**Step 6: Configure OSPF routing on R1, ISP, and R3.**

a. Assign 1 as the OSPF process ID and advertise all networks on R1, ISP, and R3. The OSPF

configuration for R1 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 209.165.201.0 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**

R3(config)# **router ospf 1**

R3(config-router)# **network 192.168.30.0 0.0.0.255 area 0**

R3(config-router)# **network 192.168.40.0 0.0.0.255 area 0**

R3(config-router)# **network 10.2.2.0 0.0.0.3 area 0**

**Part 2: Configure and Verify Extended Numbered and Named ACLs**

Extended ACLs can filter traffic in many different ways. Extended ACLs can filter on source IP addresses,

source ports, destination IP addresses, destination ports, as well as various protocols and services.

Security policies are as follows:

**1. Allow web traffic originating from the 192.168.10.0/24 network to go to any network.**

**2. Allow an SSH connection to the R3 serial interface from PC-A.**

**3. Allow users on 192.168.10.0/24 network access to 192.168.20.0/24 network.**

**4. Allow web traffic originating from the 192.168.30.0/24 network to access R1 via the web interface and the 209.165.200.224/27 network on ISP. The 192.168.30.0/24 network should NOT be allowed to access any other network via the web.**

In looking at the security policies listed above, you will need at least two ACLs to fulfill the security policies. A

best practice is to place extended ACLs as close to the source as possible. We will follow this practice for

these policies.

**Step 1: Configure a numbered extended ACL on R1 for security policy numbers 1 and 2.**

You will use a numbered extended ACL on R1. What are the ranges for extended ACLs? **100 – 199**

a. Configure the ACL on R1. Use 100 for the ACL number.

**R1(config)# access-list 100 remark Allow Web & SSH Access**

**R1(config)# access-list 100 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22**

**R1(config)# access-list 100 permit tcp any any eq 80**

What does the 80 signify in the command output listed above?

**80 is the destination port. TCP port 80 is a well-known port used for the HTTP protocol.**

To what interface should ACL 100 be applied?

**There are two possible answers here: G0/1 and S0/1/0. Placing it on G0/1 could block the users on network 192.168.10.0/24 from getting to any other LANs attached to R1 such as the 192.168.20.0/24 network. For this reason you will place it on S0/0/0.**

In what direction should ACL 100 be applied?

**If G0/1 interface was used for the previous answer, ACL 100 should be applied going in. If studentanswered with S0/0/0, ACL 100 would be applied going out.**

From the PC-A command prompt, issue a ping to 10.2.2.1. Explain your results.

**The pings failed. Message was “Reply from 192.168.10.1: Destination net unreachable.” This is**

**because of the implicit deny any at the end of every ACL. ACL 100 only allows out Web and SSH traffic.**

**Step 2: Configure a named extended ACL on R3 for security policy number 3.**

a. Configure the policy on R3. Name the ACL WEB-POLICY.

R3(config)# **ip access-list extended WEB-POLICY**

R3(config-ext-nacl)# **permit tcp 192.168.30.0 0.0.0.255 host 10.1.1.1 eq 80**

R3(config-ext-nacl)# **permit tcp 192.168.30.0 0.0.0.255 209.165.200.224 0.0.0.31 eq 80**

b. Apply ACL WEB-POLICY to the S0/0/1 interface.

R3(config-ext-nacl)# **interface S0/0/1**

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

c. Verify the ACL WEB-POLICY.

1) From R3 privileged EXEC mode command prompt, issue the **show ip interface s0/0/1** command.

What, if any, is the name of the ACL? **WEB-POLICY**

In what direction is the ACL applied? **Out**

From R3 privileged EXEC mode command prompt, issue the **show ip interface s0/0/1** command.

What, if any, is the name of the ACL? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ WEB-POLICY

In what direction is the ACL applied? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Out

2) Open up a web browser on PC-C and access http://209.165.200.225 (the ISP router). It should be

successful; troubleshoot, if not.

3) From PC-C, open a web session to http://10.1.1.1 (R1). It should be successful; troubleshoot, if not.

4) From PC-C, open a web session to http://209.165.201.1 (ISP router). It should fail; troubleshoot, if

not.

5) From a PC-C command prompt, ping PC-A. What was your result and why?

**The pings failed. Only web traffic is allowed to exit from the 192.168.30.0/24 network.**

**Part 3: Modify and Verify Extended ACLs**

Because of the ACLs applied on R1 and R3, no pings or any other kind of traffic is allowed between the LAN

networks on R1 and R3. Management has decided that all traffic between the 192.168.10.0/24 and

192.168.30.0/24 networks should be allowed. You must modify both ACLs on R1 and R3.

**Step 1: Modify ACL 100 on R1.**

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

How many lines are there in this access list? **2 lines, numbered 10 and line 20**

b. Enter global configuration mode and modify the ACL on R1.

R1(config)# **ip access-list extended 100**

R1(config-ext-nacl)# **30 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255**

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

c. Issue the **show access-lists** command.

Where did the new line that you just added appear in ACL 100? **Line 30. The last line in the ACL.**

**Step 2: Modify ACL WEB-POLICY on R3.**

a. From R3 privileged EXEC mode, issue the **show access-lists** command.

How many lines are there in this access list? **2 lines, numbered 10 and 20**

b. Enter global configuration mode and modify the ACL on R3.

R3(config)# **ip access-list extended WEB-POLICY**

R3(config-ext-nacl)# **30 permit ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255**

R3(config-ext-nacl)# **end**

c. Issue the **show access-lists** command to verify that the new line was added at the end of the ACL.

Where did the new line that you just added appear in ACL 100?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Line 30. The last line in the ACL.**

**Step 3: Verify modified ACLs.**

a. From PC-A, ping the IP address of PC-C. Were the pings successful? \_\_\_\_\_\_\_\_\_\_\_\_\_\_ Yes

b. From PC-C, ping the IP address of PC-A. Were the pings successful? \_\_\_\_\_\_\_\_\_\_\_\_\_\_ Yes

Why did the ACLs work immediately for the pings after you changed them?

**The ACLs on both R1 and R3 were still applied to their respective interfaces with the ip access-group command.**

**Las ACL en R1 y R3 todavía se aplicaron a sus respectivas interfaces con el comando ip access-group.**

**Reflection**

1. Why is careful planning and testing of ACLs required?

**ACLs can unintentionally block legitimate traffic from entering or leaving a network.**

**Las ACL pueden bloquear involuntariamente el tráfico legítimo para que no entre o salga de una red.**

2. Which type of ACL is better: standard or extended?

**They both have their purpose and place in a network.**

* **A standard ACL is easy to write and configure if you need to permit or deny all traffic. The downside of a standard ACL is that it can only check source addresses and has no granularity.**
* **Extended ACLs can be written to filter any kind of traffic generated. However, they can be complex to configure and understand.**

**Ambos tienen su propósito y su lugar en una red.**

**• Una ACL estándar es fácil de escribir y configurar si necesita permitir o denegar todo el tráfico. La desventaja de una ACL estándar es que solo puede verificar direcciones de origen y no tiene granularidad.**

**• Se pueden escribir ACL extendidas para filtrar cualquier tipo de tráfico generado. Sin embargo, su configuración y comprensión pueden resultar complejas.**