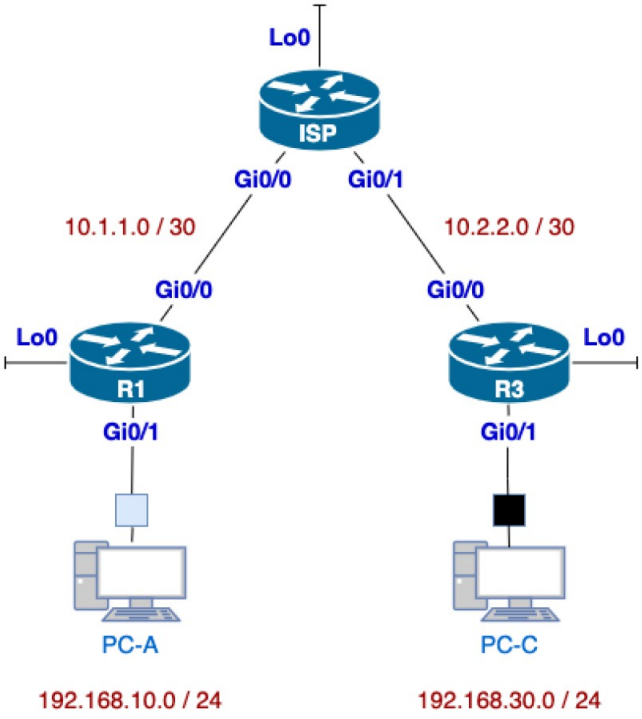
Lab 8 – Configuring and Verifying Standard IPv4 ACLs

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Gi0/1	192.168.10.1	255.255.255.0	N/A
	Lo0	192.168.20.1	255.255.255.0	N/A
	Gi0/0	10.1.1.1	255.255.255.252	N/A
ISP (R2)	Gi0/0	10.1.1.2	255.255.255.252	N/A
	Gi0/1	10.2.2.2	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
R3	Gi0/1	192.168.30.1	255.255.255.0	N/A
	Lo0	192.168.40.1	255.255.255.0	N/A
	Gi0/0	10.2.2.1	255.255.255.252	N/A
PC-A	NIC	192.168.10.3	255.255.255.0	?
PC-C	NIC	192.168.30.3	255.255.255.0	?

In-Lab Marks:
[1 mark] Demo your ability to change any match-counter for the named ACL (Part 3, Step 2c.5)
[1 mark] Demo your ability to change any match-counter for the modified Named ACL (Part 4, Step 1c.3)

The pre-lab is worth **20%**, the in-lab is worth **40%**, and the post-lab is worth **40%** of this lab.

© 2022 Cisco. Adapted for 22F- NET2000 by C. Ayala and M. Anderson

Objectives

Part 1: Set Up the Topology and Initialize Devices

Part 2: Configure Devices and Verify Connectivity

- Assign a static IP address to PCs.
- Configure basic settings on routers.
- Configure OSPF routing on R1, ISP, and R3.
- Verify connectivity between devices.

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.

Part 4: Modify a Standard 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.

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 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 have been erased and have no startup configurations.

Note: Work in pairs for this entire lab.

Part1: Set Up the Topology and Initialize Devices

Set up the network topology and clear any configurations, if necessary.

Part2: Configure Devices and Verify Connectivity

In Part 2, you 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 for the routers.

a. Console into the router and enter global configuration mode.

b. Use notepad or another editor to modify your basic configuration from previous labs: you'll need to adjust interface names (including loopbacks), IP addresses to match the topology for this lab. Ensure Telnet access is properly configured.

c. Copy the edited configurations to each device. Be sure you **watch the console** to spot any errors; correct the configuration as required.

© 2022 Cisco. Adapted for 22F- NET2000 by C. Ayala and M. Anderson

Step 3: Verify connectivity between devices.

Note: It is very important to test whether connectivity is working **before** you configure and apply access lists! You want to ensure that your network is properly functioning before you start to filter traffic.
ALL pings should be successful.

a. From PC-A, ping PC-C and the loopback interface on R3.

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

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

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

Part3: 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.

When planning ACLs, keep in mind:

- What wildcard mask would you use to allow all the required hosts?
- On which router would you place the ACL?
- On which interface would place the ACL? On which direction (in, out) would you apply it?

a. 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
```

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

```
R3(config)# interface g0/1
R3(config-if)# ip access-group 1 out
```

c. 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.

1) 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
```

© 2022 Cisco. Adapted for 22F- NET2000 by C. Ayala and M. Anderson

2) 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
```

3) 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. The ping should succeed.

4) 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. The ping should be 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
```

d. From the R1 prompt, ping PC-C's IP address again.

```
R1# ping 192.168.30.3
```

The ping will fail. When you ping from the router, it uses the closest interface to the destination as its source address. The pings had a source address of 10.1.1.1. The access list on R3 only allows the 192.168.10.0/24 and the 192.168.20.0/24 networks access.

© 2022 Cisco. Adapted for 22F- NET2000 by C. Ayala and M. Anderson

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.

Plan your ACL:

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

a. 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)# deny any
R1(config-std-nacl)# end
```

b. 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
```

c. Verify a named ACL.

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

```
R1# show ip 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
    30 deny   any
```

2) On R1, issue the **show ip interface g0/1** command.

```
R1# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.10.1/24
  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 BRANCH-OFFICE-POLICY
  Inbound access list is not set
<Output omitted>
```

3) Test the ACL. From the command prompt on PC-C, ping PC-A's IP address. Pings should succeed.

© 2022 Cisco. Adapted for 22F- NET2000 by C. Ayala and M. Anderson

4) 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. Pings should fail.
Monitor the ACL counters using '*show ip access-lists*' between successive pings. Which statement counter is increasing?

5) 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. Pings should succeed.
Monitor the ACL counters using '*show ip access-lists*' between successive pings. Which statement counter is increasing

Part4: Modify a Standard ACL

It is common in business for security policies to change. For this reason, ACLs may need to be modified. In Part 4, 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 1: Modify a named standard ACL.

a. From R1 privileged EXEC mode, display the full ACL with statement numbering using **show access-lists**:

```
R1# show ip 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 deny   any
```

b. Add two additional lines at the end of the ACL. From global config mode, modify the ACL, BRANCH-OFFICE-POLICY. To keep the ordering as required, the concluding *deny any* will need to be deleted & re-added.

```
R1#(config)# ip access-list standard BRANCH-OFFICE-POLICY
R1(config-std-nacl)# no 30 deny any
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
```

© 2022 Cisco. Adapted for 22F- NET2000 by C. Ayala and M. Anderson

c. Verify the 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 (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
    999 deny   any
```

Q. Do you have to (re-)apply the BRANCH-OFFICE-POLICY to the G0/1 interface on R1?

2) 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 to access 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.
The pings should succeed.

3) On R1, re-issue the '*show access-lists*' command between successive pings to see which counters have changed.

Reflection

(Preferably done during the lab session, time permitting.)

Q. For each ping test, can you identify exactly why the ping did or did not succeed? Be sure you understand since you'll **need** to know this for further lab work on extended and IPv6 ACLs.

Q. In the *sample* outputs above, are the ACL counters necessarily correct for each of the matching statements?

Q. Is there a difference in the output between 'show access-lists' for numbered ACLs and 'show **ip** access-lists' for named ACLs, or can you use them interchangeably?

Q. Which IOS commands *completely ignored* comment (*remark*) statements, and which ones include them? Don't forget to test & compare with *show run*.
(Many would say that unfortunately Cisco's treatment of ACL comments isn't entirely consistent!)

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

Q. How long should it take you to redo the config and cross-check your results using PT with 2911 routers?
A challenge: try it and actually time yourself. Fortunately PT does an excellent job of simulating IPv4 ACLs.

© 2022 Cisco. Adapted for 22F- NET2000 by C. Ayala and M. Anderson