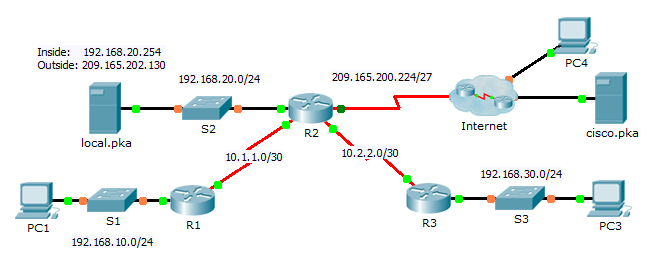
Packet Tracer – Implementing Static and Dynamic NAT

1. Topology



1. Objectives

Part 1: Configure Dynamic NAT with PAT

Part 2: Configure Static NAT

Part 3: Verify NAT Implementation

1. Configure Dynamic NAT with PAT
   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.

**ip access-list standard R2NAT**

**permit 192.168.10.0 0.0.0.255**

**permit 192.168.20.0 0.0.0.255**

**permit 192.168.30.0 0.0.0.255**

* 1. Configure a pool of addresses for NAT.

Configure **R2** with a NAT pool named **R2POOL** that uses the first address in the 209.165.202.128/30 address space. The second address is used for static NAT later in Part 2.

**ip nat pool R2POOL 209.165.202.129 209.165.202.129 netmask 255.255.255.252**

* 1. Associate the named ACL with the NAT pool and enable PAT.

**ip nat inside source list R2NAT pool R2POOL overload**

* 1. Configure the NAT interfaces.

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

**int fa0/0**

**ip nat inside**

**int s0/0/0**

**ip nat inside**

**int s0/0/1**

**ip nat inside**

**int s0/1/0**

**ip nat outside**

1. Configure Static NAT

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

**ip nat inside source static 192.168.20.254 209.165.202.130**

1. Verify NAT Implementation
   1. Access services across the Internet.
      1. From the web browser of **PC1**, or **PC3**, access the web page for **cisco.pka**.
      2. From the web browser for **PC4**, access the web page for **local.pka**.
   2. View NAT translations.

View the NAT translations on **R2**.

R2# **show ip nat translations**