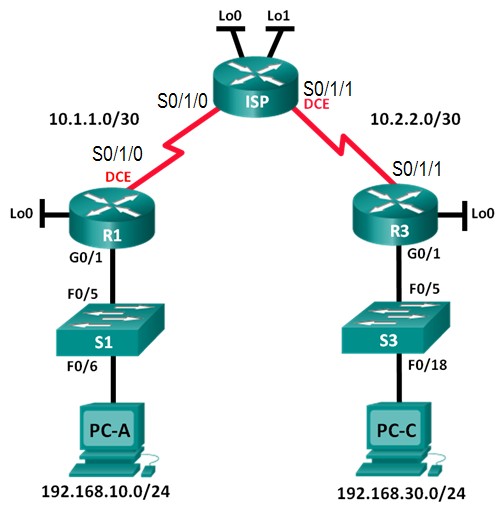


**Lab 9.3.2.13 – Configuring and Verifying Extended ACLs**

## Topology

**209.165.200.224 /27**

**209.165.201.0 /27**



**192.168.40.0 /24**

**192.168.20.0 /24**

**Addressing Table**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Subnet Mask** | **Default Gateway** |
| R1 | G0/1 | 192.168.10.1 | 255.255.255.0 | N/A |
|  | Lo0 | 192.168.20.1 | 255.255.255.0 | N/A |
|  | S0/1/0 (DCE) | 10.1.1.1 | 255.255.255.252 | N/A |
| ISP | S0/1/0 | 10.1.1.2 | 255.255.255.252 | N/A |
|  | S0/1/1 (DCE) | 10.2.2.2 | 255.255.255.252 | N/A |
|  | Lo0 | 209.165.200.225 | 255.255.255.224 | N/A |
|  | Lo1 | 209.165.201.1 | 255.255.255.224 | N/A |
| R3 | G0/1 | 192.168.30.1 | 255.255.255.0 | N/A |
|  | Lo0 | 192.168.40.1 | 255.255.255.0 | N/A |
|  | S0/1/1 | 10.2.2.1 | 255.255.255.252 | N/A |
| S1 | VLAN 1 | 192.168.10.11 | 255.255.255.0 | 192.168.10.1 |
| S3 | VLAN 1 | 192.168.30.11 | 255.255.255.0 | 192.168.30.1 |
| PC-A | NIC | 192.168.10.3 | 255.255.255.0 | 192.168.10.1 |
| PC-C | NIC | 192.168.30.3 | 255.255.255.0 | 192.168.30.1 |

**Objectives**

**Part 1: Configure Devices and Verify Connectivity**

* Configure basic settings on PCs, routers, and switches.
* Configure OSPF routing on R1, ISP, and R3.

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

* Configure, apply, and verify a numbered extended ACL.
* Configure, apply, and verify a named extended ACL.

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

**Background / Scenario**

Extended access control lists (ACLs) are extremely powerful. They offer a much greater degree of control than standard ACLs as to the types of traffic that can be filtered, as well as where the traffic originated and where it is going.

In this lab, you will set up filtering rules for two offices represented by R1 and R3. Management has established some access policies between the LANs located at R1 and R3, which you must implement. The ISP router between R1 and R3 does not have any ACLs placed on it. You would not be allowed any administrative access to an ISP router as you can only control and manage your own equipment.

## Required Resources

* 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
* 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
* 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)

**Part 1: Configure Devices and Verify Connectivity**

In Part 1, you will configure basic settings on the routers, switches, and PCs. Refer to the Topology and Addressing Table for device names and address information.

### Step 1: Configure IP addresses on PC-A and PC-C.

**Step 2: Configure basic settings on R1.**

1. Disable DNS lookup.
2. Configure the device name as shown in the topology.
3. Create a loopback interface on R1.
4. Configure interface IP addresses as shown in the Topology and Addressing Table.
5. Configure a privileged EXEC mode password of **class**.
6. Assign a clock rate of **128000** to the S0/0/0 interface.
7. Assign **cisco** as the console and vty password and enable Telnet access. Configure **logging synchronous** for both the console and vty lines.

**Step 3: Configure basic settings on ISP.**

1. Configure the device name as shown in the topology.
2. Create the loopback interfaces on ISP.
3. Configure interface IP addresses as shown in the Topology and Addressing Table.
4. Disable DNS lookup.
5. Assign **class** as the privileged EXEC mode password.
6. Assign a clock rate of **128000** to the S0/0/1 interface.

g. Assign **cisco** as the console and vty password and enable Telnet access. Configure **logging synchronous** for both console and vty lines.

**Step 4: Configure basic settings on R3.**

1. Configure the device name as shown in the topology.
2. Create a loopback interface on R3.
3. Configure interface IP addresses as shown in the Topology and Addressing Table.
4. Disable DNS lookup.
5. Assign **class** as the privileged EXEC mode password.
6. Assign **cisco** as the console password and configure **logging synchronous** on the console line.
7. Enable **SSH** on **R3**.

R3(config)# **ip domain-name cisco.com**

R3(config)# **username admin privilege 15 secret class**

R3(config)# **crypto key generate rsa**

**Press enter and then type the value of 1024**

R3(config)# **line vty 0 4**

R3(config-line)# **login local**

R3(config-line)# **transport input ssh**

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

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

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 area 0**

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

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

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

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

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

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

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

### Step 7: Verify connectivity between devices.

**Note**: It is very important to verify connectivity **before** you configure and apply ACLs! Ensure that your network is properly functioning before you start to filter out traffic.

1. From **PC-A**, ping **PC-C** and **the loopback** and **serial** interfaces on **R3**.

Were your pings successful? \_\_\_\_\_\_\_\_

b. From **R1**, ping **PC-C** and the **loopback** and **serial** interface on **R3**.

Were your pings successful? \_\_\_\_\_\_\_\_

c. From **PC-C**, ping **PC-A** and the **loopback** and **serial** interface on **R1**.

Were your pings successful? \_\_\_\_\_\_\_\_

d. From **R3**, ping **PC-A** and the **loopback** and **serial** interface on **R1**.

Were your pings successful? \_\_\_\_\_\_\_\_

e. From **PC-A**, ping the **loopback interfaces** on the **ISP** router.

Were your pings successful? \_\_\_\_\_\_\_\_

f. From **PC-C**, ping the **loopback interfaces** on the **ISP** router.

Were your pings successful? \_\_\_\_\_\_\_\_

# 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, 2 and 3.

You will use a **numbered extended ACL** on **R1**. What are the ranges for **extended ACLs**?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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?

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

To what interface should **ACL 100** be applied?

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

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

In what direction should **ACL 100** be applied?

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

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

1. Apply ACL 100 to the S0/0/0 interface.

R1(config)# **interface s0/0/0**

R1(config-if)# **ip access-group 100 out**

1. Verify ACL 100.
2. Establish an **SSH connection** from **PC-A** to **R3** using **10.2.2.1** for the IP address. Log in with **admin** and **class** for your credentials. It should be successful; troubleshoot, if not.

On **PC-A**, execute de following command in the CLI: **ssh -l admin 10.2.2.1**

Password: **class**

1. From privileged EXEC mode prompt on **R1**, issue the **show access-lists** command.

R1# **show access-lists**

Extended IP access list 100

10 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22 (22 matches)

20 permit tcp any any eq www (111 matches)

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

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

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

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

### Step 2: Configure a named extended ACL on R3 for security policy number 4.

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 S0/1/1 interface.

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

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 s0/1/1** command.

What, if any, is the name of the ACL?

In what direction is the ACL applied?

1. From a **PC-C** command prompt, **ping** to [209.165.200.225](http://209.165.200.225/) (the **Lo0** of the **ISP router**). It should be fail.
2. From a **PC-C** command prompt, **ping** to [10.1.1.1](http://10.1.1.1/) (**R1**). It should be fail.
3. From a **PC-C** command prompt, **ping** to [209.165.201.1](http://209.165.201.1/) **(ISP router**). It should be fail.
4. From a **PC-C** command prompt, **ping** 192.168.10.3 **(PC-A)**. What was your result and why?

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

1. From a **PC-A** command prompt, **ping** to [209.165.200.225](http://209.165.200.225/) (the **Lo0** of the **ISP router**). It should be fail
2. From a **PC-A** command prompt, **ping** to [209.165.201.1](http://209.165.201.1/) (**ISP router**). It should be fail
3. From a **PC-A** command prompt, ping to [10.1.1.1](http://10.1.1.1/) (R1). It should be successful; troubleshoot, if not.

# 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?

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**?

**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?

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.

**Step 3: Verify modified ACLs.**

1. From **PC-A**, ping the IP address of 192.168.30.3 **(PC-C)**. Were the pings successful?
2. From **PC-C**, ping the IP address of 192.168.10.3 **(PC-A)**. Were the pings successful?

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

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

**Reflection**

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

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