Lab 6.3.6 Standard ACLs - Overview

Estimated time: 60 min.

Objectives:

This Lab will focus on your ability to accomplish the following tasks:

- Review the characteristics and capabilities of standard IP Access Control Lists (ACLs)
- Construct a standard ACL to permit or deny specific traffic
- Apply a standard IP ACL to a router interface
- Test the ACL to determine if the desired results were achieved
- Remove an ACL from a router interface
- Delete an ACL from a router

Background:

In this lab you will work with Standard Access Control Lists (ACLs) to regulate the traffic that is allowed to pass through a router based on the source, either a specific host (typically a workstation or server) or an entire network (any host or server on that network). A Standard ACL is a simple and effective tool to control which packets should be allowed to pass through a router from one network to another. Standard ACLs are a basic form of control with limited capabilities. They can filter (permit or deny) packets coming into or going out of a router interface based only on the IP address of the source network or host. As a result, they should be applied near the destination address since you cannot specify the destination address.

Other routed (or routable) protocols such as IPX or AppleTalk can also have ACLs or filters but this lab will focus on IP ACLs. When a standard IP ACL is applied, it will filter (permit or deny) the entire IP protocol suite (IP, TCP, SMTP, HTTP, Telnet etc.). When creating Standard IP ACLs they are numbered from 1 to 99. In the next lab you will work with Extended IP ACLs which are numbered from 100 to 199. Refer to the text or online lesson for IPX and AppleTalk ACL numbering.

These are the steps necessary to use ACLs effectively:

- Determine the ACL requirements (based on security needs etc.)
- Construct the ACL
- Verify the statements in the ACL
- Apply the ACL to a router interface
- Verify that the ACL is applied correctly to the intended interface
- Verify that the ACL is functioning properly

Tools / Preparation:

Prior to starting the lab, the teacher or lab assistant should have the standard router lab with all 5 routers set up. Work individually or in teams. Before beginning this lab you

should read the Networking Academy Second Year Companion Guide, Chapter 6 - ACLs. You should also review semester 3 On-line Chapter 6. The following is a list of equipment required.

- Standard Cisco 5-router lab setup with hubs and switches
- Workstation connected to the router's console port with a rollover cable

Web Site Resources

LAN Switching basics
General information on all Cisco products - (Scroll down to chapter 15 - Switches)
1900 / 2820 series Ethernet switches
2900 series Fast Ethernet switches
Terms and acronyms
IP routing protocol IOS command summary
Access Control Lists - Overview and Guidelines

Notes:

_____

_____

_____

_____

_____

In this lab you will construct, apply and test a standard IP ACL. Exercise A is required and B is optional but recommended. Exercise A is intended to block packets from a specific host on one network from getting to any host on another network. Exercise B will block traffic from all hosts on a specific network from getting to any host on an entire network. Answers are provided for both exercises. Refer to the standard lab diagram in the overview section.

Exercise A (required).
ACL 1 prevents IP traffic from a specific host (workstation with 192.5.5.2 IP address) attached to the Ethernet hub off Router LAB-A interface E0, from reaching an entire network (210.93.105.0, the network between Routers LAB-D & LAB-E)

Exercise B (optional)
ACL 2 prevents IP traffic from all hosts on a specific network 219.17.100.0 (an Ethernet network off Router LAB-B) from reaching an entire network 223.8.151.0 (an Ethernet network off router LAB-C)

Step 1 - Determine the ACL requirements.

Which traffic (packets) from which hosts or networks will be blocked (denied) or allowed (permitted)? Since you will use a standard IP ACL, you can only filter on the source address. With exercise A, you wish to block traffic from host address 192.5.5.2 from an Ethernet on Router LAB-A. With exercise B, you wish to block traffic from network address 219.17.100.0 on Router LAB-B.

Step 2 - Construct the ACL.

Define the ACL statements in Router(config)# mode. ACL statements are additive. Each statement adds to the ACL. If there is more than one statement in the ACL (typical) and you want to change a prior statement you must delete the ACL and start again. In these examples you are blocking packets from only one host IP address or one network. The format or syntax of the standard IP ACL statement is shown below:

access-list list# {permit / deny} source IP address [wildcard mask] [log]

NOTE:

(Any number between 1 and 99 can be used for a standard IP ACL. To delete the ACL, repeat the access-list # portion of the command with the word NO in front.)

Complete the ACL command with the correct source address and wildcard mask that would accomplish the requirements for either exercise A or B (or both). The first statement would be used for ACL 1. The second statement would be used for ACL 2.

Exercise A. access-list 1 deny _____

Exercise B. access-list 2 deny _____

1. What is the purpose of a Zero (0) in a wildcard mask?

_____

2. How many bits does each decimal zero in the wildcard mask above represent?

_____

3. What is the purpose of a 255 in a wildcard mask ?

_____

4. How many bits does the 255 represent?

_____

5. Since ACLs always end with an implicit "deny any", using just one of the statements above would cause this list to deny a single source address, but then implicitly deny any

other source address too. Our objective is to only deny access from a single host, so you need to add a second statement to allow all other traffic. Enter the second ACL statement that would allow all other traffic (the same statement would be used for exercise A or B:

_____

6. Why are both statements using the same ACL number (1) ?

_____

7. What would be happen if the 1st statement was "Access-list 1" and the 2nd "Access-list 2"?

_____

Step 3 - Verify the statements in the ACL.

Use the following command to check your statements and verify that everything was typed in correctly. If you want to correct a mistake or make a change to an existing statement you must delete the ACL and start again. To delete the ACL, repeat the access-list # portion of the command with the word NO in front.

```
Router#show access-list 1
```

1. How many statements are in your ACL?

_____

Step 4 - Apply the ACL to a router interface.

Since standard ACLs can only specify or check source addresses, you must apply the filter as close to the destination as possible. On which router and which interface would you apply the ACL for each of the sample exercises A or B? Refer to the standard lab diagram and fill in the following table with the IP address(es) to be blocked, the network you wish to keep them out of, the router where the ACL will be applied, the interface it will be applied to and whether it will block INcoming or OUTgoing

Exercise	IP host or network to be Denied (blocked)	Network to keep packets out of	Router where ACL will be applied	Interface where ACL will be applied (S0, S1, E0, etc)	Block Incoming or Outgoing? (IN or OUT)
A (ACL 1)					
B (ACL 2)					

NOTE:

Remember to put Standard ACLs close to the destination

Enter the following commands to apply ACL 1 to interface S1 to block incoming packets on interface S1 for router LAB-D. The real router name (e.g. LAB-D), would appear instead of "Router" in the prompt. For ACL 2, the ACL would be applied to interface E0 on LAB-C for outgoing packets.

```
Router(config)#interface Serial 1
Router(config-if)#ip access-group 1 in
```

Step 5 - Verify the ACL is Applied Correctly to the Intended Interface.

Use the following command to check to see that the ACL is applied to the correct interface on the correct router:

```
Router#show running-config
```

1. What results were displayed that proves that the ACL is applied correctly?

NOTE:

To remove an ACL from an interface, first configure the interface as with step 4 and then repeat the second command with the word NO in front (no ip access-group 1).

Step 6 - Verify that the ACL is functioning properly.

Test the ACL by trying to send packets from the source network that is to be permitted or denied. Issue several ping commands to test these ACLs. Several tests are given for each exercise.

Exercise	Test#	Ping from	To	Should be successful?	Was it
A	1	Workstation (192.5.5.2) off router LAB-A	Workstation (210.93.105.2) offrouter LAB-E		
	2	Workstation (192.5.5.2) off router LAB-A	Router LAB-C Interface S0 (204.204.7.1)		
B	1	Workstation (219.17.100.X) off Router LAB-B	Router LAB-E Interface E0 (210.93.105.2) or workstation (210.93.105.X)		
	2	Workstation (219.17.100.X) off Router LAB-B	Router LAB-C Interface E0 (223.8.151.1)		

	3	Workstation (219.17.100.X) off Router LAB-B	Workstation (223.8.151.2) off router LAB-C		