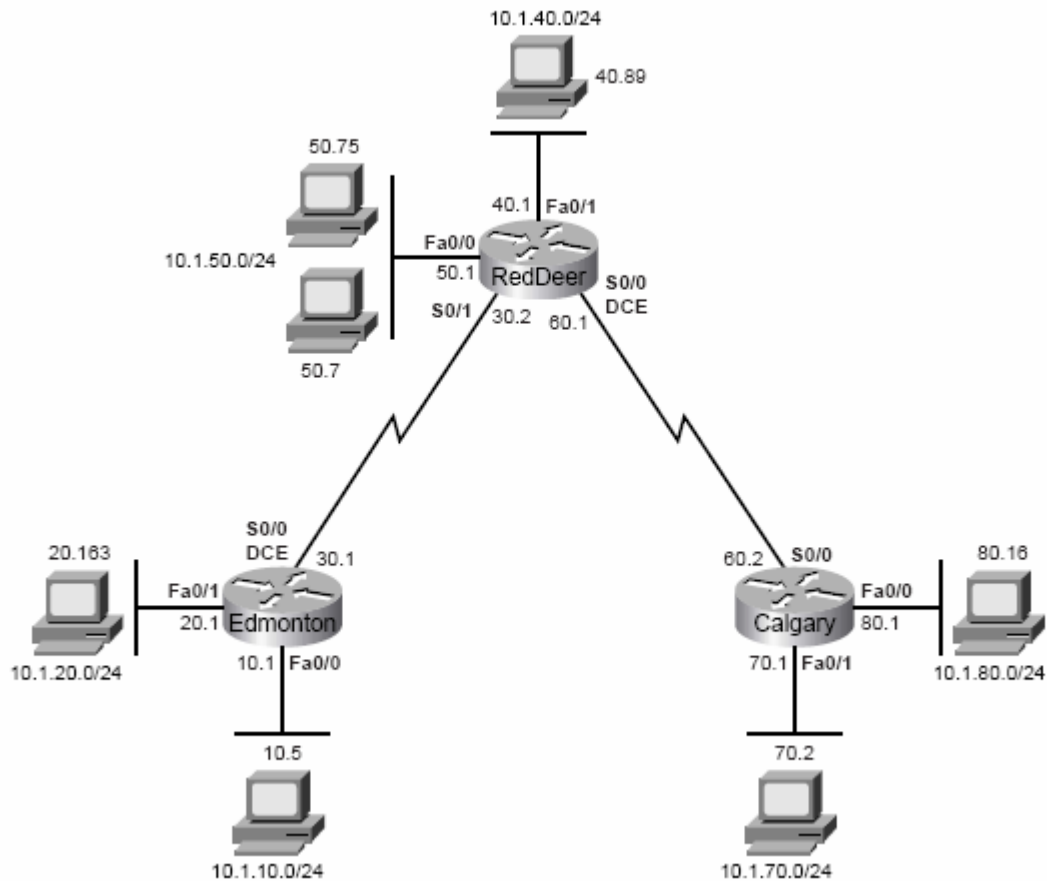


Challenge Lab 11-10b: Three Routers with Multiple ACL Configurations (Form B)

Figure 11-7b Three Router ACL Configuration Topology (Form B)



Objectives

- Cable and configure routers with basic configuration
- Configure RIP routing
- Implement multiple ACL security policies
- Verify ACL configurations

Equipment

This lab can be done with any combination of routers. However, all routers must have at least two Ethernet or FastEthernet interfaces. If your lab equipment does not support this lab, then complete Challenge Lab 11-10a: Three Routers with Multiple ACL Configurations (Form A). The security requirements for the two forms of this lab are similar. The tasks are adjusted to fit routers with only one Ethernet or FastEthernet interface.

Although the topology shows seven PCs, you only need two each time you test an ACL. This can be achieved by moving PCs from LAN to LAN and changing the IP addressing.

NetLab Compatibility Notes

This lab can be completed using NetLab. However, you will not be able to effectively test your access control lists.

Task 1: Cable the Lab

1. Cable the lab as shown in the Figure 11-6.
2. If you use different interface designations, then change the topology labels accordingly.

Task 2: Router, Routing, and PC Configuration

You may need to refer to your notes and labs from previous chapters in order to complete this section.

1. Configure all routers with basic configurations according to your Instructor's requirements.
2. Configure and activate all the necessary interfaces.
3. Configure dynamic routing using RIP.
4. Configure PCs with appropriate addressing.

Task 3: Verify and Troubleshoot Your Network Configuration

1. Each router should have eight routes. The routing table for RED_DEER is shown here.

```
RED_DEER#show ip route
!Codes omitted for brevity
 10.0.0.0/24 is subnetted, 8 subnets
R    10.1.10.0 [120/1] via 10.1.30.1, 00:00:09, Serial0/1
C    10.1.30.0 is directly connected, Serial0/1
R    10.1.20.0 [120/1] via 10.1.30.1, 00:00:09, Serial0/1
C    10.1.40.0 is directly connected, FastEthernet0/1
C    10.1.60.0 is directly connected, Serial0/0
C    10.1.50.0 is directly connected, FastEthernet0/0
R    10.1.70.0 [120/1] via 10.1.60.2, 00:00:17, Serial0/0
R    10.1.80.0 [120/1] via 10.1.60.2, 00:00:22, Serial0/0
```

2. Use ping to test connectivity throughout the network. Make sure that all LANs are reachable before configuring access control lists in the next step.

Task 4: Configure and Verify Access Control Lists

Use the space provided below each Security Policy to write out the access control list.

Security Policy #1

Block the 10.1.10.0 network from accessing the 10.1.40.0 network. All other access to 10.1.40.0 is allowed.

- Standard or Extended? _____
- Router? _____
- Interface? _____
- Direction? _____

Verify Security Policy #1

For this policy, you need only the 10.1.40.89 host configured. You can use extended ping from the EDMONTON router, specifying the 10.1.10.1 interface address as the source address. The ping should fail. A regular ping from the EDMONTON as well as pings from any other destination should succeed.

Security Policy #2

Host 10.1.10.5 is not allowed to access host 10.1.50.7. All other hosts are allowed to access 10.1.50.7.

- Standard or Extended? _____
- Router? _____
- Interface? _____
- Direction? _____

Verify Security Policy #2

Host 10.1.10.5 should not be able to ping 10.1.50.7. All other addresses should be able to ping 10.1.50.7. Host 10.1.10.5 should be able to ping 10.1.50.75 and the 10.1.50.1 interface.

Security Policy #3

Host 10.1.70.2 is allowed Telnet access to the RED_DEER router. In addition, EDMONTON and CALGARY routers should be able to telnet to the RED_DEER router. All other Telnet access to RED_DEER is blocked.

Hint: The IP address that EDMONTON will use to telnet to RED_DEER is 10.1.30.1. The IP address that CALGARY uses to telnet to RED_DEER is 10.1.60.2

- Standard or Extended? _____
- Router? _____
- Interface or Line? _____
- Direction? _____

Verify Security Policy #3

You only need one PC to test this policy. From a command prompt on host 10.1.70.2, you should be able to Telnet to any address on RED_DEER. You should also be able to Telnet from either router. All other hosts should NOT be able to Telnet to RED_DEER.

Security Policy #4

Host 10.1.20.163 is allowed to Telnet to host 10.1.70.2. No other host on the 10.1.20.0/24 network should be allowed Telnet access to 10.1.70.2. All other access is allowed.

Note: To test Telnet access to a host, you can install a Telnet server or simulated Telnet server on host 10.1.70.2. Use your favorite search engine to find a freeware Telnet server or simulator you can install. For example, ServTerm 1.0 at <http://www.pc-tools.net/win32/servterm/> can simulate any port number you wish to test. So it can also be used to simulate a Web server, Mail server, or File server.

- Standard or Extended? _____
- Router? _____
- Interface? _____
- Direction? _____

Verify Security Policy #4

Host 10.1.20.163 should be allowed to telnet to 10.1.70.2. Configure the workstation with a different IP address from the 10.1.20.0/24 network to test that Telnet access is denied.

Security Policy #5

Hosts 10.1.50.1 through 10.1.50.63 are not allowed web access to 10.1.80.16. All other hosts are allowed web access to 10.1.80.16. All other access is allowed.

- Standard or Extended? _____
- Router? _____
- Interface? _____
- Direction? _____

Verify Security Policy #5

To test this policy, you will need a Web server installed and running on host 10.1.80.16. You can use ServTerm 1.0 to simulate a Web server or download and install one of the many freeware Web servers available on the Internet. Web access from host 10.1.50.7 to host 10.1.80.16 should be blocked. All other hosts should have web access 10.1.80.16. Also, test to make sure that 10.1.50.7 has web access to other destinations. For example, 10.1.50.7 should be able to open a web page from one of the three routers as long as the routers have the HTTP service active.

Security Policy #6

Only hosts from the 10.1.50.0/24 LAN should be allowed to access the HTTP service on the CALGARY router. Make sure that HTTP is enabled on CALGARY with the **ip http server** command. All other hosts should be denied this access.

- Standard or Extended? _____
- Router? _____

Verify Security Policy #6

A host from the 10.1.50.0/24 LAN should be able to open a web browser to any valid address on the CALGARY router. No other host should be able to gain access to CALGARY through a web browser.

Security Policy #7

Use the name "NOPINGS" to configure a named ACL that will stop all pings from the 10.1.70.0/24 network from reaching hosts on the 10.1.10.0/24 network. All other access should be allowed.

- Standard or Extended? _____
- Router? _____
- Interface? _____
- Direction? _____

Verify Security Policy #7

Host 10.1.70.2 should not be able to ping host 10.1.10.5. However host 10.1.70.2 should be able to ping all other addresses. All other hosts should be able to ping 10.1.10.5.