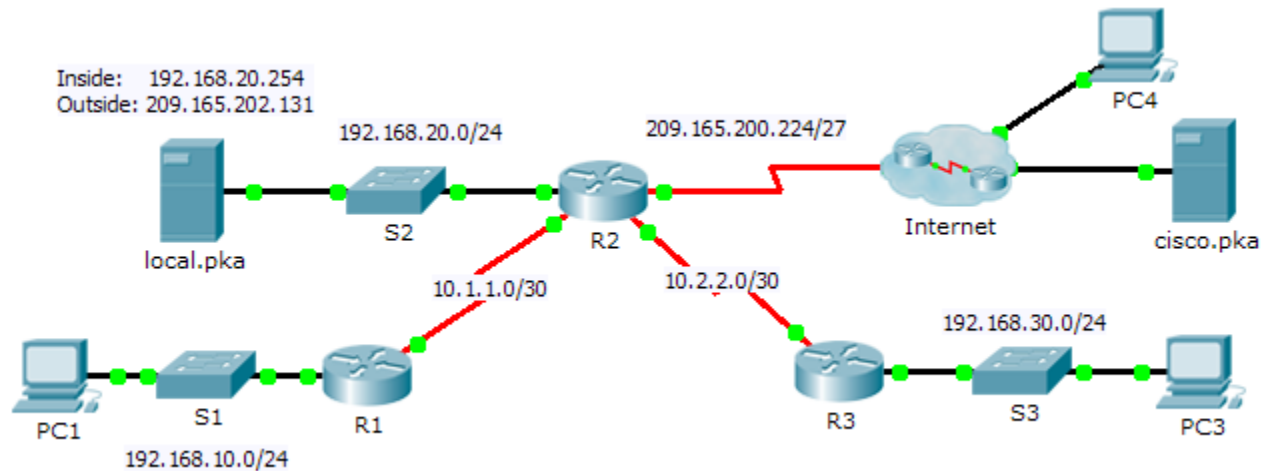


Packet Tracer – Implementing Static and Dynamic NAT

Topology



Objectives

Part 1: Configure Dynamic NAT with PAT

Part 2: Configure Static NAT

Part 3: Verify NAT Implementation

Part 1: Configure Dynamic NAT with PAT

Step 1: Configure traffic that will be permitted for NAT translations.

On R2, configure a standard ACL named R2NAT that uses three statements to permit, in order, the following private address spaces: 192.168.10.0/24, 192.168.20.0/24, and 192.168.30.0/24.

Step 2: Configure a pool of addresses for NAT.

- a. Configure R2 with a NAT pool that uses the first two addresses in the 209.165.202.128/30 address space. The fourth address is used for static NAT later in Part 2.

Step 3: Associate the named ACL with the NAT pool and enable PAT.

Step 4: Configure the NAT interfaces.

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

Part 2: Configure Static NAT

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

Part 3: Verify NAT Implementation

Step 1: Access services across the Internet.

- a. From the web browser of **PC1**, or **PC3**, access the web page for **cisco.pka**.
- b. From the web browser for **PC4**, access the web page for **local.pka**.

Step 2: View NAT translations.

View the NAT translations on **R2**.

```
R2# show ip nat translations
```