Lab 6.8.1.1 Extended 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 extended IP Access Control Lists (ACLs)
- Construct an extended IP ACL to permit or deny specific traffic
- Apply an extended IP ACL to a router interface
- Test the ACL to determine if the desired results were achieved

Background:

Extended ACLs are a more advanced form of control with more flexibility in the way packets are controlled. Extended ACLs can filter (permit or deny) packets based on source or destination address and on the type of traffic (e.g. FTP, Telnet, HTTP etc.). Since extended ACLs can block traffic based on destination address, they can be placed near the source which helps to reduce network traffic.

In this lab you will work with Extended ACLs to regulate the traffic that is allowed to pass through the router based on the source and type of traffic. ACLs are an important tool to control which packets and what type of packets should be allowed to pass through a router from one network to another.

There are different types of ACLs for different routed protocols such as IP, Novell IPX and AppleTalk. With this lab, you will work only with Extended IP ACLs which are created with a number from 100 to 199.

These are the steps necessary to use ACLs effectively:

1. Determine the ACL requirements (based on company security needs etc.)
2. Construct the ACL.
3. Verify the statements in the ACL
4. Apply the ACL to a router interface.
5. Verify that the ACL is applied correctly to the intended interface.
6. 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 an extended IP ACL using the following standard lab setup. You may do either Exercise A or exercise B outlined in Step 1 below.

Step 1 - Determine the ACL Requirements.

Which traffic (packets) will be blocked (denied) or allowed (permitted)? Since you will use an extended IP ACL, you can control not only the source address but also the destination address. You can also pick and choose the specific protocols in the IP protocol suite that you want to allow or prevent from entering the destination network (e.g. TCP. UDP, ICMP, HTTP, Telnet etc.).

Exercise A: Prevent **`Telnet`** traffic from a specific host 192.5.5.2 (a workstation off router LAB-A) from reaching an entire network 210.93.105.0 (the network between Routers LAB-D & LAB-E)

Exercise B: Prevent **`Telnet`** traffic from a specific host 210.93.105.2 (a workstation off router LAB-E) from reaching an entire network 192.5.5.0 (off Router LAB-A).

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 prior statement you must delete the ACL and start again. In

these examples you will be blocking packets from only one host IP address or one network based on the destination network and higher level IP protocol (e.g. telnet) being used. The format or syntax of the extended IP ACL statements that you will be using shown below:

```
access-list list# {permit/deny} [protocol] source IP
wildcard mask [port] dest. IP wildcard mask [port]
[established] [log] [other options]
```

NOTE:

Any number from 100 and 199 can be used for an extended IP ACL)

Complete the ACL command with the correct source and destination address that would accomplish the requirements for either exercise A or B (or both). With extended access-lists, you must also specify the protocol (IP, TCP, UDP, ICMP). Since you are filtering telnet, which uses TCP, remember to include TCP in the command.

Exercise A (ACL 101)
access-list 101 deny

_____

Exercise B (ACL 102)
access-list 102 deny

_____

1. Why is the source wildcard mask given as 0.0.0.0?

_____

2. Why is the destination wildcard mask given as 0.0.0.255?

_____

3. What are you checking with the "eq telnet"?

_____

4. What would it mean if you left off the eq telnet?

_____

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 to 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):

_____

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 101
```

1. How many statements are in your ACL?

_____

Step 4 - Apply the ACL to a Router Interface.

Because you are now using extended ACLs and can filter on both the source and destination address, you can apply the filter as close to the source as possible, saving on bandwidth. Also remember you can decide to apply the ACL to incoming packets or outgoing packets. Unless IN is specified the ACL will be applied to OUT packets only (IN and OUT are always viewed from outside the router). Which router and which interface would you apply the ACL for each of the sample exercises A or B? Refer to the extended lab diagram and answer the following questions.

Exercise A.

1. On which router, LAB-B or LAB-D, would you apply the filter that would prevent router LAB-A's telnet packets from being transmitted to the D/E LAN (network 210.93.105.0)?

_____

2. On which interface would this list be applied?

_____

3. Complete the commands that would apply this list to that interface:

```
Router(config)#
```

_____

```
Router(config-if)#
```

_____

Exercise B.

1. On which router, lab-b or lab-d, would you apply the filter that would prevent router LAB-E's packets from being transmitted to the A LAN (network 201.100.11.0)?

_____

2. On which interface would this list be applied?

3. Complete the commands that would apply this list to that interface:

```
Router(config)#
```

```
Router(config-if)#
```

Step 5 - Verify the ACL is Applied to the Correct 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 101 in).

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 #	Telnet from	To	Should be successful?	Was it?
A	1	Workstation (192.5.5.2) off router Lab-A	Workstation (210.93.105.2) offrouter Lan-E		
	2	Workstation (192.5.5.2) off router Lab-A	Workstation (223.8.151.2) offrouter Lab-C		
Exercise	**Test #**	**Telnet from**	**To**	**Should be successful?**	**Was it?**
B	1	Workstation (210.93.105.2) offrouter Lab-E	Workstation (192.5.5.2) off router Lab-A		
	2	Workstation (210.93.105.2) off router Lab-	Workstation (219.17.100.2) offrouter Lab-B		

		E			

Use the following command with one of the routers where the ACL was applied to verify that packets are being blocked:

```
Router#show access-list 101
```

1. What was the result of the command? How could you tell the ACL was working?