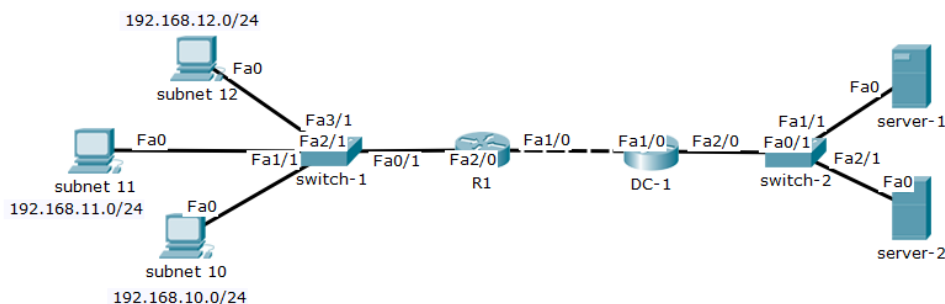# Extended ACL-2

## Lab Summary

Configure an extended numbered ACL to filter packets based on the following requirements.

1. Configure extended access list number 100
2. Deny all traffic from hosts on VLAN 10 to server-1
3. Deny FTP traffic from hosts on VLAN 11 to server-2
4. Deny all traffic from hosts on VLAN 12 to server-1 and server-2
5. Permit all traffic not matching on any previous ACL statements
6. Apply ACL 100 outbound on R1 interface FastEthernet1/0

**Figure 1**  Lab Topology



## Lab Configuration

Start Packet Tracer File: **Extended ACL-2**

Verify that FTP and web server access is permitted from all hosts/subnets.

192.168.10.0/24 (hosts): **http://192.168.3.1** (yes)

192.168.10.0/24 (hosts): c:\> **ftp 192.168.3.2**

Username **cisco**  Password **cisco** (yes)

192.168.11.0/24 (hosts): **http:// 192.168.3.1** (yes)

192.168.11.0/24 (hosts): c:\> **ftp://192.168.3.2**

Username **cisco**  Password **cisco**  (yes)

192.168.12.0/24 (hosts): **http:// 192.168.3.1**  (yes)

192.168.12.0/24 (hosts): c:\> **ftp://192.168.3.2**

Username **cisco**  Password **cisco**  (yes)

Click on *R1* icon and select *CLI* folder. Hit <enter> key for user prompt.

Step 1: Enter global configuration mode

R1> **enable**
Password: **cisconet**
R1# **configure terminal**

Step 2: Deny all traffic from hosts on VLAN 10 to server-1

R1(config)# **access-list 100 deny ip 192.168.10.0 0.0.0.255 host 192.168.3.1**

Step 3: Deny FTP traffic from hosts on VLAN 11 to server-2.

R1(config)# **access-list 100 deny tcp 192.168.11.0 0.0.0.255 host 192.168.3.2 eq ftp**

Step 4: Deny all traffic from hosts on VLAN 12 to server-1 and server-2.

R1(config)# **access-list 100 deny ip 192.168.12.0 0.0.0.255 any**

Step 5: Permit all traffic not matching on any previous ACL statements.

R1(config)# **access-list 100 permit ip any any**

Step 6: Apply ACL 100 outbound on R1 interface Fa1/0.

R1(config)# **interface fastethernet1/0**
R1(config-if)# **ip access-group 100 out**
R1(config-if)# **end**
R1# **copy running-config startup-config**

Step 7: Verify Lab

Verify ACL 100 configuration is correct with the following commands.

R1# **show running-config**

R1# **show access-lists**

Extended IP access list 100
    10 deny ip 192.168.10.0 0.0.0.255 host 192.168.3.1
    20 deny tcp 192.168.11.0 0.0.0.255 host 192.168.3.2 eq ftp
    30 deny ip 192.168.12.0 0.0.0.255 any
    40 permit ip any any

Confirm ACL 100 is working correctly with the following commands.

192.168.10.0/24 (hosts): c:\> **ping 192.168.3.1** (no)

192.168.10.0/24 (hosts): c:\> **ping 192.168.3.2** (yes)

192.168.11.0/24 (hosts): c:\> **ftp 192.168.3.2** (no)

192.168.11.0/24 (hosts): **http://192.168.3.1** (yes)

192.168.12.0/24 (hosts): c:\> **ping 192.168.3.1** (no)

192.168.12.0/24 (hosts): c:\> **ping 192.168.3.2** (no)