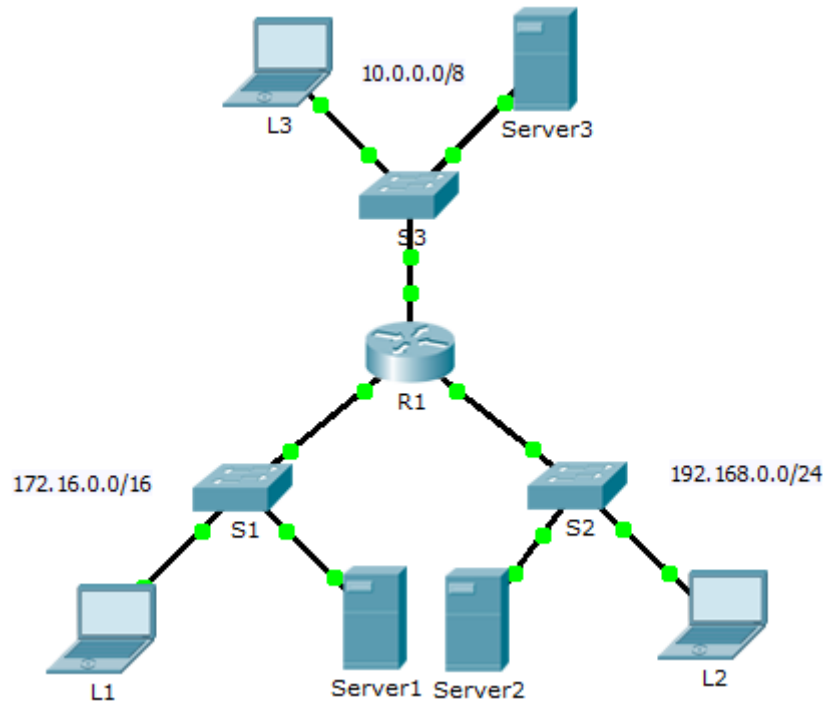# Packet Tracer – Troubleshooting Standard IPv4 ACLs

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:

- Hosts from the 192.168.0.0/24 network are unable to access network 10.0.0.0/8.

- L3 can't access any devices in network 192.168.0.0/24.

- L3 can't access **Server1** or **Server2**. **L3** should only access **Server3**.

- Hosts from the 172.16.0.0/16 network have full access to **Server1**, **Server2** and **Server3**.

  Note: All FTP usernames and passwords are "**cisco**".

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**.

Part 1:   Troubleshoot ACL Issue 1

Hosts from the 192.168.0.0/24 network should not be able to access any devices on the 10.0.0.0/8 network. 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**, attempt to access FTP and HTTP services of **Server1**, **Server2**, and **Server3**.

b. Using **L2**, ping **Server1**, **Server2**, and **Server3**.

c. View the running configuration on **R1**. Examine access list **FROM_192** and its placement on the interfaces. Is the access list placed on the correct interface and in the correct direction? Is there any statement in the list that permits or denies traffic to other networks? Are the statements in the correct order?

d. Perform other tests, as necessary.

Step 2:   Implement a solution.

Make the necessary adjustments to **FROM_192,** 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.

Part 2:   Troubleshoot ACL Issue 2

L3 should not be able to reach **Server1** or **Server2**. 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**, attempt to access FTP and HTTP services of **Server1**, **Server2**, and **Server3**.

b. Using **L3**, ping **Server1**, **Server2**, and **Server3**.

c. View the running configuration on **R1**. Examine access list **FROM_10** and its placement on the interfaces. Is the access list placed on the correct interface and in the correct direction? Is there any statement in the list that permits or denies traffic to other networks? Are the statements in the correct order?

d. Run other tests as necessary.

Step 2: Implement a solution.

Make the necessary adjustments to access list **FROM_10,** or to its placement, to fix the problem.

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

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

Part 3: Troubleshoot ACL Issue 3

Hosts from the 172.16.0.0/16 network should have full access to **Server1**, **Server2** and **Server3** but this is not currently the case, as **L1** can't communicate to **Server2** or **Server3.**

Step 1: Determine the ACL problem.

As you perform the following tasks, compare the results to the expectations of the ACL.

a. Using **L1**, attempt to access FTP and HTTP services of **Server1**, **Server2**, and **Server3**.

b. Using **L1**, ping **Server1**, **Server2**, and **Server3**.

c. View the running configuration on **R1**. Examine access list **FROM_172** and its placement on the interfaces. Is the access list placed on the correct port in the correct direction? Is there any statement in the list that permits or denies traffic to other networks? Are the statements in the correct order?

d. Run other tests as necessary.

Step 2: Implement a solution.

Make an adjustment to access list **FROM_172** or to its placements to fix the problem.

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

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

Part 4: Reflection (Optional)

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?

Suggested Scoring Rubric

Question Location	Possible Points	Earned Points
Documentation Score	**10**	
Packet Tracer Score	**90**	
Total Score	**100**	