**ACL Standard**

**Part 2: Configure Devices and Verify Connectivity**

1. **Configure OSPF routing on R1, ISP and R3**

Assign 1 as the OSPF process ID and advertise all networks on R1, ISP, and R3. The OSPF configuration for R1 and ISP is included for reference.

R1(config)# **router ospf 1**

R1(config-router)# **network 192.168.10.0 0.0.0.255 area 0**

R1(config-router)# **network 192.168.20.0 0.0.0.255 area 0**

R1(config-router)# **network 10.1.1.0 0.0.0.3 area 0**

ISP(config)# **router ospf 1**

ISP(config-router)# **network 209.165.200.224 0.0.0.31 area 0**

ISP(config-router)# **network 10.1.1.0 0.0.0.3 area 0**

ISP(config-router)# **network 10.2.2.0 0.0.0.3 area 0**

1. **Verify connectivity between devices**

**Part 3: Configure and Verify Standard Numbered and Named ACLs**

1. **Configure a numbered standard ACL**

Configure the ACL on R3. Use 1 for the access list number.

R3(config)# **access-list 1 remark Allow R1 LANs Access**

R3(config)# **access-list 1 permit 192.168.10.0 0.0.0.255**

R3(config)# **access-list 1 permit 192.168.20.0 0.0.0.255**

R3(config)# **access-list 1 deny any**

Apply the ACL to the appropriate interface in the proper direction.

R3(config)# **interface g0/1**

R3(config-if)# **ip access-group 1 out**

On R3, issue the **show access-lists 1** command.

R3# **show** **access-list 1**

Standard IP access list 1

10 permit 192.168.10.0, wildcard bits 0.0.0.255

20 permit 192.168.20.0, wildcard bits 0.0.0.255

30 deny any

On R3, issue the **show ip interface g0/1** command.

R3# **show ip interface g0/1**

GigabitEthernet0/1 is up, line protocol is up

Internet address is 192.168.30.1/24

Broadcast address is 255.255.255.255

Address determined by non-volatile memory

MTU is 1500 bytes

Helper address is not set

Directed broadcast forwarding is disabled

Multicast reserved groups joined: 224.0.0.10

Outgoing access list is 1

Inbound access list is not set

Output omitted

1. **Configure a named standard ACL**

Create the standard named ACL BRANCH-OFFICE-POLICY on R1.

R1(config)# **ip access-list standard BRANCH-OFFICE-POLICY**

R1(config-std-nacl)# **permit host 192.168.30.3**

R1(config-std-nacl)# **permit 192.168.40.0 0.0.0.255**

R1(config-std-nacl)# **end**

R1#

\*Feb 15 15:56:55.707: %SYS-5-CONFIG\_I: Configured from console by console

Apply the ACL to the appropriate interface in the proper direction.

R1# **config t**

R1(config)# **interface g0/1**

R1(config-if)# **ip access-group BRANCH-OFFICE-POLICY out**

Verify a named ACL.

* + - 1. On R1, issue the **show access-lists** command.

R1# **show** **access-lists**

Standard IP access list BRANCH-OFFICE-POLICY

10 permit 192.168.30.3

20 permit 192.168.40.0, wildcard bits 0.0.0.255

**Part 4: Modify a Standard ACL**

1. **Modify a named standard ACL**

From R1 privileged EXEC mode, issue a **show access-lists** command.

R1# **show access-lists**

Standard IP access list BRANCH-OFFICE-POLICY

10 permit 192.168.30.3 (8 matches)

20 permit 192.168.40.0, wildcard bits 0.0.0.255 (5 matches)

Add two additional lines at the end of the ACL. From global config mode, modify the ACL, BRANCH-OFFICE-POLICY.

R1#(config)# **ip access-list standard BRANCH-OFFICE-POLICY**

R1(config-std-nacl)# **30 permit 209.165.200.224 0.0.0.31**

R1(config-std-nacl)# **40 deny any**

R1(config-std-nacl)# **end**

Verify the ACL.

On R1, issue the **show access-lists** command.

R1# **show access-lists**

Standard IP access list BRANCH-OFFICE-POLICY

10 permit 192.168.30.3 (8 matches)

20 permit 192.168.40.0, wildcard bits 0.0.0.255 (5 matches)

30 permit 209.165.200.224, wildcard bits 0.0.0.31

40 deny any