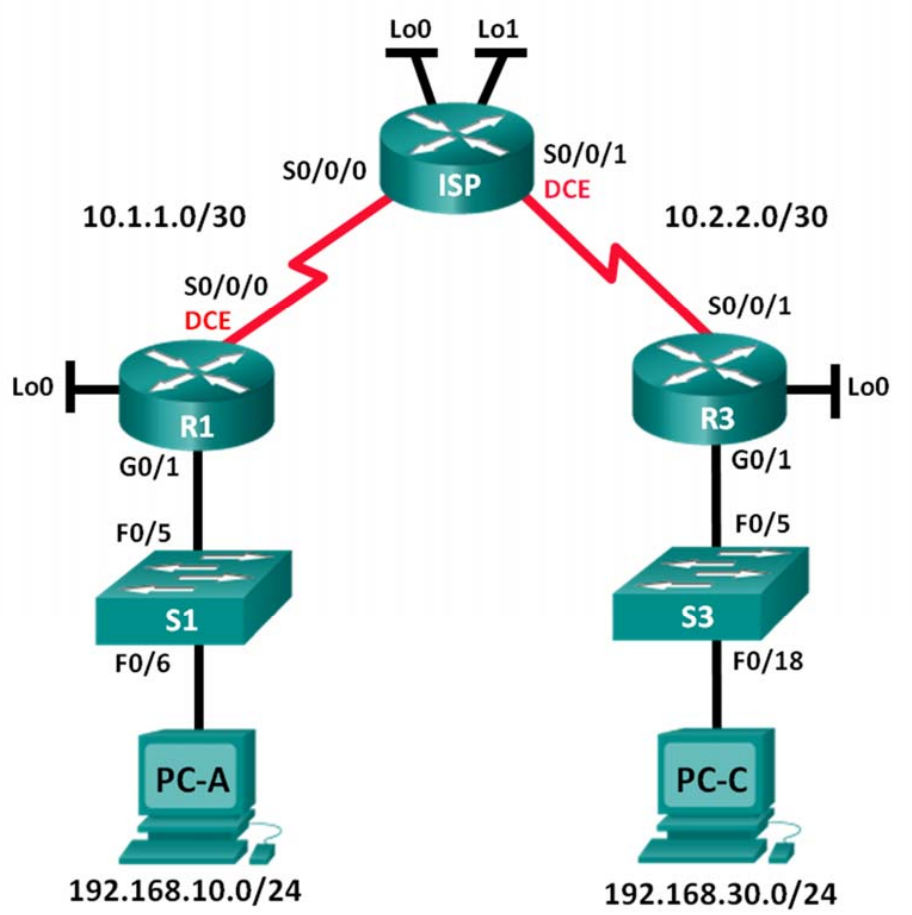
Lab 6a – Configuring and Verifying Standard IPv4 ACLs

Topology



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
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
ISP	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (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
	S0/0/1	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: Set Up the Topology and Initialize Devices

- Set up equipment to match the network topology.
- Initialize and reload the routers and switches.

Part 2: Configure Devices and Verify Connectivity

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

Part 3: Configure and Verify Standard Numbered and Named ACLs

- Configure, apply, and verify a numbered standard ACL.
- Configure, apply, and verify a named ACL.
- Modify and verify a named standard ACL.
- Test the ACL.
- Modify and verify a named standard ACL.
- Test the ACL.

Background / Scenario

Network security is an important issue when designing and managing IP networks. The ability to configure proper rules to filter packets, based on established security policies, is a valuable skill.

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.

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

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Part 1: Set Up the Topology and Initialize Devices

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

Step 1: Cable the network as shown in the topology.

Step 2: Initialize and reload the routers and switches.

Part 2: Configure Devices and Verify Connectivity

In Part 2, 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.

- Disable DNS lookup.
- Configure the device name as shown in the topology.
- Create a loopback interface on R1.
- Configure interface IP addresses as shown in the Topology and Addressing Table.
- Configure a privileged EXEC mode password of **class**.
- Assign a clock rate of **128000** to the S0/0/0 interface.
- Assign **cisco** as the console and vty password and enable Telnet access. Configure **logging synchronous** for both the console and vty lines.
- Enable web access on R1 to simulate a web server with local authentication for user **admin**.

```
R1(config)# ip http server
R1(config)# ip http authentication local
R1(config)# username admin privilege 15 secret class
```

Step 3: Configure basic settings on ISP.

- Configure the device name as shown in the topology.
- Create the loopback interfaces on ISP.
- Configure interface IP addresses as shown in the Topology and Addressing Table.
- Disable DNS lookup.

- Assign **class** as the privileged EXEC mode password.
- Assign a clock rate of **128000** to the S0/0/1 interface.
- Assign **cisco** as the console and vty password and enable Telnet access. Configure **logging synchronous** for both console and vty lines.
- Enable web access on the ISP. Use the same parameters as in Step 2.

Step 4: Configure basic settings on R3.

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

```
R3(config)# ip domain-name cisco.com
R3(config)# crypto key generate rsa modulus 1024
R3(config)# line vty 0 4
R3(config-line)# login local
R3(config-line)# transport input ssh
```

- Enable web access on R3. Use the same parameters as in Step 2.

Step 5: Configure basic settings on S1 and S3.

- Configure the hostnames as shown in the topology.
- Disable DNS lookup.
- Assign **cisco** as the console password.
- Configure a privileged EXEC mode password of **class**.
- Configure the management interface IP addresses as shown in the Topology and Addressing Table.
- Configure a default gateway address.

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

- Configure RIP version 2 and advertise all networks on R1, ISP, and R3. The RIPv2 configuration for R1 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
```

- 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.

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.

- From PC-A, ping PC-C and the loopback and serial interfaces on R3.
- From R1, ping PC-C and the loopback and serial interface on R3.
- From PC-C, ping PC-A and the loopback and serial interface on R1.
- From R3, ping PC-A and the loopback and serial interface on R1.

Part 3: Configure and Verify Standard Numbered and Named ACLs

Step 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.

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?

.....

Following Cisco's recommended best practices, on which router would you place this ACL? .....

On which interface would you place this ACL? In what direction would you apply it?

.....

.....

- 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
```

- 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.

  To see access list 1 in its entirety with all ACEs, which command would you use?

  .....

  What command would you use to see where the access list was applied and in what direction?

  .....

- 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
```

- Test the ACL to see if it allows traffic from the 192.168.10.0/24 network access to the 192.168.30.0/24 network. From the PC-A command prompt, ping the PC-C IP address. Were the pings successful? .....
- Test the ACL to see if it allows traffic from the 192.168.20.0/24 network access to the 192.168.30.0/24 network. You must do an extended ping and use the loopback 0 address on R1 as your source. Ping PC-C's IP address. Were the pings successful? .....

```
R1# ping
Protocol [ip]:
Target IP address: 192.168.30.3
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.20.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.3, timeout is 2 seconds:
Packet sent with a source address of 192.168.20.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
```

- 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?

.....

.....

Step 2: 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.

Following Cisco's recommended best practices, on which router would you place this ACL? .....

On which interface would you place this ACL? In what direction would you apply it?

.....

- 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
```

Looking at the first permit ACE in the access list, what is another way to write this?

.....

- 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
```

Step 3: Verify a named 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
    20 permit 192.168.40.0, wildcard bits 0.0.0.255
```

Is there any difference between this ACL on R1 with the ACL on R3? If so, what is it?

.....

.....

- Test the ACL. From the command prompt on PC-C, ping PC-A's IP address. .....
- Test the ACL to ensure that only the PC-C host is allowed access to the 192.168.10.0/24 network. You must do an extended ping and use the G0/1 address on R3 as your source. Ping PC-A's IP address. Were the pings successful? .....
- Test the ACL to see if it allows traffic from the 192.168.40.0/24 network access to the 192.168.10.0/24 network. You must perform an extended ping and use the loopback 0 address on R3 as your source. Ping PC-A's IP address. Were the pings successful? .....

Step 4: Modify a Standard ACL

It is common in business for security policies to change. For this reason, ACLs may need to be modified. In this step, you will change one of the previous ACLs you configured, to match a new management policy being put in place.

Management has decided that users from the 209.165.200.224/27 network should be allowed full access to the 192.168.10.0/24 network. Management also wants ACLs on all of their routers to follow consistent rules. A **deny any** ACE should be placed at the end of all ACLs. You must modify the BRANCH-OFFICE-POLICY ACL.

You will add two additional lines to this ACL. There are two ways you could do this:

OPTION 1: Issue a **no ip access-list standard BRANCH-OFFICE-POLICY** command in global configuration mode. This would effectively take the whole ACL out of the router. Depending upon the router IOS, one of the following scenarios would occur: all filtering of packets would be cancelled and all packets would be allowed through the router; or, because you did not take off the **ip access-group** command on the G0/1 interface, filtering is still in place. Regardless, when the ACL is gone, you could retype the whole ACL, or cut and paste it in from a text editor.

OPTION 2: You can modify ACLs in place by adding or deleting specific lines within the ACL itself. This can come in handy, especially with ACLs that have many lines of code. The retyping of the whole ACL or cutting and pasting can easily lead to errors. Modifying specific lines within the ACL is easily accomplished.

Note: For this lab, use Option 2.

Step 5: 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
```

Step 6: 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
```

Do you have to apply the BRANCH-OFFICE-POLICY to the G0/1 interface on R1?

.....

.....

- From the ISP command prompt, issue an extended ping. Test the ACL to see if it allows traffic from the 209.165.200.224/27 network access to the 192.168.10.0/24 network. You must do an extended ping and use the loopback 0 address on ISP as your source. Ping PC-A's IP address. .....

Reflection

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

   .....

   .....

   .....

2. Why are the RIP routing updates not blocked by the implicit **deny any** access control entry (ACE) or ACL statement of the ACLs applied to R1 and R3?

   .....

   .....

   .....