Lab ID: 10.215A265.SUP1.1

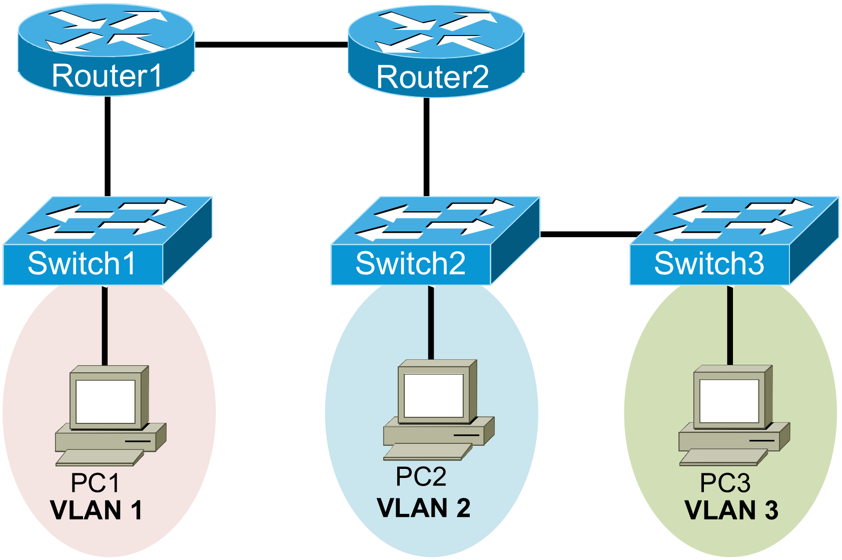
Supplemental Lab: ACL Practice Lab 2: Standard ACLs

Objective

Practice configuring standard 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**} *source-address source-wildcard*	creates an ACL that denies or permits IP traffic from the specified address or address range
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 access-lists [*access-list-number* | *access-list-name*]	displays the contents of current ACLs
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 Standard ACLs

In this task, you will configure multiple standard ACLs to permit and deny traffic from various sources across the topology. You should use standard ACL best practices wherever possible. You will not be able to configure Router2 in this lab. Therefore, any ACLs you implement should be configured on Router1. The virtual terminal (vty) line passwords on Router1 and Router2 are configured as **boson**.

1. From each PC, verify that you can ping the Loopback 0 interface addresses of Router1 (1.1.1.1) and Router2 (2.2.2.2).

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

   PC1: 10.10.1.101
   PC2: 10.10.2.102
   PC3: 10.10.3.103

3. From each PC, verify that you can telnet to Router1's Loopback 0 interface (1.1.1.1).

4. Create standard ACL **1**, and configure it to deny traffic from virtual LAN (VLAN) 2 (10.10.2.0/24) and VLAN 3 (10.10.3.0/24). All other traffic sources from Router2 should be permitted. Use no more than two rules when configuring ACL 1.

5. Apply standard ACL 1 to the correct interface and in a direction that will prevent traffic from VLAN 2 and VLAN 3 from accessing any of the networks on Router1.

6. From each PC, attempt to telnet to Router1's Loopback 0 interface (1.1.1.1). Only PC1's attempt should succeed.

7. From each PC, attempt to ping Router1's Loopback 0 interface (1.1.1.1). Only PC1's ping should succeed.

8. Create standard ACL **2**, and configure it to deny traffic from VLAN 1 (10.10.1.0/24). All other traffic sources should be permitted. Use no more than two rules when configuring ACL 2.

9. Apply standard ACL 2 to an interface and in a direction that will prevent remote networks from pretending to reside on VLAN 1.

10. Display and examine the rules you created for both ACL 1 and ACL 2.

11. Based on what you have configured so far, apply either ACL 1 or ACL 2 to an interface and in a direction that will prevent hosts connected to Router1 from pretending to be hosts on VLAN 2 or VLAN 3.

Lab Solutions

Task 1: Practice Configuring Standard ACLs

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 each PC, 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
```

4. On Router1, you should issue the following commands to create standard ACL **1** and configure it to deny traffic from VLAN 2 (10.10.2.0/24) and VLAN 3 (10.10.3.0/24):

```
Router1>enable
Router1#configure terminal
Router1(config)#access-list 1 deny 10.10.2.0 0.0.1.255
```

The wildcard mask of 0.0.1.255 is equivalent to a subnet mask of 255.255.254.0. A network address of 10.10.2.0 with a subnet mask of 255.255.254.0 creates the 10.10.2.0/23 network, which includes the range of IP address from 10.10.2.0 through 10.10.3.255.

In addition to the commands above, you should issue the following command to permit all other types of traffic:

```
Router1(config)#access-list 1 permit any
```

The command above explicitly permits traffic from any source. If you do not add the above rule to ACL 1, the ACL will apply the implicit deny rule to any traffic that does not match a source address from the 10.10.2.0/23 network.

5. You should issue the following commands to apply standard ACL 1 to the correct interface and in the correct direction:

```
Router1(config)#interface fastethernet 0/0
Router1(config-if)#ip access-group 1 in
```

The commands above apply ACL 1 to the FastEthernet 0/0 interface in the inbound direction. Standard ACLs should always be applied as close to the destination as possible. In this lab, you want to prevent traffic from VLAN 2 and VLAN 3 from accessing any of the networks on Router1. The closest interface to all the networks on Router1 when traffic is coming from VLAN 2 and VLAN 3 is the FastEthernet 0/0 interface. In addition, the traffic from VLAN 2 and VLAN 3 is inbound traffic on the FastEthernet 0/0 interface. Therefore, applying the ACL in the inbound direction will both prevent VLAN 2 and VLAN 3 from accessing Router1's networks and prevent Router1 from having to process the traffic before dropping it.

6. From PC1, the attempt to telnet to Router1's Loopback 0 interface (1.1.1.1) should succeed. From PC2 and PC3, the attempt should fail.

7. From PC1, the attempt to ping Router1's Loopback 0 interface (1.1.1.1) should succeed. From PC2 and PC3, the attempt should fail.

8. On Router1, you should issue the following commands to create standard ACL **2** and configure it to deny traffic from VLAN 1 (10.10.1.0/24):

```
Router1(config)#access-list 2 deny 10.10.1.0 0.0.0.255
```

In addition, you should issue the following command to permit all other sources of traffic:

```
Router1(config)#access-list 2 permit any
```

9. You should issue the following commands to apply standard ACL 2 to an interface and in a direction that will prevent remote networks from pretending to reside on VLAN 1:

```
Router1(config)#interface fastethernet 1/0
Router1(config-if)#ip access-group 2 out
```

The commands above apply ACL 2 to the interface that is directly connected to the destination network of 10.10.1.0/24. ACL 2 is applied in the outbound direction because any traffic that is destined for the 10.10.1.0/24 network has already been processed by the router by the time it reaches the FastEthernet 1/0 interface. Therefore, traffic is flowing out of the FastEthernet 1/0 interface toward VLAN 1 (10.10.1.0/24).

10. You should issue the following commands to display and examine the rules you created for both ACL 1 and ACL 2:

```
Router1(config-if)#end
Router1#show access-lists
Standard IP access list 1
    10 deny 10.10.2.0 0.0.1.255 (20 matches)
    20 permit any (50 matches)
Standard IP access list 2
    10 deny 10.10.1.0 0.0.0.255 (0 matches)
    20 permit any (10 matches)
```

11. Based on what you have configured so far, you should issue the following commands to apply ACL 1 to Router1's FastEthernet 0/0 interface (192.168.51.49) in the outbound direction:

```
Router1#configure terminal
Router1(config)#interface fastethernet 0/0
Router1(config-if)#ip access-group 1 out
```

Because you cannot configure Router2, the FastEthernet 0/0 interface on Router1 is the interface closest to the destination networks of VLAN 2 (10.10.2.0/24) and VLAN 3 (10.10.3.0/24). Additionally, any traffic that is destined for either of those networks from Router1 will be flowing outbound through the FastEthernet 0/0 interface.

Sample Configuration Scripts

Router1

```
Router1#show running-config
Building configuration...
Current configuration : 1005 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 1 in
!
interface FastEthernet1/0
 ip address 10.10.1.1 255.255.255.0
 no ip directed-broadcast
 ip access-group 2 out
!
```

Router1 (continued)

```
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 1 deny   10.10.2.0 0.0.1.255
access-list 1 permit any
access-list 2 deny   10.10.1.0 0.0.0.255
access-list 2 permit any
!
line con 0
line aux 0
line vty 0 4
 login
 password boson
!
no scheduler allocate
end
```