Lab ID: 10.215A266.SUP1.1

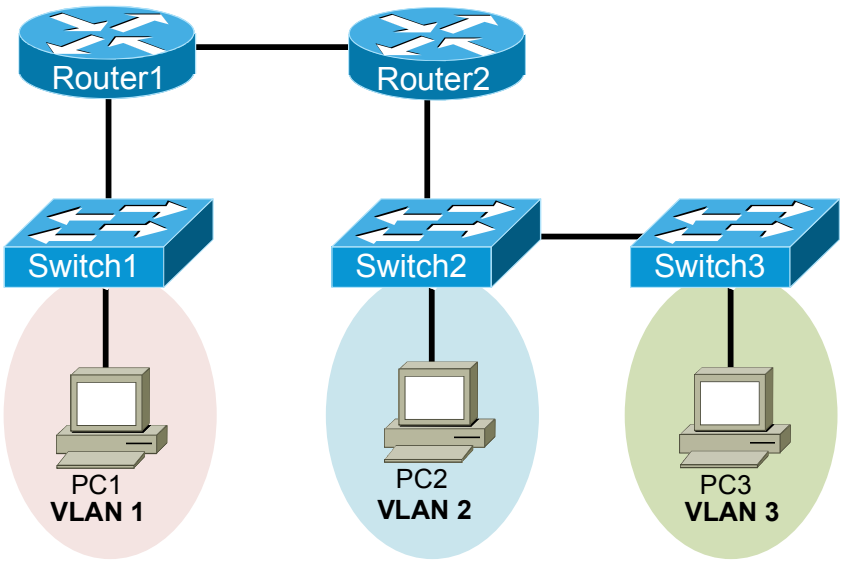
Supplemental Lab: ACL Practice Lab 3: Extended ACLs

Objective

Practice configuring extended access control lists (ACLs) on Cisco routers. Verify the ACLs by using **show** commands and network connectivity tests.

Lab Topology

The topology diagram below represents the NetMap in the Simulator.



Command Summary

Command	Description
access-list *access-list-number* {**deny** | **permit**} *protocol source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]]	defines an extended IP ACL for the traffic type specified by the protocol parameter
configure terminal	enters global configuration mode from privileged EXEC mode
enable	enters privileged EXEC mode
end	ends and exits configuration mode
exit	exits one level in the menu structure
interface *type number*	changes from global configuration mode to interface configuration mode
ip access-group {*access-list-number* | *access-list-name*} {**in** | **out**}	controls access to an interface

Command	Description
ping *ip-address*	sends an Internet Control Message Protocol (ICMP) echo request to the specified address
show running-config	displays the active configuration file
telnet *ip-address*	starts the terminal emulation program from a PC, router, or switch; permits you to access devices remotely over the network

The IP addresses and subnet masks used in this lab are shown in the tables below:

IP Addresses

Device	Interface	IP Address	Subnet Mask
Router1	FastEthernet 0/0	192.168.51.49	255.255.255.252
	FastEthernet 1/0	10.10.1.1	255.255.255.0
	Loopback 0	1.1.1.1	255.255.255.255
Router2	FastEthernet 0/0	192.168.51.50	255.255.255.252
	FastEthernet 1/0.2	10.10.2.1	255.255.255.0
	FastEthernet 1/0.3	10.10.3.1	255.255.255.0
	Loopback 0	2.2.2.2	255.255.255.255

Device	IP Address	Subnet Mask	Default Gateway
PC1	10.10.1.101	255.255.255.0	10.10.1.1
PC2	10.10.2.102	255.255.255.0	10.10.2.1
PC3	10.10.3.103	255.255.255.0	10.10.3.1

Lab Tasks

Task 1: Practice Configuring Extended ACLs

In this task, you will configure multiple extended ACLs to permit and deny traffic from various protocols and sources across the topology. You should use extended ACL best practices wherever possible. When all tasks are complete, each PC should remain able to ping the address of the Loopback 0 interface on each router. Pings to other destinations should succeed or fail per the instructions below. All passwords in this lab are configured to **boson**.

1. From each PC, verify that you can ping the Loopback 0 interfaces of both Router1 (1.1.1.1) and Router2 (2.2.2.2). The pings should succeed.

2. From each PC, verify that you can ping every other PC in the topology. The pings should succeed.

   PC1: 10.10.1.101
   PC2: 10.10.2.102
   PC3: 10.10.3.103

3. From PC1, verify that you can telnet to Router2's Loopback 0 interface (2.2.2.2).

4. From PC2, verify that you can telnet to Router1's Loopback 0 interface (1.1.1.1).

5. From PC3, verify that you can telnet to Router1's Loopback 0 interface (1.1.1.1).

6. On the appropriate device, create extended ACL **101**. The ACL should permit Telnet traffic from PC2 and PC3 to Router1's Loopback 0 interface (1.1.1.1). Limit the ACL you create to a single rule. Specify the port number, the source wildcard mask, and the destination wildcard mask in the command syntax.

7. On the appropriate device, apply extended ACL 101 to the correct interface in the correct direction.

8. On the appropriate device, create extended ACL **102**. The ACL should permit Telnet traffic from PC1 to Router2's Loopback 0 interface (2.2.2.2). Specify the port number, the source wildcard mask, and the destination wildcard mask in the command syntax.

9. On the appropriate device, apply extended ACL 102 to the correct interface in the correct direction.

10. From PC1, verify that you can telnet to Router2's Loopback 0 interface (2.2.2.2).

11. From PC1, attempt to ping Router2's Loopback 0 interface (2.2.2.2). The pings should fail.

12. From PC2 and PC3, verify that you can telnet to Router1's Loopback 0 interface (1.1.1.1).

13. From PC2 and PC3, attempt to ping Router1's Loopback 0 interface (1.1.1.1). The pings should fail.

14. From PC2, attempt to ping PC3 (10.10.3.103). The ping should succeed.

15. On the appropriate device, edit extended ACL 101 to permit ICMP traffic from Router2 to any network connected to Router1.

16. On the appropriate device, edit extended ACL 102 to permit ICMP traffic from Router1 to any network connected to Router2.

17. From PC1, ping Router2's Loopback 0 interface (2.2.2.2). The ping should succeed.

18. From PC2 and PC3, attempt to ping Router1's Loopback 0 interface (1.1.1.1). The pings should succeed.

Lab Solutions

Task 1: Practice Configuring Extended ACLs

All passwords in this lab are configured to **boson**.

1. Pings from each PC to the Loopback 0 interfaces of Router1 (1.1.1.1) and Router2 (2.2.2.2) should succeed.

2. Pings from each PC to PC1 (10.10.1.101), PC2 (10.10.2.102), and PC3 (10.10.3.103) should succeed.

3. From PC1, you should issue the following commands to verify that you can telnet to Router2's Loopback 0 interface (2.2.2.2):

```
C:>telnet 2.2.2.2
Password:boson
Router2>exit
```

4. From PC2, you should issue the following commands to verify that you can telnet to Router1's Loopback 0 interface (1.1.1.1):

```
C:>telnet 1.1.1.1
Password:boson
Router1>exit
```

5. From PC3, you should issue the following commands to verify that you can telnet to Router1's Loopback 0 interface (1.1.1.1):

```
C:>telnet 1.1.1.1
Password:boson
Router1>exit
```

6. On Router2, you should issue the following commands, including the port number, source wildcard mask, and destination wildcard mask, to create extended ACL **101** and configure it to permit Telnet traffic from PC2 and PC3 to Router1's Loopback 0 interface (1.1.1.1):

```
Router2>enable
Router2#configure terminal
Router2(config)#access-list 101 permit tcp 10.10.2.0 0.0.1.255 1.1.1.1 0.0.0.0 eq 23
```

This command configures extended ACL 101 to permit TCP connections matching the Telnet port, which is port number 23, as long as those connections come from the 10.10.2.0/23 network. The /23 network includes the range of IP addresses from 10.10.2.0 through 10.10.3.255; it is equivalent to a subnet mask of 255.255.254.0. To limit ACL 101 to a single rule, you therefore need to use a source network address of 10.10.2.0 and a source wildcard mask of 0.0.1.255, which is the inverse of the subnet mask 255.255.254.0.

7. On Router2, you should issue the following commands to apply extended ACL 101 to the FastEthernet 0/0 interface in the outbound direction:

```
Router2(config)#interface fastethernet 0/0
Router2(config-if)#ip access-group 101 out
```

Unlike standard ACLs, extended ACLs should be applied as close to the source of the traffic as possible. In this case, the single ACL 101 is configured to match traffic from multiple sources. Therefore, the single interface closest to the source of the traffic is Router2's FastEthernet 0/0 interface, which is directly connected to Router1. Because the Telnet traffic from PC2 and PC3 will have already been processed by Router2 when the traffic reaches the FastEthernet 0/0 interface, you should apply the ACL in the outbound direction.

8. On Router1, you should issue the following commands, including the port number, the source wildcard mask, and the destination wildcard mask, to create extended ACL **102** and configure the ACL to permit Telnet traffic from PC1 to Router2's Loopback 0 interface (2.2.2.2):

```
Router1>enable
Router1#configure terminal
Router1(config)#access-list 102 permit tcp 10.10.1.0 0.0.0.255 2.2.2.2 0.0.0.0 eq 23
```

9. On Router1, you should issue the following commands to apply extended ACL 102 to the FastEthernet 0/0 interface in the outbound direction:

```
Router1(config)#interface fastethernet 0/0
Router1(config-if)#ip access-group 102 out
```

10. From PC1, you should issue the following commands to verify that you can telnet to Router2's Loopback 0 interface (2.2.2.2):

```
C:>telnet 2.2.2.2
Password:boson
Router2>exit
```

11. From PC1, a ping to Router2's Loopback 0 interface (2.2.2.2) should fail.

12. From PC2 and PC3, you should issue the following commands to verify that you can telnet to Router1's Loopback 0 interface (1.1.1.1):

```
C:>telnet 1.1.1.1
Password:boson
Router1>exit
```

13. From PC2 and PC3, a ping to Router1's Loopback 0 interface (1.1.1.1) should fail.

14. From PC2, a ping to PC3 (10.10.3.103) should succeed because there are no ACLs configured that would block ICMP traffic between PC2 and PC3 through Router2.

15. On Router2, you should issue the following commands to edit extended ACL 101 to permit ICMP traffic from Router2 to any network connected to Router1:

```
Router2>enable
Router2#configure terminal
Router2(config)#access-list 101 permit icmp any any
```

16. On Router1, you should issue the following commands to edit extended ACL 102 to permit ICMP traffic from Router1 to any network connected to Router2:

```
Router1>enable
Router1#configure terminal
Router1(config)#access-list 102 permit icmp any any
```

17. From PC1, a ping to Router2's Loopback 0 interface (2.2.2.2) should succeed.

18. From PC2 and PC3, a ping to Router1's Loopback 0 interface (1.1.1.1) should succeed.

Sample Configuration Scripts

Router1

```
Router1#show running-config
Building configuration...
Current configuration : 952 bytes
!
Version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router1
!
ip subnet-zero
!
ip cef
no ip domain-lookup
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
 no ip directed broadcast
!
interface FastEthernet0/0
 ip address 192.168.51.49 255.255.255.252
 no ip directed-broadcast
 ip access-group 102 out
!
interface FastEthernet1/0
 ip address 10.10.1.1 255.255.255.0
 no ip directed-broadcast
!
router ospf 100
 log-adjacency-changes
 network 1.1.1.1 0.0.0.0 area 0
 network 10.10.1.0 0.0.0.255 area 0
 network 192.168.51.48 0.0.0.3 area 0
!
ip classless
no ip http server
!
access-list 102 permit tcp 10.10.1.0 0.0.0.255 host 2.2.2.2 eq 23
access-list 102 permit icmp any any
!
line con 0
line aux 0
line vty 0 4
 login
 password boson
!
no scheduler allocate
end
```

Router2

```
Router2#show running-config
Building configuration...
Current configuration : 1157 bytes
!
Version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router2
!
ip subnet-zero
!
ip cef
no ip domain-lookup
!
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
 no ip directed broadcast
!
interface FastEthernet0/0
 ip address 192.168.51.50 255.255.255.252
 no ip directed-broadcast
 ip access-group 101 out
!
interface FastEthernet1/0
 no ip address
 no ip directed-broadcast
!
interface FastEthernet1/0.2
 encapsulation dot1q 2
 ip address 10.10.2.1 255.255.255.0
!
interface FastEthernet1/0.3
 encapsulation dot1q 3
 ip address 10.10.3.1 255.255.255.0
!
router ospf 100
 log-adjacency-changes
 network 2.2.2.2 0.0.0.0 area 0
 network 10.10.2.0 0.0.0.255 area 0
 network 10.10.3.0 0.0.0.255 area 0
 network 192.168.51.48 0.0.0.3 area 0
!
ip classless
no ip http server
!
access-list 101 permit tcp 10.10.2.0 0.0.1.255 host 1.1.1.1 eq 23
access-list 101 permit icmp any any
!
line con 0
line aux 0
line vty 0 4
 login
 password boson
!
no scheduler allocate
end
```