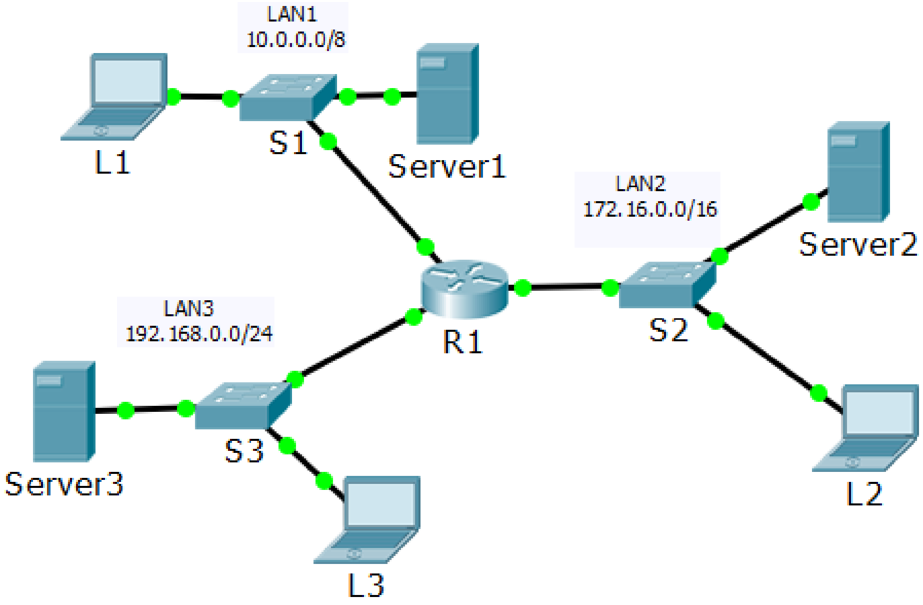
Packet Tracer – Troubleshooting Standard IPv4

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	10.0.0.1	255.0.0.0	N/A
	G0/1	172.16.0.1	255.255.0.0	N/A
	G0/2	192.168.0.1	255.255.255.0	N/A
Server1	NIC	172.16.255.254	255.255.0.0	172.16.0.1
Server2	NIC	192.168.0.254	255.255.255.0	192.168.0.1
Server3	NIC	10.255.255.254	255.0.0.0	10.0.0.1
L1	NIC	172.16.0.2	255.255.0.0	172.16.0.1
L2	NIC	192.168.0.2	255.255.255.0	192.168.0.1
L3	NIC	10.0.0.2	255.0.0.0	10.0.0.1

Objectives

Part 1: Troubleshoot ACL Issue 1

Part 2: Troubleshoot ACL Issue 2

Part 3: Troubleshoot ACL Issue 3

Scenario

This network is meant to have the following three policies implemented:

1. Do not allow hosts from the LAN1 (10.0.0.0/8) network access to the LAN2 (172.16.0.0/16) network. Permit all other access.
2. Do not allow host L2 in LAN2 (172.16.0.0/16) network access to the LAN3 (192.168.0.0/24). Permit all other access.
3. Only permit host L3 in LAN3 (192.168.0.0/24) network access to the LAN1 (10.0.0.0/8).

No other restrictions should be in place. Unfortunately, the rules that have been implemented are not working correctly. Your task is to find and fix the errors related to the access lists on **R1**.

Note: To attain full marks in this lab, it is best to remove and re-enter ACLs. It is also best to remove and re-enter any invalid **ip access-group** command.

Part 1: Troubleshoot ACL Issue 1

Do not allow hosts from the LAN1 (10.0.0.0/8) network access to LAN2 (172.16.0.0/16) network. Permit all other access. This is not currently the case.

Step 1: Determine the ACL problem.

As you perform the following tasks, compare the results to what you would expect from the ACL.

a. Using **L1**, open the Command Prompt and ping Server2 using the **ping –t 172.16.255.254** command. As expected, the pings should not be successful. However, hosts in LAN3 should be able to access LAN2.

b. Using **L3**, open the Command Prompt and ping Server2. The pings should be successful.

c. View the running configuration on **R1**. Examine access list **DENY-LAN1** ACL and its placement on the interfaces. Is there any statement in the list that permits or denies traffic to other networks? Are the statements in the correct order? Is the access list configured on the correct interface and in the correct direction?

d. Perform other tests, as necessary.

Step 2: Implement a solution.

Make the necessary adjustments to the **DENY-LAN1** ACL or to its placement, to fix the problem.

Step 3: Verify that the problem is resolved and document the solution.

If the problem is resolved, document the solution; otherwise return to Step 1.

Using the comand show access-lists i found out that the item in the list DENY-LAN1 is not correct. Replace "deny any" with "permit any".

Part 2: Troubleshoot ACL Issue 2

Do not allow host L2 in LAN2 (172.16.0.0/16) network access to the LAN3 (192.168.0.0/24). Permit all other access. This is not currently the case.

Step 1: Determine the ACL problem.

As you perform the following tasks, compare the results to what you would expect from the ACL.

a. Using **L2**, open the Command Prompt and ping Server3 using the **ping –t 192.168.0.254** command. The pings should not be successful. However, other hosts in LAN2 should be able to access LAN3.

b. Using **Server2**, open the Command Prompt and ping Server3. The pings should be successful.

c. View the running configuration on **R1**. Examine access list **DENY-L2** ACL and its placement on the interfaces. Is there any statement in the list that permits or denies traffic to other networks? Are the statements in the correct order? Is the access list configured on the correct interface and in the correct direction?

d. Perform other tests, as necessary.

Step 2: Implement a solution.

Make the necessary adjustments to the **DENY-L2** ACL or to its placement, to fix the problem.

Step 3: Verify that the problem is resolved and document the solution.

If the problem is resolved, document the solution; otherwise return to Step 1.

Using the comand show access-lists i found out that the order of items in the list DENY-L2 is not correct. "deny host 172.16.0.2" should come first, then "permit any"

Part 3: Troubleshoot ACL Issue 3

Only permit host L3 in LAN3 (192.168.0.0/24) network access to the LAN1 (10.0.0.0/8). This is not currently the case.

Step 1: Determine the ACL problem.

As you perform the following tasks, compare the results to what you would expect from the ACL.

a. Using **L3**, open the Command Prompt and ping L1 using the **ping –t 10.0.0.2** command. The pings should be successful.

b. Using **Server3**, open the Command Prompt and ping L1. The pings should not be successful.

c. View the running configuration on **R1**. Examine access list **PERMIT-L3** ACL and its placement on the interfaces. Is there any statement in the list that permits or denies traffic to other networks? Are the statements in the correct order? Is the access list configured on the correct interface and in the correct direction?

d. Perform other tests, as necessary.

Step 2: Implement a solution.

Make the necessary adjustments to the **PERMIT-L3** ACL or to its placement, to fix the problem.

Step 3: Verify that the problem is resolved and document the solution.

If the problem is resolved, document the solution; otherwise return to Step 1.

Using the comand show running-config i found out that list PERMIT-L3 is assigned with option in. It should be assigned with option out.

Part 4: Reflection

Access-lists pose a logical problem which often has more than one solution. Can you think of a different set of rules or placements that would yield the same required access filtering?

We could change rules the way that these access-lists should be assigned to networks with option "in", but that would require more rules and would be redundant.