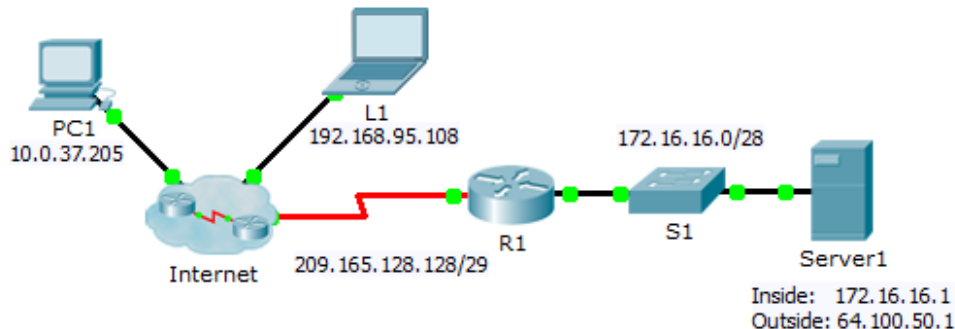# Packet Tracer – Configuring Static NAT

Topology

Objectives

Part 1: Test Access without NAT

Part 2: Configure Static NAT

Part 3: Test Access with NAT

Scenario

In IPv4 configured networks, clients and servers use private addressing. Before packets with private addressing can cross then Internet, they need to be translated to public addressing. Servers that are accessed from outside the organization are usually assigned both a public and a private static IP address. In this activity, you will configure static NAT so that outside devices can access and inside server at its public address.

Part 1: Test Access without NAT

Step 1: Attempt to connect to Server1 using Simulation Mode.

a. From **PC1** or **L1**, attempt to connect to the **Server1** web page at 172.16.16.1. Use the Web Browser to browse **Server1** at 172.16.16.1. The attempts should fail.

b. From **PC1**, ping the **R1** S0/0/0 interface. The ping should succeed.

Step 2: View R1 routing table and running-config.

a. View the running configuration of **R1**. Note that there are no commands referring to NAT.

b. Verify that the routing table does not contain entries referring to the IP addresses used by **PC1** and **L1**.

c. Verify that NAT is not being used by **R1**.

```
R1# show ip nat translations
```

Part 2: Configure Static NAT

Step 1: Configure static NAT statements.

Refer to the Topology. Create a static NAT translation to map the **Server1** inside address to its outside address.

Step 2: Configure interfaces.

Configure the correct inside and outside interfaces.

Part 3: Test Access with NAT

Step 1: Verify connectivity to the Server1 web page.

a. Open the command prompt on **PC1** or **L1**, attempt to ping the public address for **Server1**. Pings should succeed.

b. Verify that both **PC1** and **L1** can now access the **Server1** web page.

Step 2: View NAT translations.

Use the following commands to verify the static NAT configuration:

```
show running-config
show ip nat translations
show ip nat statistics
```