

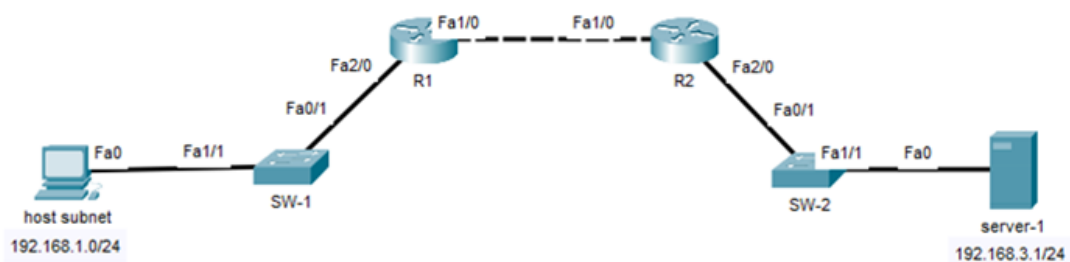
# Standard ACL

## Lab Summary

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

1. Configure a standard ACL and assign number 99
2. Deny all traffic from host subnet 192.168.1.0/24
3. Permit all other traffic that does not match ACL
4. Apply ACL inbound on R2 interface Fa1/0 to activate

**Figure 1** Lab Topology



## Lab Configuration

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

Verify there is application traffic access permitted from host subnet 192.168.1.0/24 to server-1 and R2 (telnet).

```
host: ping 192.168.3.1 (yes)
host: http://192.168.3.1 (yes)
host: c:\> telnet 192.168.2.2
Password: cisco (yes)
R2> enable
Password: cisco (yes)
```

Click on *R2* icon and select *CLI* folder.

Step 1: Enter global configuration mode

```
R2> enable
R2# configure terminal
```

Step 2: Create a standard numbered ACL to deny all traffic from host subnet 192.168.1.0/24.

```
R2(config)# access-list 99 deny 192.168.1.0 0.0.0.255  
R2(config)# access-list 99 permit any
```

Step 3: Apply standard ACL 99 inbound on R2 interface FastEthernet1/0.

```
R2(config)# interface fastEthernet1/0  
R2(config-if)# ip access-group 99 in  
R2(config-if)# end  
R2# copy running-config startup-config
```

Step 4: Verify Lab

Verify there is no traffic permitted from 192.168.1.0/24 host subnet to server-1.

host: c:/> **ping 192.168.3.1** (no)

Pinging 192.168.3.1 with 32 bytes of data:

Reply from 192.168.1.3: Destination host unreachable.

Reply from 192.168.1.3: Destination host unreachable.

Reply from 192.168.1.3: Destination host unreachable.

Reply from 192.168.1.3: Destination host unreachable.

Ping statistics for 192.168.3.1:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

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

Verify there is no traffic permitted from 192.168.1.0/24 host subnet to R2.

host: c:/> **ping 192.168.2.2** (no)

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.1.3: Destination host unreachable.

Reply from 192.168.1.3: Destination host unreachable.

Reply from 192.168.1.3: Destination host unreachable.

Reply from 192.168.1.3: Destination host unreachable.

Ping statistics for 192.168.2.2:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

```
host: c:\> telnet 192.168.2.2 (no)
```

```
Trying 192.168.2.2 ...
```

```
% Connection timed out; remote host not responding
```

### Lab Notes

There is no traffic or network connectivity permitted for host subnet 192.168.1.0/24 past R1. Standard ACL is applied near the destination to prevent excessive filtering since it is less specific than an extended ACL.

### **Standard Numbered ACL**

The number range is from 1-99 and 1300-1999. It is comprised of permit or deny statement/s from a source address with a wildcard mask only. The single deny statement requires that you add **permit any** as a last statement for **any** standard ACL or all packet are denied from all sources.

### **Standard Named ACL**

They are defined with a name instead of number and have the same rules as a standard ACL. The following ACL is named **internet** and will deny all traffic from all hosts connected to 192.168.1.0/24 subnet. It will log any packets that are denied.

```
ip access-list internet log  
deny 192.168.1.0 0.0.0.255  
permit any
```