



COE 371L

Computer Networks I

Fall 2019

Lab #9

Section #2

Title: Configuring and Verifying Standard IPv4 ACLs

9.5/10

Name : Amir Mohideen, Zayed Mohamed

ID: 74559, 75771

Lab – Configuring and Verifying Standard IPv4 ACLs

1. Set Up the Topology and Initialize Devices

In Part 1, you set up the network topology and clear any configurations, if necessary.

* 1. Cable the network as shown in the topology.
  2. Initialize and reload the routers and switches.

1. Configure Devices and Verify Connectivity
   1. Configure IP addresses on PC-A and PC-C.
   2. Configure basic settings for the routers.
   3. (Optional) Configure basic settings on the switches.
   4. Configure Rip routing on R1, ISP, and R3.
      1. Configure RIP version 2 and advertise all networks on R1, ISP, and R3. The RIP configuration for R1 and ISP is included for reference.

R1(config)# **router rip**

R1(config-router)# **version 2**

R1(config-router)# **network 192.168.10.0**

R1(config-router)# **network 192.168.20.0**

R1(config-router)# **network 10.1.1.0**

ISP(config)# **router rip**

ISP(config-router)# **version 2**

ISP(config-router)# **network 209.165.200.224**

ISP(config-router)# **network 10.1.1.0**

ISP(config-router)# **network 10.2.2.0**

**[Report – 2Pts] RIP configuration on router R3**

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

* + 1. After configuring Rip on R1, ISP, and R3, verify that all routers have complete routing tables, listing all networks. Troubleshoot if this is not the case.
  1. Verify connectivity between devices.

1. Configure and Verify Standard Numbered and Named ACLs
   1. Configure a numbered standard ACL.

Standard ACLs filter traffic based on the source IP address only. A typical best practice for standard ACLs is to configure and apply it as close to the destination as possible. For the first access list, create a standard numbered ACL that allows traffic from all hosts on the 192.168.10.0/24 network and all hosts on the 192.168.20.0/24 network to access all hosts on the 192.168.30.0/24 network. The security policy also states that a **deny any** access control entry (ACE), also referred to as an ACL statement, should be present at the end of all ACLs.

**[Report – 1Pts]** What wildcard mask would you use to allow all hosts on the 192.168.10.0/24 network to access the 192.168.30.0/24 network?

0.0.0.255

**[Report – 1Pts]** Following Cisco’s recommended best practices, on which router would you place this ACL?

R3

**[Report – 1Pts]** On which interface would you place this ACL? In what direction would you apply it?

Both Gigabit 0/1 and ACL applied when exiting.

* + 1. Configure the ACL on R3. Use 1 for the access list number.
    2. Apply the ACL to the appropriate interface in the proper direction.
    3. Verify a numbered ACL.

The use of various **show** commands can aid you in verifying both the syntax and placement of your ACLs in your router.

**[Report – 1Pts]** To see access list 1 in its entirety with all ACEs, which command would you use?

R3# show access-lists

**[Report – 1Pts]** What command would you use to see where the access list was applied and in what direction?

R3# show ip interface

* + 1. **[Report – 2Pts]** From the R1 prompt, ping PC-C’s IP address again.

R1# **ping 192.168.30.3**

Was the ping successful? Why or why not?

Pinging was not successful as the closest interface to the source address is being used. The source address is 10.1.1.1 but the access addresses only include 192.168.10.0 and 192.168.20.0

* 1. Configure a named standard ACL.

Create a named standard ACL that conforms to the following policy: allow traffic from all hosts on the 192.168.40.0/24 network access to all hosts on the 192.168.10.0/24 network. Also, only allow host PC-C access to the 192.168.10.0/24 network. The name of this access list should be called BRANCH-OFFICE-POLICY.

**[Report – 1Pts]** Following Cisco’s recommended best practices, on which router would you place this ACL? R1

**[Report – 1Pts]** On which interface would you place this ACL? In what direction would you apply it?

G0/1, should be applied while exiting

* + 1. Create the standard named ACL BRANCH-OFFICE-POLICY on R1.

**[Report – 1Pts]** Looking at the first permit ACE in the access list, what is another way to write this?

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

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

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

R1(config-std-nacl)# end

R1 (config-std-nacl)# permit 192.168.30.3 0.0.0.0

* + 1. 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

* + 1. 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

**[Report – 2Pts]** Is there any difference between this ACL on R1 with the ACL on R3? If so, what is it?

Yes, there is a difference. On R3 there is an extra ACE but it is not an issue since every ACL implements a deny any statement by default.

1. Modify a Standard ACL
   1. Modify a named standard ACL.
      1. From R1 privileged EXEC mode, issue a **show access-lists** command.
      2. Add two additional lines at the end of the ACL. From global config mode, modify the ACL, BRANCH-OFFICE-POLICY.
      3. Verify the ACL.
         1. On R1, issue the **show access-lists** command.

**[2Pt]** Do you have to apply the BRANCH-OFFICE-POLICY to the G0/1 interface on R1?

No, because the ip access group branch policy is still in the G0/1 interface

[Report – 4Pts] Reflection 3/4

* 1. As you can see, standard ACLs are very powerful and work quite well. Why would you ever have the need for using extended ACLs?

When filtering is done based on the source address, we need to use extended ACLs since standard ACLs are restricted. Moreover, they either allow or deny every protocol and service. One more thing to mention is that although extended ACLs are harder to implement, they are more suitable for complex networks.

* 1. Typically, more typing is required when using a named ACL as opposed to a numbered ACL. Why would you choose named ACLs over numbered?

A named ACL is preferred over numbered because we can document ACL with names in this type of ACL

Usingnamed ACLs gives you the ability to modify specific lines within the ACL itself, without retyping the whole thing