NetSim®
NETWORK SIMULATOR®

Lab ID: 10.215A264.SUP1.1

NetSim® NETWORK SIMULATOR®

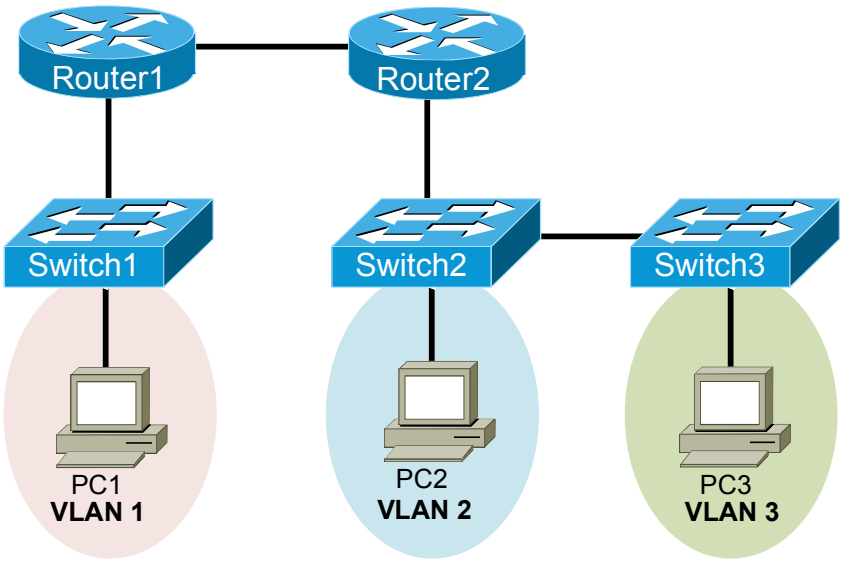
Supplemental Lab: ACL Practice Lab 1: Standard ACLs

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
ping *ip-address*	sends an Internet Control Message Protocol (ICMP) echo request to the specified address
show running-config	displays the active configuration file

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. 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.

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. On the appropriate device, create standard ACL **1**. Standard ACL 1 should permit traffic from the 10.10.3.0/24 network to the 10.10.1.0/24 network. Devices from other networks should be able to ping the gateway address of 10.10.1.1 but no other address on the 10.10.1.0/24 network.

4. On the appropriate device, apply standard ACL 1 to the correct interface and in the correct direction.

5. On the appropriate device, create standard ACL **2**. Standard ACL 2 should permit traffic from the 10.10.1.0/24 network to the 10.10.3.0/24 network. Devices on other networks should be able to ping the 10.10.3.1 gateway address but no other address on the 10.10.3.0/24 network.

6. On the appropriate device, apply standard ACL 2 to the correct interface and in the correct direction.

7. On the appropriate device, create standard ACL **3**. Standard ACL 3 should permit traffic from any network on Router1 to any network on Router2.

8. On the appropriate device, apply standard ACL 3 to the correct interface and in the correct direction.

9. On the appropriate device, create standard ACL **4**. Standard ACL 4 should permit traffic from any network on Router2 to any network on Router1.

10. On the appropriate device, apply standard ACL 4 to the correct interface and in the correct direction.

11. On the appropriate device, add a rule to ACL 1 that permits traffic from Router2's Loopback 0 interface. Use a source address and wildcard mask in the command syntax.

12. On the appropriate device, add a rule to ACL 2 that permits traffic from Router1's Loopback 0 interface Use the **host** keyword in the command syntax.

13. On the appropriate device, add a rule to ACL 2 that permits traffic from the 10.10.2.0/24 network.

14. From each PC, attempt to ping every other IP address in the topology. You have completed this lab when the pings succeed or fail according to the following table:

	1.1.1.1	2.2.2.2	10.10.1.101	10.10.2.102	10.10.3.103
PC1	Yes	Yes	Yes	No	Yes
PC2	Yes	Yes	No	Yes	Yes
PC3	Yes	Yes	Yes	Yes	Yes

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. On Router1, you should issue the following commands to create standard ACL **1** and configure it to permit traffic from the 10.10.3.0/24 network:

```
Router1>enable
Router1#configure terminal
Router1(config)#access-list 1 permit 10.10.3.0 0.0.0.255
```

   Because you want to explicitly permit traffic from 10.10.3.0/24 to 10.10.1.0/24, you should configure the ACL on Router1 because standard ACLs should be applied as close to the destination as possible.

4. On Router1, you should issue the following commands to apply ACL 1 to the FastEthernet 1/0 interface in the outbound direction:

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

   Standard ACLs should be applied as close to the destination as possible. Because you are permitting traffic to the 10.10.1.0/24 network, which is directly connected to Router1's FastEthernet 1/0 interface, you should apply the ACL in the outbound direction.

5. On Router2, you should issue the following commands to create standard ACL **2** and configure it to permit traffic from the 10.10.1.0/24 network:

```
Router2>enable
Router2#configure terminal
Router2(config)#access-list 2 permit 10.10.1.0 0.0.0.255
```

6. On Router2, you should issue the following commands to apply standard ACL 2 to the FastEthernet 1/0.3 subinterface, which is directly connected to the 10.10.3.0/24 network:

```
Router2(config)#interface fastethernet 1/0.3
Router2(config-subif)#ip access-group 2 out
```

7. On Router2, you should issue the following commands to create standard ACL **3** and configure it to permit traffic from any network:

```
Router2(config-subif)#exit
Router2(config)#access-list 3 permit any
```

The **any** keyword in the command above is equivalent to a network address of 0.0.0.0 and a wildcard mask of 255.255.255.255. Together, a network address of 0.0.0.0 and a subnet mask of 0.0.0.0 represent any network. The wildcard mask of 255.255.255.255 is the equivalent of the subnet mask of 0.0.0.0.

8. On Router2, you should issue the following commands to apply standard ACL 3 to the FastEthernet 0/0 interface in the inbound direction:

```
Router2(config)#interface fastethernet 0/0
Router2(config-if)#ip access-group 3 in
```

Because you want to allow any network from Router1 to connect to any network on Router2, you should apply ACL 3 to Router2's FastEthernet 0/0 interface, which is the interface that is closest to the destination. You should apply ACL 3 in the inbound direction so that Router2 identifies the traffic before it is processed by the router.

9. On Router1, you should issue the following commands to create standard ACL **4** and configure it to permit traffic from any network on Router2:

```
Router1(config-if)#exit
Router1(config)#access-list 4 permit any
```

10. On Router1, you should issue the following commands to apply standard ACL 4 to the FastEthernet 0/0 interface in the inbound direction:

```
Router1(config)#interface fastethernet 0/0
Router1(config-if)#ip access-group 4 in
```

11. On Router1, you should issue the following command, including an IP address and a wildcard mask, to modify standard ACL 1 so that it permits traffic from Router2's Loopback 0 interface (2.2.2.2):

```
Router1(config-if)#exit
Router1(config)#access-list 1 permit 2.2.2.2 0.0.0.0
```

You can add rules to a standard ACL by issuing new **access-list** commands with the appropriate ACL number and the rule you want to add. However, this method of adding rules is cumulative. Therefore, you cannot edit a specific rule within the ACL by using this method.

This step specifies that you are to use the IP address and subnet mask of Router2's Loopback interface as shown in the command above. The wildcard mask of 0.0.0.0 is equivalent to the single-host subnet mask of 255.255.255.255. If the use of an IP address and wildcard mask were not specified, you could specify a single host address by issuing the **access-list** command with the **host** keyword, as shown below:

```
Router1(config)#access-list 1 permit host 2.2.2.2
```

12. On Router2, you should issue the following commands to modify standard ACL 2 so that it permits traffic from Router1's Loopback 0 interface (1.1.1.1) using the **host** keyword:

```
Router2(config-if)#exit
Router2(config)#access-list 2 permit host 1.1.1.1
```

13. On Router2, you should issue the following command to modify standard ACL 2 so that it permits traffic from the 10.10.2.0/24 network:

```
Router2(config)#access-list 2 permit 10.10.2.0 0.0.0.255
```

14. From each PC, you should ping the following IP addresses:

Router1's Loopback 0 interface: 1.1.1.1
Router2's Loopback 0 interface: 2.2.2.2
PC1: 10.10.1.101
PC2: 10.10.2.102
PC3: 10.10.3.103

Of the specified pings, only pings from PC1 to the 10.10.2.0/24 network and pings from PC2 to PC1 (10.10.1.101) network should fail. All other pings should succeed.

Sample Configuration Scripts

Router1	Router1 (continued)
Router1#show running-config Building configuration... Current configuration : 972 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 4 in ip access-group 102 out ! interface FastEthernet1/0 ip address 10.10.1.1 255.255.255.0 no ip directed-broadcast ip access-group 1 out !	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 permit 10.10.3.0 0.0.0.255 access-list 1 permit host 2.2.2.2 access-list 4 permit any ! line con 0 line aux 0 line vty 0 4 login password boson ! no scheduler allocate end

Router2	Router2 (continued)
Router2#show running-config Building configuration... Current configuration : 1297 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 3 in 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 ip access-group 2 out ! 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 2 permit 10.10.1.0 0.0.0.255 access-list 2 permit host 1.1.1.1 access-list 2 permit 10.10.2.0 0.0.0.255 access-list 3 permit any ! line con 0 line aux 0 line vty 0 4 login password boson ! no scheduler allocate end