Lab ID: 9.9K714A056.SAI1.2

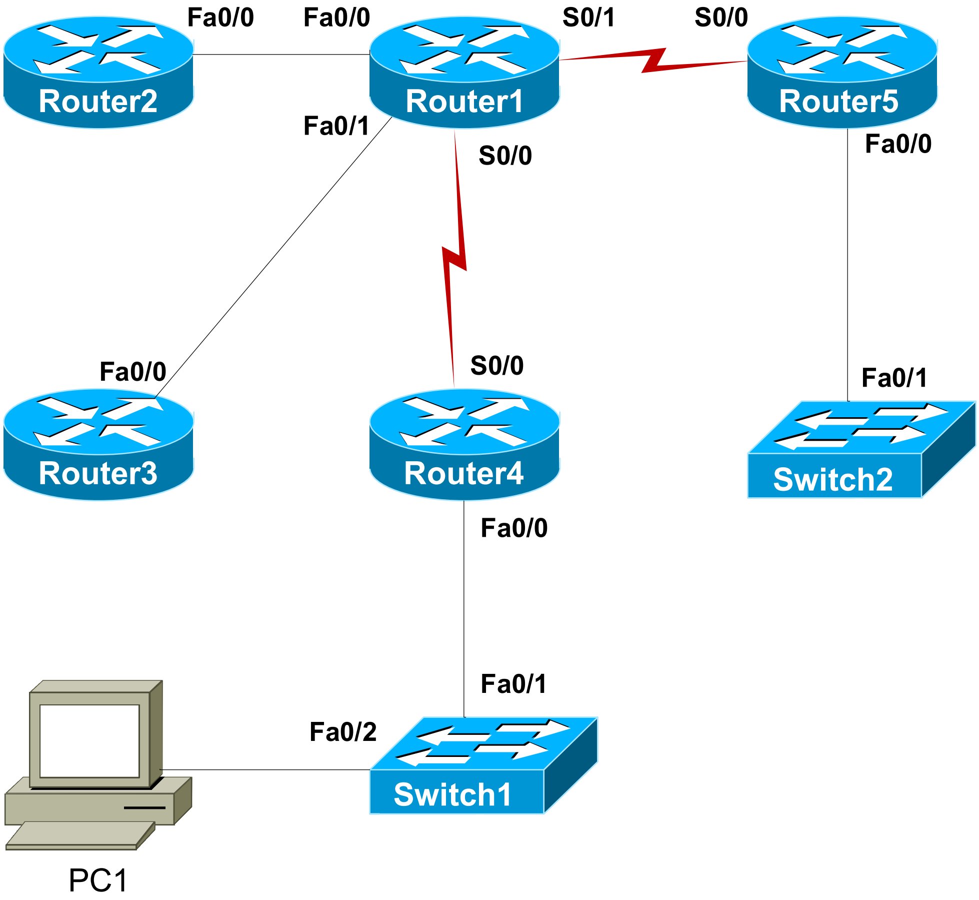
Stand-Alone Lab: Standard Access Lists

Objective

Learn to configure standard access control lists (ACLs). Configure the appropriate settings on Router1, Router2, and Router4.

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
clock rate *clock-rate*	sets the clock rate for a Data Communications Equipment (DCE) interface
configure terminal	enters global configuration mode from privileged EXEC mode
enable	enters privileged EXEC mode
end	ends and exits configuration mode

Command	Description
exit	exits one level in the menu structure
hostname *host-name*	sets the device name
interface *type number*	changes from global configuration mode to interface configuration mode
ip address *ip-address subnet-mask*	assigns an IP address to an interface
ip access-group {*access-list-number* | *access-list-name*} {**in** | **out**}	controls access to an interface
network *network-address*	activates the specified routing protocol on the specified network
no shutdown	enables an interface
ping *ip-address*	sends an Internet Control Message Protocol (ICMP) echo request to the specified address
router rip	enables Routing Information Protocol (RIP) routing
show access-lists [*access-list-number* | *access-list-name*]	displays the contents of current ACLs
show ip interface	displays IP information for an interface
show running-config	displays the active configuration file
version 2	enables RIP version 2 (RIPv2)

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

IP Addresses

Device	Interface	IP Address	Subnet Mask
Router1	FastEthernet 0/0 Serial 0/0	24.17.2.1 24.17.2.17	255.255.255.240 255.255.255.240
Router2	FastEthernet 0/0	24.17.2.2	255.255.255.240
Router4	Serial 0/0	24.17.2.18	255.255.255.240

Lab Tasks

Task 1: Configure the Routers with IP Addresses and with RIPv2

1. Configure Router1 with the appropriate host name, IP addresses, and subnet masks; refer to the IP Addresses table. Enable the interfaces. Configure a clock rate of 64 Kbps on the Serial 0/0 interface. A clock rate must be configured on Router1 because it is the DCE end of the link to Router4.

2. Configure Router2 with the appropriate host name, IP address, and subnet mask; refer to the IP Addresses table. Enable the interface.

3. Configure Router4 with the appropriate host name, IP address, and subnet mask; refer to the IP Addresses table. Enable the interface.

4. Verify the configuration by pinging from Router1 to Router2's FastEthernet 0/0 interface (24.17.2.2) and from Router1 to Router4's Serial 0/0 interface (24.17.2.18). The pings should be successful.

5. Configure RIPv2 to advertise the networks on all three routers' configured interfaces.

6. Allow a short period of time to elapse for the network to converge, and then ping Router2's FastEthernet 0/0 interface (24.17.2.2) from Router4. The ping should be successful.

Task 2: Configure Standard ACLs

This task involves configuring an ACL to block the traffic from Router4 destined to Router2.

1. How many standard ACLs can be configured on a router?________________________________

2. Standard ACLs filter all IP traffic and filter based on only the source IP address. What command should you issue, using ACL **1**, to block traffic from the Serial 0/0 interface of Router4 destined to Router2? ____

3. What router should the ACL be created on, and why? ____________________________________

4. On the appropriate router, issue the commands that will create ACL **1** to block traffic from Router4 destined to Router2.

5. Ping from Router4 to Router2's FastEthernet 0/0 interface (24.17.2.2). The ping should succeed. Why does the ping succeed after the ACL is created? ____________________________________

6. Should the ACL be applied in the inbound or the outbound direction? ______________________

7. Apply the ACL to the correct interface and in the best direction on the appropriate router.

8. Ping from Router4 to Router2's FastEthernet 0/0 interface (24.17.2.2) again. The ping should fail.

Task 3: Edit Standard ACLs

This task involves editing the ACL configured in the previous task.

1. On Router1, ping Router2's FastEthernet 0/0 interface (24.17.2.2). Why does the ping fail? ______
   ____

2. What command should be issued to allow all other traffic to reach Router2? __________________

3. On Router2, edit ACL 1 to allow all other traffic to reach Router2.

4. On Router1, ping Router2's FastEthernet 0/0 interface (24.17.2.2) again. The ping should succeed.

Task 4: Verify ACLs

This task involves using **show** commands to display configured ACLs. Perform the following steps on Router2:

1. Display the access lists that have been created on the router. Examine the output.

2. Review the ACL statements configured on Router2.

3. View which ACLs are applied to the interfaces.

Lab Solutions

Task 1: Configure the Routers with IP Addresses and with RIPv2

1. On Router1, you should issue the following commands to configure the appropriate host name, IP addresses, and subnet masks, to enable the interfaces, and to configure a clock rate on the Serial 0/0 interface:

```
Router>enable
Router#configure terminal
Router(config)#hostname Router1
Router1(config)#interface fastethernet 0/0
Router1(config-if)#ip address 24.17.2.1 255.255.255.240
Router1(config-if)#no shutdown
Router1(config-if)#interface serial 0/0
Router1(config-if)#ip address 24.17.2.17 255.255.255.240
Router1(config-if)#clock rate 64000
Router1(config-if)#no shutdown
```

2. On Router2, you should issue the following commands to configure the appropriate host name, IP address, and subnet mask and to enable the interface:

```
Router>enable
Router#configure terminal
Router(config)#hostname Router2
Router2(config)#interface fastethernet 0/0
Router2(config-if)#ip address 24.17.2.2 255.255.255.240
Router2(config-if)#no shutdown
```

3. On Router4, you should issue the following commands to configure the appropriate host name, IP address, and subnet mask and to enable the interface:

```
Router>enable
Router#configure terminal
Router(config)#hostname Router4
Router4(config)#interface serial 0/0
Router4(config-if)#ip address 24.17.2.18 255.255.255.240
Router4(config-if)#no shutdown
```

4. Verify the configuration by pinging from Router1 to Router2’s FastEthernet 0/0 interface and from Router1 to Router4’s Serial 0/0 interface. The pings should be successful.

```
Router1(config-if)#end
Router1#ping 24.17.2.2
Router1#ping 24.17.2.18
```

5. Issue the following commands to configure RIPv2 to advertise the networks on all three routers' configured interfaces:

```
Router1#configure terminal
Router1(config)#router rip
Router1(config-router)#version 2
Router1(config-router)#network 24.0.0.0

Router2(config-if)#router rip
Router2(config-router)#version 2
Router2(config-router)#network 24.0.0.0

Router4(config-if)#router rip
Router4(config-router)#version 2
Router4(config-router)#network 24.0.0.0
```

6. Allow a short period of time to elapse for the network to converge, and then ping from Router4 to Router2's FastEthernet 0/0 interface (24.17.2.2). The ping should be successful.

```
Router4(config-router)#end
Router4#ping 24.17.2.2
```

Task 2: Configure Standard ACLs

1. Up to 99 standard IP ACLs, numbered 1 through 99, can be configured on a router. ACLs can be identified by an access list number or an access list name. Numbered ACLs ranging from 1 through 99 are standard ACLs and can identify traffic based on only the source IP address. Numbered ACLs ranging from 100 through 199 are extended ACLs and can identify traffic based on source and destination IP addresses as well as traffic type.

   You should create an ACL to match the types of traffic you want to filter and then assign the ACL to the interface through which the traffic passes.

2. You should issue the **access-list 1 deny host 24.17.2.18** command to block traffic from Router4's Serial 0/0 interface, 24.17.2.18, destined to Router2.

3. The ACL should be created on Router2. Standard ACLs block traffic based on the source address, so it is a best practice to configure standard ACLs as close as possible to the destination that you want to prevent traffic from reaching. Placing a standard ACL too close to the source of the traffic will prevent any traffic from getting past that device. For example, configuring a standard ACL on Router1 would prevent Router4 from accessing Router1 and Router2, which is not the intended purpose.

   Conversely, it is a best practice to configure extended ACLs as close as possible to the source of the traffic because extended ACLs can filter traffic based on the destination and traffic type. This allows specific traffic to be dropped as soon as it leaves the source. By configuring an extended ACL close to the source, you can minimize wasted network bandwidth by preventing packets from traveling through the network before they are dropped at the destination.

4. On Router2, issue the following command to create an ACL to block traffic from Router4 destined to Router2:

```
Router2(config-router)#exit
Router2(config)#access-list 1 deny host 24.17.2.18
```

5. A ping from Router4 to Router2's FastEthernet 0/0 interface (24.17.2.2) succeeds after the ACL is created because the ACL has not yet been applied to an interface. An ACL must be created on the device and then applied to an interface on the device before the device will be able to filter traffic.

```
Router4#ping 24.17.2.2
```

6. In this lab, the ACL should be applied in the inbound direction because the goal is to block traffic from getting in to Router2. If, however, the goal were to keep traffic from leaving Router2, the ACL would then be applied in the outbound direction.

7. You should issue the following commands to apply the ACL to the correct interface and in the best direction on the appropriate router:

```
Router2(config)#interface fastethernet 0/0
Router2(config-if)#ip access-group 1 in
```

8. Ping from Router4 to Router2's FastEthernet 0/0 interface again. The ping should fail.

```
Router4#ping 24.17.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 24.17.2.2, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5), round-trip min/avg/max = 1/2/4 ms
```

Task 3: Edit Standard ACLs

1. The ping from Router1 to the FastEthernet 0/0 interface on Router2 (24.17.2.2) fails because the previously created ACL is blocking all traffic from entering Router2. At the end of every ACL is an implicit **deny any** statement that will block all traffic that has not been explicitly allowed by the preceding statements in the ACL.

   ACLs can consist of multiple access list statements. Packets are compared to each statement in sequence until a match is found. The **permit** and **deny** keywords are used to indicate whether matching packets should be forwarded or dropped, respectively. If the packet does not match any of the access list statements, the packet is dropped. This is called the *implicit deny* rule; all traffic is dropped unless it matches one of the access list statements that is configured with the **permit** keyword.

2. You should issue the **access-list 1 permit any** command on Router2 to create a statement that will allow all traffic not blocked by the preceding statement. The only preceding statement in this lab is the statement configured in Task 2 to block the 24.17.2.18 address from reaching Router2. This statement alone is sufficient because a router will parse the statements in an ACL in the order they were added. However, you should be careful when editing an ACL, because you must remove all statements in an ACL in order to insert one in the middle.

3. On Router2, issue the following commands to edit ACL 1 to allow all other traffic to reach Router2:

   ```
   Router2(config-if)#exit
   Router2(config)#access-list 1 permit any
   ```

4. A ping from Router1 to Router2's FastEthernet 0/0 interface should succeed.

   ```
   Router1(config-router)#end
   Router1#ping 24.17.2.2
   ```

Task 4: Verify ACLs

Perform the following steps on Router2:

1. Issue the **show access-lists** command to display which access lists have been created on the router. The output will also tell you which statements have been used and how many packets have been either permitted or denied. Below is sample output:

   ```
   Router2(config)#end
   Router2#show access-lists
   Standard IP access list 1
       10 deny   host 24.17.2.18 (5 matches)
       20 permit any (5 matches)
   ```

2. You should issue the **show running-config** command to review the ACL statements configured on Router2. Below is sample output:

```
Router2#show running-config
Building configuration...
!
Version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router2
!
ip subnet-zero
!
<output omitted>
!
interface FastEthernet0/0
 ip address 24.17.2.2 255.255.255.240
 no ip directed-broadcast
 ip access-group 1 in
!
<output omitted>
!
access-list 1 deny   host 24.17.2.18
access-list 1 permit any
!
line con 0
line aux 0
line vty 0 4
!
no scheduler allocate
end
```

3. You should issue the **show ip interface fastethernet 0/0** command to view which ACLs are applied to the interfaces. Below is sample output:

```
Router2#show ip interface fastethernet 0/0
FastEthernet0/0 is up, line protocol is up
  Internet address is 24.17.2.2/28
  Broadcast address is 255.255.255.255
  MTU 1500 bytes,
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is 1
  Proxy ARP Is Enabled
  Security Level Is Default
  Split horizon Is Enabled
  ICMP redirects are always sent
<output omitted>
```

Sample Configuration Script

Router2

```
Router2#show running-config
Building configuration...
Current configuration : 790 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 Serial0/0
 no ip address
 no ip directed-broadcast
 shutdown
!
interface Serial0/1
 no ip address
 no ip directed-broadcast
 shutdown
!
```

Router2 (continued)

```
interface FastEthernet0/0
 ip address 24.17.2.2 255.255.255.240
 no ip directed-broadcast
 ip access-group 1 in
!
interface FastEthernet0/1
 no ip address
 no ip directed-broadcast
 shutdown
!
router rip
 version 2
 network 24.0.0.0
!
ip classless
no ip http server
!
access-list 1 deny   host 24.17.2.18
access-list 1 permit any
!
line con 0
line aux 0
line vty 0 4
!
no scheduler allocate
end
```