Lab ID: 9.9K1114A057.SAI1.2

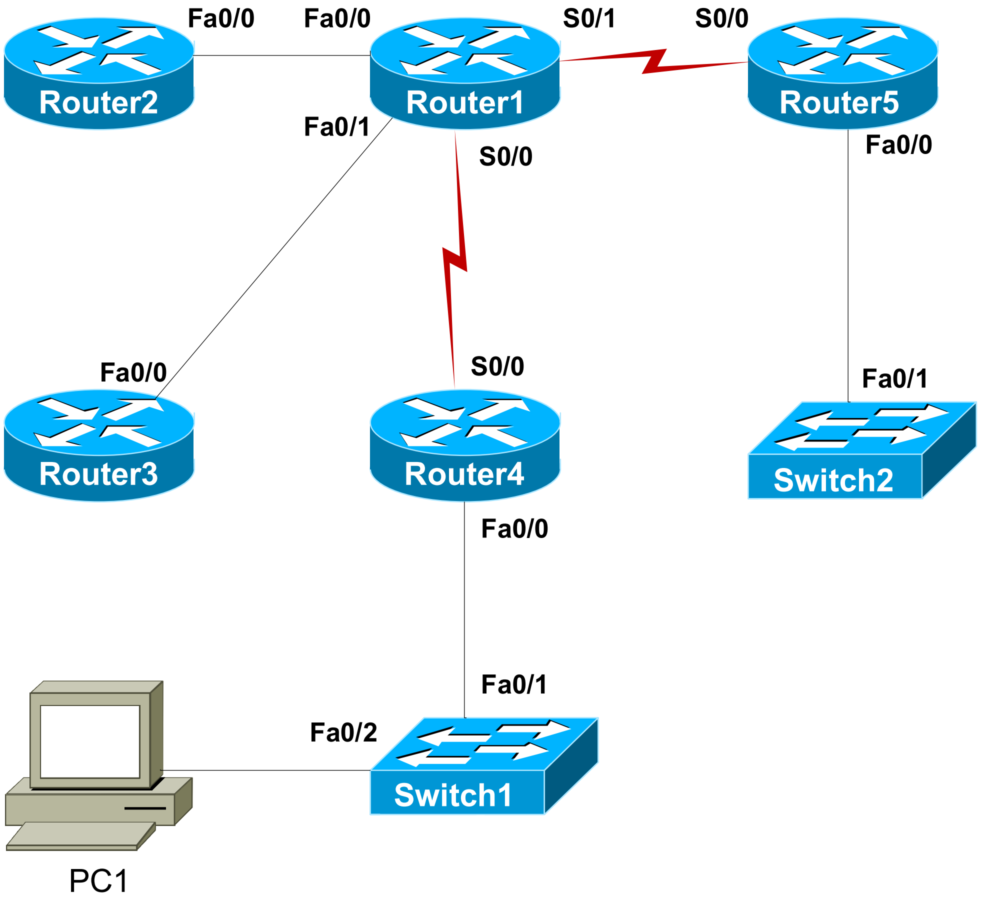
Stand-Alone Lab: Extended Access Lists

Objective

Learn to configure extended access control lists (ACLs). Verify the ACLs by using **show** commands and network connectivity tests. 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**} *protocol source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**log**]	defines an extended IP access control list (ACL) for the traffic type specified by the protocol parameter
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

Command	Description
disconnect {*ip-addres*s | **console**}	closes an active console port or Telnet session
enable	enters privileged EXEC mode
end	ends and exits configuration mode
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
line vty 0 4	enters configuration mode for virtual terminal (Telnet) lines
login	enables password checking at login
network *network-address*	activates the specified routing protocol on the specified network
no shutdown	enables an interface
password *password*	specifies the password that is required for a user to log in
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
telnet *ip-address*	starts the terminal emulation program from a PC, router, or switch; permits you to access devices remotely over the network
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

This task involves configuring IP addresses on the router interfaces and enabling 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).

5. Configure RIPv2 on all three routers, and advertise the networks of all configured interfaces.

6. After allowing time for the network to converge, verify that you can ping from Router4 to Router2's FastEthernet 0/0 interface (24.17.2.2). The ping should be successful.

Task 2: Configure Extended ACLs

In this task, you will configure extended ACLs to accomplish two things. First, they will allow only Telnet traffic from the subnet of Router1's Serial 0/0 interface to come into Router1. Second, they will allow any traffic from Router1's FastEthernet 0/0 subnet to travel anywhere. Numbered access lists ranging from 100 through 199 are extended ACLs and can identify traffic based on source and destination IP addresses as well as traffic type. This lab requires that you identify traffic based on source and destination IP address as well as the type of traffic; therefore, you should use an extended ACL in this configuration.

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.

1. What type of transport protocol is Telnet? ________________________________

2. When you are creating ACLs, what keyword should you use to display output to the router console every time an ACL statement on an ACL is invoked? ____________________________

3. On Router1, create ACL **101** to permit only Telnet traffic from the subnet configured on the Serial 0/0 interface.

4. On Router1, create ACL **102** to permit all traffic from the subnet configured on the FastEthernet 0/0 interface.

5. On Router1, assign ACL **101** to Serial 0/0 in the inbound direction, and assign ACL **102** to FastEthernet 0/0 in the inbound direction.

Task 3: Verify Extended ACLs

This task involves verifying that the extended ACLs created in the previous task are configured correctly.

1. On Router4, try to ping Router1's Serial 0/0 interface (24.17.2.17). The ping should fail.

2. In order to test Telnet access, you must permit Telnet login. On Router1, issue the appropriate commands to configure Telnet access, using **boson** as the password.

3. On Router4, try to telnet to Router1's Serial 0/0 interface. The session attempt should be successful.

4. On Router4, press the Ctrl+Shift+6 key combination followed immediately by the X key to return to the Router4 prompt. Issue the **disconnect 1** command to close the connection to Router1.

5. On Router2, ping Router1's Serial 0/0 interface (24.17.2.1) and Router4's Serial 0/0 interface (24.17.2.18). The ping to Router1 should succeed, and the ping to Router4 should fail. Why? ____
____

6. On Router1, verify that the access lists are configured on the interfaces.

7. On Router1, view which access lists are applied to the interfaces.

8. On Router1, display which ACLs have been created on a router. The output will also tell you which statements of the ACL have been used and how many packets have been permitted or denied.

Lab Solutions

Task 1: Configure the Routers

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.

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

5. Configure RIPv2 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. After allowing time for the network to converge, verify that you can ping Router2's FastEthernet 0/0 interface (24.17.2.2) from Router4. The ping should be successful.

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

Task 2: Configure Extended ACLs

1. Telnet is a Transmission Control Protocol (TCP) transport protocol.

2. When creating ACLs, you should use the **log** keyword to display output to the router console every time an ACL statement on an ACL is invoked.

3. On Router1, issue the following commands to create ACL **101** to permit only Telnet traffic from the subnet configured on the Serial 0/0 interface:

```
Router1(config-router)#exit
Router1(config)#access-list 101 permit tcp 24.17.2.16 0.0.0.15 any eq telnet log
```

Numbered access lists ranging from 100 through 199 are extended ACLs and can identify traffic based on source and destination IP addresses as well as traffic type. This lab requires that you identify traffic based on source and destination IP address as well as the type of traffic; therefore, you should use an extended ACL in this configuration.

4. On Router1, issue the following command to create ACL **102** to permit all traffic from the subnet configured on the FastEthernet 0/0 interface:

```
Router1(config)#access-list 102 permit ip 24.17.2.0 0.0.0.15 any log
```

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.

5. On Router1, issue the following commands to assign ACL **101** to Serial 0/0 in the inbound direction and to assign ACL **102** to FastEthernet 0/0 in the inbound direction:

```
Router1(config)#interface serial 0/0
Router1(config-if)#ip access-group 101 in
Router1(config-if)#interface fastethernet 0/0
Router1(config-if)#ip access-group 102 in
```

Task 3: Verify Extended ACLs

1. On Router4, try to ping Router1's Serial 0/0 interface. The ping should fail.

```
Router4#ping 24.17.2.17
```

2. In order to test Telnet access, you must permit Telnet login. On Router1, issue the following commands to configure Telnet access:

```
Router1(config-if)#exit
Router1(config)#line vty 0 4
Router1(config-line)#login
Router1(config-line)#password boson
```

3. On Router4, try to telnet to Router1's Serial 0/0 interface. The session attempt should be successful.

```
Router4#telnet 24.17.2.17
Trying 24.17.2.17 ... Open
Password:boson
Router1>
```

4. On Router4, press the Ctrl+Shift+6 key combination followed immediately by the X key to return to the Router4 prompt. Issue the **disconnect 1** command to close the connection to Router1.

```
Router1>Press Ctrl+Shift+6 X
Router4#disconnect 1
Closing connection to 24.17.2.17
```

5. The ping leaving Router2 destined to Router1's FastEthernet 0/0 interface (24.17.2.1) succeeds because there is connectivity and no ACL filtering ICMP traffic. The ping leaving Router2 destined for Router4's Serial 0/0 interface (24.17.2.18) fails because, once the ping reaches Router4, the source and destination addresses are switched, which causes Router1 to block the ping reply. The ping reply is blocked because the ACL configured on Router1's Serial 0/0 interface blocks traffic, other than TCP traffic, with the source address of 24.17.2.18.

```
Router2(config-router)#end
Router2#ping 24.17.2.1
Router2#ping 24.17.2.18
```

6. On Router1, issue the **show running-config** command to verify that the access lists are configured on the interfaces. Sample output is shown below:

```
Router1>enable
Router1#show running-config
Building configuration...
!
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 Serial0/0
 ip address 24.17.2.17 255.255.255.240
 no ip directed-broadcast
 clock rate 64000
 ip access-group 101 in
!
interface Serial0/1
 no ip address
 no ip directed-broadcast
 shutdown
!
<output omitted>
!
interface FastEthernet0/0
 ip address 24.17.2.1 255.255.255.240
 no ip directed-broadcast
 ip access-group 102 in
!
<output omitted>
!
```

(continued on next page)

(continued from previous page)

```
 router rip
 version 2
 network 24.0.0.0
!
ip classless
no ip http server
!
access-list 101 permit tcp 24.17.2.16 0.0.0.15 any eq telnet log
access-list 102 permit ip 24.17.2.0 0.0.0.15 any log
!
line con 0
line aux 0
line vty 0 4
 login
 password boson
!
no scheduler allocate
end
```

7. On Router1, issue the **show ip interface** command to view which access lists are applied to the interfaces. Sample output is shown below:

```
Router1#show ip interface
Serial0/0 is up, line protocol is up
  Internet address is 24.17.2.17/28
  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 101
<output omitted>

FastEthernet0/0 is up, line protocol is up
  Internet address is 24.17.2.1/28
  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 102
<output omitted>
FastEthernet0/1 is administratively down, line protocol is down
  Internet protocol processing disabled
```

8. On Router1, issue the **show access-lists** command to display which ACLs have been created on a router. The output will also tell you which statements of the ACL have been used and how many packets have been permitted or denied. Sample output is below:

```
Router1#show access-lists
Extended IP access list 101
    10 permit tcp 24.17.2.16 0.0.0.15 any eq telnet log (1 matches)
Extended IP access list 102
    10 permit ip 24.17.2.0 0.0.0.15 any log (4 matches)
```

Sample Configuration Script

Router1

```
Router1#show running-config
Building configuration...
Current configuration : 933 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 Serial0/0
 ip address 24.17.2.17 255.255.255.240
 no ip directed-broadcast
 clock rate 64000
 ip access-group 101 in
!
interface Serial0/1
 no ip address
 no ip directed-broadcast
 shutdown
!
interface FastEthernet0/0
 ip address 24.17.2.1 255.255.255.240
 no ip directed-broadcast
 ip access-group 102 in
!
```

Router1 (continued)

```
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 101 permit tcp 24.17.2.16
0.0.0.15 any eq telnet log
access-list 102 permit ip 24.17.2.0
0.0.0.15 any log
!
line con 0
line aux 0
line vty 0 4
 login
 password boson
!
no scheduler allocate
end
```