Packet Tracer - Configure PAT

Objectives

Part 1: Configure Dynamic NAT with Overload

Part 2: Verify Dynamic NAT with Overload Implementation

Part 3: Configure PAT using an Interface

Part 4: Verify PAT Interface Implementation

Part 1: Configure Dynamic NAT with Overload

Step 1: Configure traffic that will be permitted.

On **R1**, configure one statement for ACL 1 to permit any address belonging to 172.16.0.0/16.

```
R1(config)# access-list 1 permit 172.16.0.0 0.0.255.255
```

Step 2: Configure a pool of address for NAT.

Configure **R1** with a NAT pool that uses the two useable addresses in the 209.165.200.232/30 address space.

```
R1(config)# ip nat pool ANY_POOL_NAME 209.165.200.233 209.165.200.234 netmask
255.255.255.252
```

Step 3: Associate ACL 1 with the NAT pool and allow addresses to be reused.

```
R1(config)# ip nat inside source list 1 pool ANY_POOL_NAME overload
```

Step 4: Configure the NAT interfaces.

Configure **R1** interfaces with the appropriate inside and outside NAT commands.

```
R1(config)# interface s0/1/0
R1(config-if)# ip nat outside
R1(config-if)# interface g0/0/0
R1(config-if)# ip nat inside
R1(config-if)# interface g0/0/1
R1(config-if)# ip nat inside
```

Part 2: Verify Dynamic NAT with Overload Implementation

Step 1: Access services across the internet.

From the web browser of each of the PCs that use **R1** as their gateway (**PC1**, **L1**, **PC2**, and **L2**), access the web page for **Server1**.

Were all connections successful? YES

Step 2: View NAT translations.

View the NAT translations on **R1**.

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

Notice that all four devices were able to communicate, and they are using just one address out of the pool. PAT will continue to use the same address until it runs out of port numbers to associate with the translation. Once that occurs, the next address in the pool will be used. While the theoretical limit would be 65,536 since the port number field is a 16 bit number, the device would likely run out of memory before that limit would be reached.

Part 3: Configure PAT using an Interface

Step 1: Configure traffic that will be permitted.

On **R2**, configure one statement for ACL 2 to permit any address belonging to 172.17.0.0/16.

Step 2: Associate ACL 2 with the NAT interface and allow addresses to be reused.

Enter the **R2** NAT statement to use the interface connected to the internet and provide translations for all internal devices.

```
R2(config)# ip nat inside source list 2 interface s0/1/1 overload
```

Step 3: Configure the NAT interfaces.

Configure **R2** interfaces with the appropriate inside and outside NAT commands.

Part 4: Verify PAT Interface Implementation

Step 1: Access services across the internet.

From the web browser of each of the PCs that use **R2** as their gateway (**PC3**, **L3**, **PC4**, and **L4**), access the web page for **Server1**.

Were all connections successful? YES

Step 2: View NAT translations.

View the NAT translations on **R2**.

Step 3: Compare NAT statistics on R1 and R2.

Compare the NAT statistics on the two devices.

Why doesn't **R2** list any dynamic mappings?