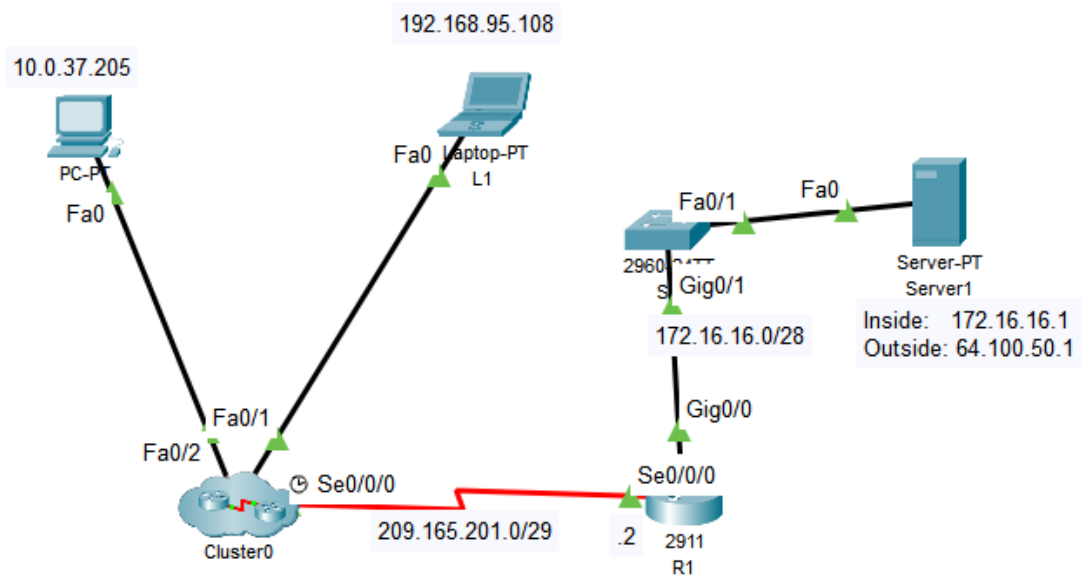
Packet Tracer: Configure Static NAT

This document provides a complete guide for configuring Static Network Address Translation (NAT) in a Packet Tracer environment. Static NAT is used to map a private IP address of an internal server to a public IP address, allowing external devices to access the server.

Objectives

- Part 1: Verify that devices on the public network cannot access the private server.
- Part 2: Configure a static NAT rule and define the router's internal and external interfaces.
- Part 3: Confirm that external devices can now successfully access the server using its public IP address.

Network Topology



Part 1: Verify Access Without NAT

Before configuring NAT, it's essential to confirm that devices on the public network cannot reach the internal server.

- Test Connectivity: From PC1 or L1, attempt to access the `Server1` web page using its private IP address, 172.16.16.1. This attempt should fail, as private IP addresses are not routable on the public internet.
- Verify Router Configuration: On router `R1`, use the following commands to confirm that no NAT configurations are currently in place.
  - `show running-config | include nat` (This should return nothing.)
  - `show ip nat translations` (This should show no active translations.)

Part 2: Configure Static NAT

Now, you will configure `R1` to perform the static NAT translation. This involves two key steps: creating the translation rule and defining the interfaces.

Step 1: Create the NAT Mapping

This command creates a one-to-one mapping between the server's private and public IP addresses.

```
R1(config)# ip nat inside source static 172.16.16.1 64.100.50.1
```

- `172.16.16.1` is the private "inside" IP address of `Server1`.
- `64.100.50.1` is the public "outside" IP address that external devices will use.

Step 2: Configure Router Interfaces

You must tell the router which interfaces are part of the private network (`inside`) and which face the public internet (`outside`).

```
R1(config)# interface g0/0
R1(config-if)# ip nat inside
R1(config-if)# exit
R1(config)# interface s0/0/0
R1(config-if)# ip nat outside
```

- The `g0/0` interface is configured as the inside interface.
- The `s0/0/0` interface is configured as the outside interface.

Part 3: Verify Access With NAT

With the configuration complete, you can now verify that the NAT translation is working.

- Test Connectivity: From an external device (PC1 or L1), use the web browser to access `Server1` using its public IP address, 64.100.50.1. The connection should now be successful.
- Verify Translations on Router: Use these commands to confirm that the NAT rules are active and that traffic is being translated correctly.
  - `show running-config | include nat`
  - `show ip nat translations` (This command will now show the static mapping you created.)
  - `show ip nat statistics` (This will provide details on the number of translations and traffic volume.)