Lab 16 - Packet Tracer - Investigate NAT Operations

# Addressing Table

The following table provides addressing for networking device interfaces only.

| Device | Interface | IP Address and Prefix |
| --- | --- | --- |
| R2 | G0/0 | 10.255.255.245/30 |
| R2 | G0/1 | 10.255.255.249/30 |
| R2 | G0/2 | 10.10.10.1/24 |
| R2 | S0/0/0 | 64.100.100.2/27 |
| R2 | S0/0/1.1 | 64.100.200.2/30 |
| R4 | G0/0 | 172.16.0.1/24 |
| R4 | S0/0/0 | 64.100.150.1/30 |
| R4 | S0/0/1.1 | 64.100.200.1/30 |
| WRS | LAN | 192.168.0.1/24 |
| WRS | Internet | 64.104.223.2/30 |

# Objectives

Part 1: Investigate NAT Operation Across the Intranet

Part 2: Investigate NAT Operation Across the Internet

Part 3: Conduct Further Investigations

# Scenario

As a frame travels across a network, the MAC addresses may change. IP addresses can also change when a packet is forwarded by a device configured with NAT. In this activity, we will investigate what happens to IP addresses during the NAT process.

# Instructions

## Investigate NAT Operation Across the Intranet

### Wait for the network to converge.

It might take a few minutes for everything in the network to converge. You can speed the process up by clicking Fast Forward Time.

### Generate an HTTP request from any PC in the Central domain.

* + - 1. Switch to **Simulation** mode and edit the filters to show only HTTP requests.
      2. Open the Web Browser of any PC in the **Central** domain and type the URL **http://branchserver.pka** and click **Go**. Minimize the browser window.
      3. Click **Capture / Forward** until the PDU is over **D1** or **D2**. Click on the most recent PDU in the Event List. Record the source and destination IP addresses.

#### Question:

To what devices do those addresses belong? 10.X.X.X and 64.100.200.1 The PC and R4.

Type your answers here.

* + - 1. Click **Capture / Forward** until the PDU is over **R2**. Record the source and destination IP addresses in the outbound packet.

#### Question:

To what devices do those addresses belong?  64.100.100.X and 64.100.200.1 R4 is the second address

Type your answers here.

* + - 1. Login to R2 from the CLI using the password **class** to enter privileged EXEC and issue the following command:

Open configuration window

R2# **show run | include pool**

ip nat pool R2Pool 64.100.100.3 64.100.100.31 netmask 255.255.255.224

ip nat inside source list 1 pool R2Pool

The address came from the NAT pool **R2Pool**.

* + - 1. Click **Capture / Forward** until the PDU is over **R4**. Record the source and destination IP addresses in the outbound packet.

#### Question:

To what devices do those addresses belong? 64.100.100.X and 172.16.0.3. First address is from R2. Branchserver is the second address

Type your answers here.

* + - 1. Click **Capture / Forward** until the PDU is over **Branchserver.pka**. Record the source and destination TCP port addresses in the outbound segment.

Type your answers here.

* + - 1. On both **R2** and **R4**, run the following command and match the IP addresses and ports recorded above to the correct line of output:

R2# **show ip nat translations**

R4# **show ip nat translations**

#### Questions:

What do the inside local IP addresses have in common? They are for private use

Type your answers here.

Did any private addresses cross the intranet? No

Type your answers here.

Close configuration window

* + - 1. Click the Reset Simulation button and remain in Simulation Model.

## Investigate NAT Operation Across the Internet

### Generate an HTTP request from any computer in the home office.

* + - 1. Open the Web Browser of any PC in the **Home Office** domain and type the URL **http://centralserver.pka** and click **Go**.
      2. Click Capture / Forward until the PDU is over WRS. Record the inbound source and destination IP addresses and the outbound source and destination addresses.

#### Question:

To what devices do those addresses belong? 192.168.0.X and 64.100.100.2, 64.104.223.2 and 64.100.100.2

Type your answers here.

* + - 1. Click **Capture / Forward** until the PDU is over **R2**. Record the source and destination IP addresses in the outbound packet.

#### Question:

To what devices do those addresses belong? 64.104.223.2 and 10.10.10.2 WRS and centralserver

Type your answers here.

* + - 1. On **R2**, run the following command and match the IP addresses and ports recorded above to the correct line of output:

Open configuration window

R2# **show ip nat translations**

Close configuration window

* + - 1. Return to Realtime mode.

#### Question:

Did all of the web pages appear in the browsers? Yes

Type your answers here.

## Conduct Further Investigations

Experiment with more packets, both HTTP and HTTPS and answer the following questions.

#### Questions:

Do the NAT translation tables grow? Yes when new conversations established more entries get entered

Type your answers here.

Does WRS have a NAT pool of addresses? No, it uses same addresses

Type your answers here.

Is this how the computers in the classroom connect to the internet? No.

Type your answers here.

Why does NAT use four columns of addresses and ports? inside global, inside local, outside local, and outside global.

Type your answers here.

Where are the networks are inside global and inside local? The inside local addresses are on the LANs within each domain and outside global addresses are from the WAN.

Type your answers here.

On which devices are NAT services operating? What do they have in common? WRS, R2, and R4, they call connect internal LANs to the WAN

Type your answers here.

End of document