

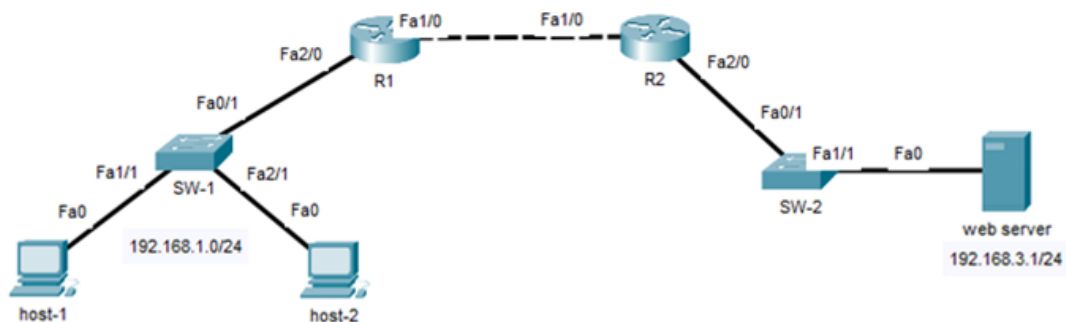
# Extended Named ACL

## Lab Summary

Configure a named access control list (ACL) to filter traffic based on the following requirements:

1. Configure a named ACL called **http-telnet-filter**
2. Add a remark that describes the purpose of the ACL
3. Deny all HTTP traffic from hosts on 192.168.1.0/24 subnets to web server
4. Deny Telnet sessions from hosts on 192.168.1.0/24 subnets to all routers
5. Permit all traffic not matching on any previous ACL statements
6. Apply the named ACL **http-telnet filter** inbound on R1 interface Fa2/0

**Figure 1** Lab Topology



## Lab Configuration

Start Packet Tracer File: **named acl.pkt**

Verify that there is web server and Telnet access permitted from host-1 and host-2.

host-1: **http://192.168.3.1** (yes)

host-1: c:\> **telnet 192.168.2.1** Password: *cisco* / Password: *cisconet* (yes)

host-1: c:\> **telnet 192.168.2.2** Password: *cisco* / Password: *cisconet* (yes)

host-2: **http://192.168.3.1** (yes)

host-2: c:\> **telnet 192.168.2.1** Password: *cisco* / Password: *cisconet* (yes)

host-2: c:\> **telnet 192.168.2.2** Password: *cisco* / Password: *cisconet* (yes)

Click on *R1* icon and select *CLI* folder.

Step 1: Enter global configuration mode

```
R1> enable  
R1# configure terminal
```

Step 2: Create a named ACL called *http-telnet-filter* and add a remark to explain.

```
R1(config)# ip access-list extended http-telnet-filter  
R1(config-ext-nacl)# remark deny access to web server and telnet
```

Step 3: Deny HTTP from hosts on 192.168.1.0/24 subnet to the web server

```
R1(config-ext-nacl)# deny tcp 192.168.1.0 0.0.0.255 host 192.168.3.1 eq  
www
```

Step 4: Deny Telnet sessions from hosts on 192.168.1.0/24 subnet to any router.

```
R1(config-ext-nacl)# deny tcp 192.168.1.0 0.0.0.255 any eq telnet
```

Step 5: Permit all traffic that does not match any previous ACL statements.

```
R1(config-ext-nacl)# permit ip any any  
R1(config-ext-nacl)# exit
```

Step 6: Apply the named ACL inbound on R1 interface Fa2/0 and save it to the running configuration.

```
R1(config)# interface fastethernet2/0  
R1(config-if)# ip access-group http-telnet-filter in  
R1(config-if)# end  
R1# copy running-config startup-config
```

Step 7: Verify Lab

Verify the ACL configuration is correct and enabled. Start the web browser from host-1 and host-2 and verify access to web server is permitted. Confirm there is no Telnet access permitted from hosts to any router. Telnet access is available from the routers. ACL is applied inbound on R1 and does not filter past that point.

```
R1# show running-config
```

```
R1# show access-lists
```

```
Extended IP access list http-telnet-filter
```

```
10 deny tcp 192.168.0.0 0.0.255.255 host 192.168.3.1 eq www  
20 deny tcp 192.168.0.0 0.0.255.255 any eq telnet  
30 permit ip any any
```

host-1: **http://192.168.3.1** (no)

host-1: c:\> **telnet 192.168.2.1** Password: *cisco* / Password: *cisconet* (no)

host-1: c:\> **telnet 192.168.2.2** Password: *cisco* / Password: *cisconet* (no)

host-1: c:\> **ftp 192.168.3.1** username: *cisco* / password: *cisco* (yes)

host-2: **http://192.168.3.1** (no)

host-2: c:\> **telnet 192.168.2.1** Password: *cisco* / Password: *cisconet* (no)

host-2: c:\> **telnet 192.168.2.2** Password: *cisco* / Password: *cisconet* (no)

host-2: c:\> **ftp 192.168.3.1** username: *cisco* / password: *cisco* (yes)

### Lab Notes

Apply any extended ACL near the source to filter packets immediately and minimize bandwidth usage. The **show access-lists** command is available for troubleshooting packet filtering that includes each statement per ACL and the specific order. The access control list (ACL) statements are numbered starting with 10 and verify how packet matching is occurring. Note as well that deleting a statement and adding a new statement will assign the ACL to the bottom of the list. That could then affect how packet matching is occurring and inadvertently permit/deny wrong traffic.