 11: Reflection

a. Why is it good practice to perform basic configurations and verify connectivity before adding ACLs to routers?

_____

_____

b. What advantages do Named ACLs offer?

_____

_____