

VxLEARN Networks

Networking & Cybersecurity Track
Simulated Employment Program

Lab Report: Examine NAT on a Wireless Router

Prepared by:
Kudzaishe Majeza
Junior Network Engineer – VxLEARN Networks

Mentor:
Titus Majeza
Senior Network Engineer

Date: 06 November 2025

Table of Contents

1. Objective
2. Background
3. Part 1 – Examine External Network Configuration
4. Part 2 – Examine Internal Network Configuration
5. Part 3 – Connect Internal Hosts
6. Part 4 – Observe NAT Translation
7. Part 5 – Packet Header Inspection
8. Reflection and Conclusion
9. Sign-Of

1. Objective

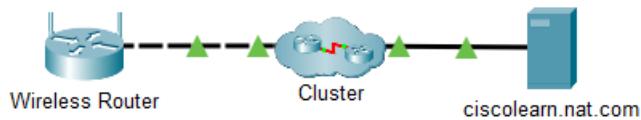
This lab demonstrates how Network Address Translation (NAT) is used on a wireless router to allow private internal devices to access external networks. The lab also uses DHCP to automatically assign IP addresses to internal hosts and examines packet header changes during NAT translation.

2. Background / Scenario

The wireless router connects a LAN (private network) to an ISP (public network).

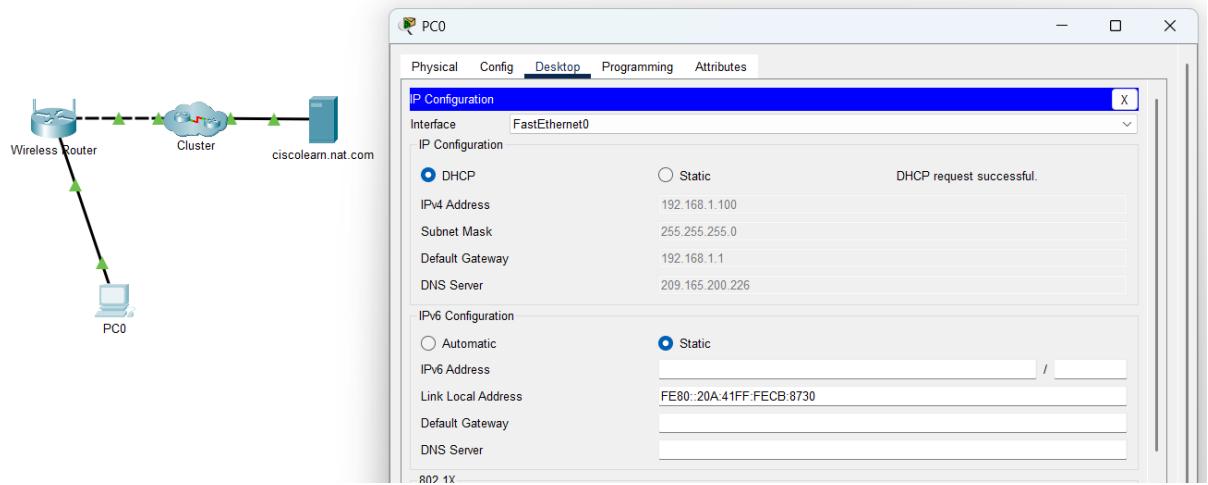
Internal devices use private IP addresses which cannot be routed across the Internet.

NAT translates these private addresses into a single public address so external communication can occur.

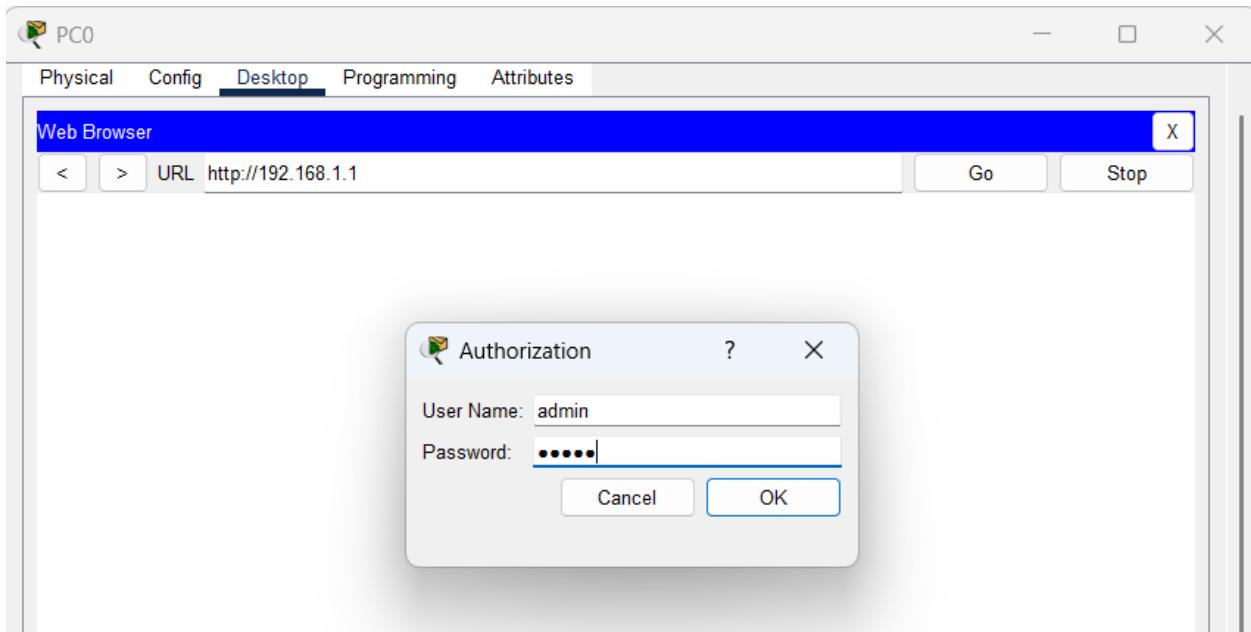


3. Part 1 – Examine External Network Configuration

1. Connected a PC to the router and enabled DHCP.
2. Recorded the default gateway address provided by DHCP.



3. Accessed the wireless router GUI in a web browser.
4. Navigated to Status → Router to view the Internet (WAN) IP Address.



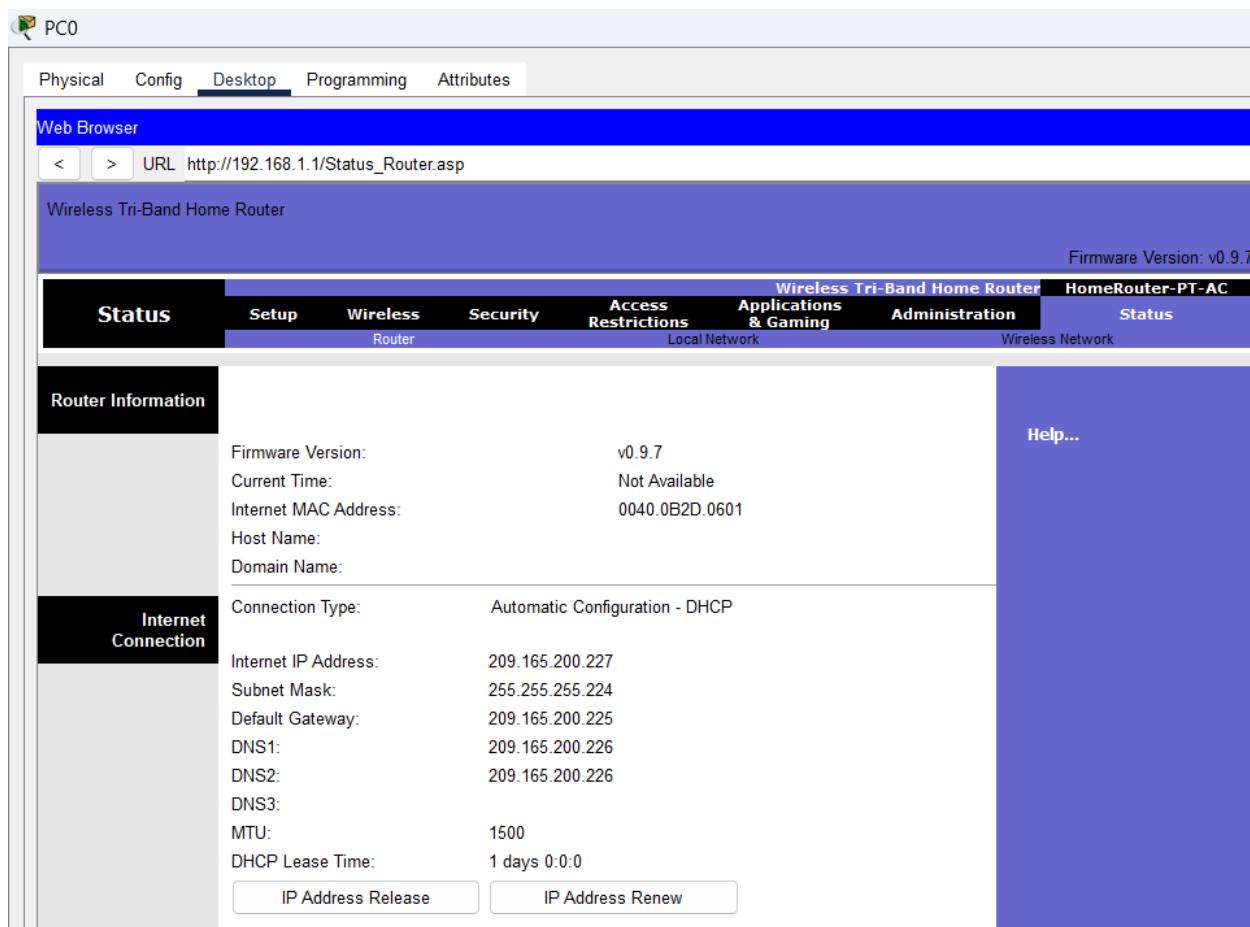


Figure 1: Router WAN Status

Is the WAN IP address private or public?

It is a public IP address, because it is assigned by the ISP and is routable across external networks.

4. Part 2 – Examine Internal Network Configuration

1. Opened Status → Local Network in the router GUI.
2. Observed the LAN IP address and DHCP server settings.
3. Identified the DHCP address pool used for local devices.

The screenshot shows a router's configuration interface titled "Wireless Tri-Band Home Router". The top navigation bar includes tabs for Status, Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, and Status. The "Status" tab is selected, and the sub-tab "Local Network" is active. The main content area displays the following information:

Local Network	
Local MAC Address:	00D0.97B5.0DD2
Router IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
DHCP Server	
DHCP Server:	Enabled
Start IP Address:	192.168.1.100
End IP Address:	192.168.1.149

A "DHCP Client Table" button is located below the DHCP server settings. A "Help..." link is visible in the top right corner of the content area.

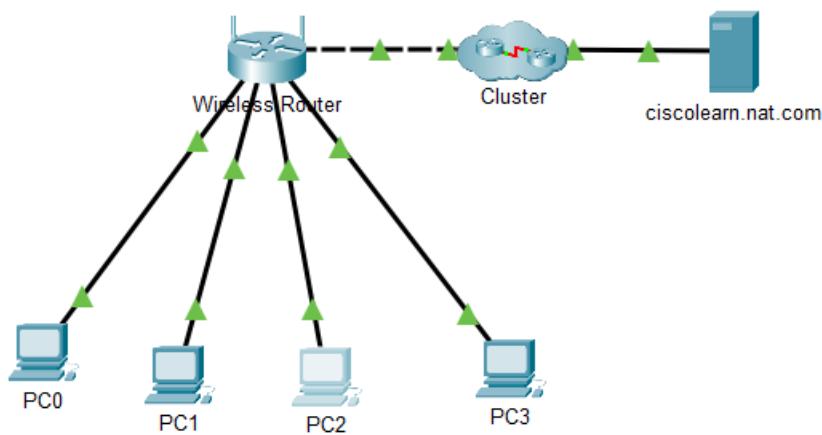
Figure 2: Local Network & DHCP Pool

Are these internal network addresses private or public?

The internal IP addresses are private, used only inside the LAN

5. Part 3 – Connect Additional PCs

1. Added three more PCs and connected them to the router.



2. Configured each PC to use DHCP.

PC1

Physical Config **Desktop** Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

DHCP Static DHCP request successful.

IPv4 Address: 192.168.1.101

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server: 209.165.200.226

PC2

Physical Config **Desktop** Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

DHCP Static DHCP request successful.

IPv4 Address: 192.168.1.102

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server: 209.165.200.226

PC3

Physical Config **Desktop** Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

DHCP Static DHCP request successful.

IPv4 Address: 192.168.1.103

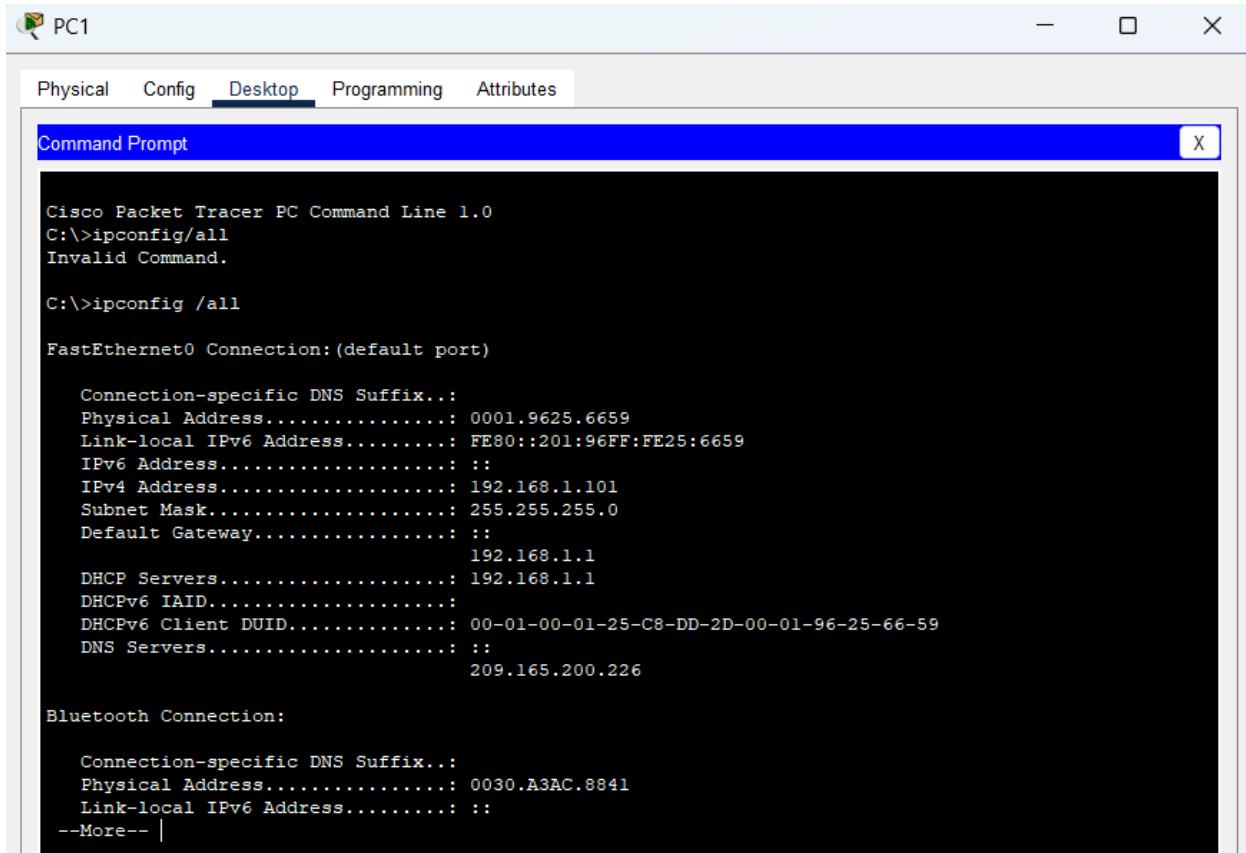
Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server: 209.165.200.226

3. Verified IP configurations using:

ipconfig /all



The screenshot shows a window titled "PC1" with a toolbar at the top labeled "Physical", "Config", "Desktop" (which is underlined), "Programming", and "Attributes". Below the toolbar is a blue header bar with the text "Command Prompt" and a close button "X". The main area of the window displays the output of the "ipconfig /all" command. The output is as follows:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig/all
Invalid Command.

C:\>ipconfig /all

FastEthernet0 Connection: (default port)

  Connection-specific DNS Suffix...:
    Physical Address.....: 0001.9625.6659
    Link-local IPv6 Address....: FE80::201:96FF:FE25:6659
    IPv6 Address.....: ::
    IPv4 Address.....: 192.168.1.101
    Subnet Mask.....: 255.255.255.0
    Default Gateway.....: ::
                           192.168.1.1
    DHCP Servers.....: 192.168.1.1
    DHCPv6 IAID.....: 
    DHCPv6 Client DUID.....: 00-01-00-01-25-C8-DD-2D-00-01-96-25-66-59
    DNS Servers.....: ::
                           209.165.200.226

Bluetooth Connection:

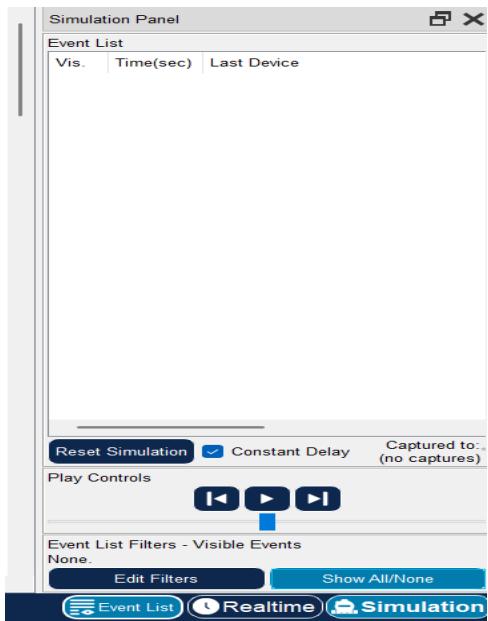
  Connection-specific DNS Suffix...:
    Physical Address.....: 0030.A3AC.8841
    Link-local IPv6 Address....: ::

--More-- |
```

Figure 3: PC IP Config Results

6. Part 4 – Observe NAT Translation

1. Switched to Simulation Mode.

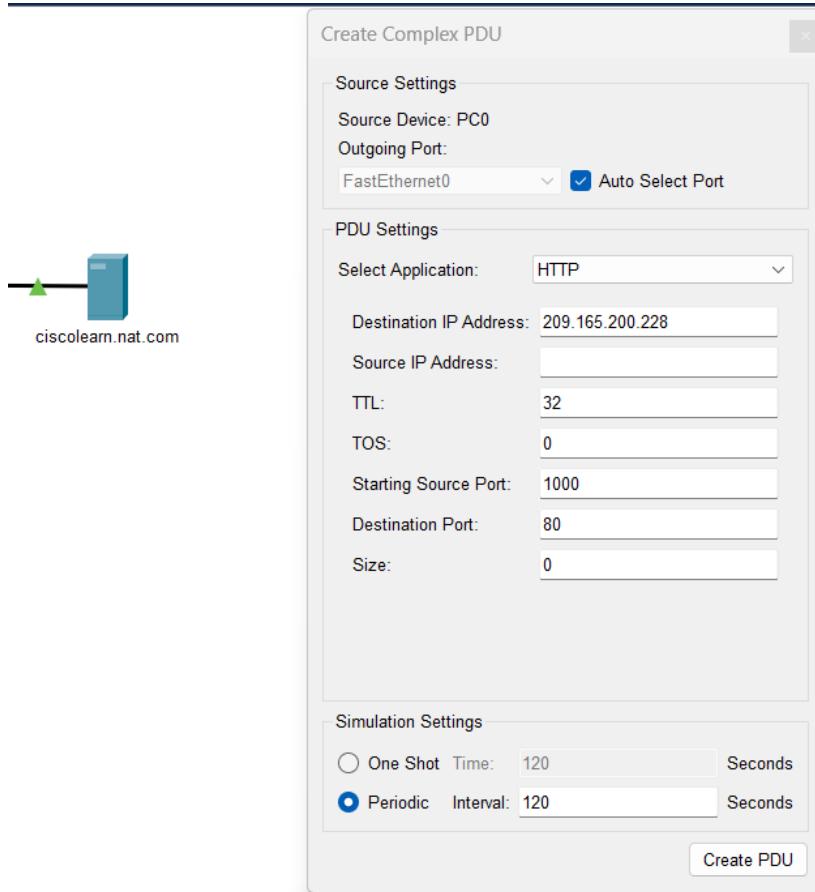


2. Filtered visible protocols to TCP and HTTP.



3. Created a Complex PDU from a PC to the external web server:

- Application: HTTP
- Destination: ciscolearn.nat.com
- Source Port: 1000
- Periodic interval: 120 seconds



4. Ran the simulation and observed packet flow crossing the router.

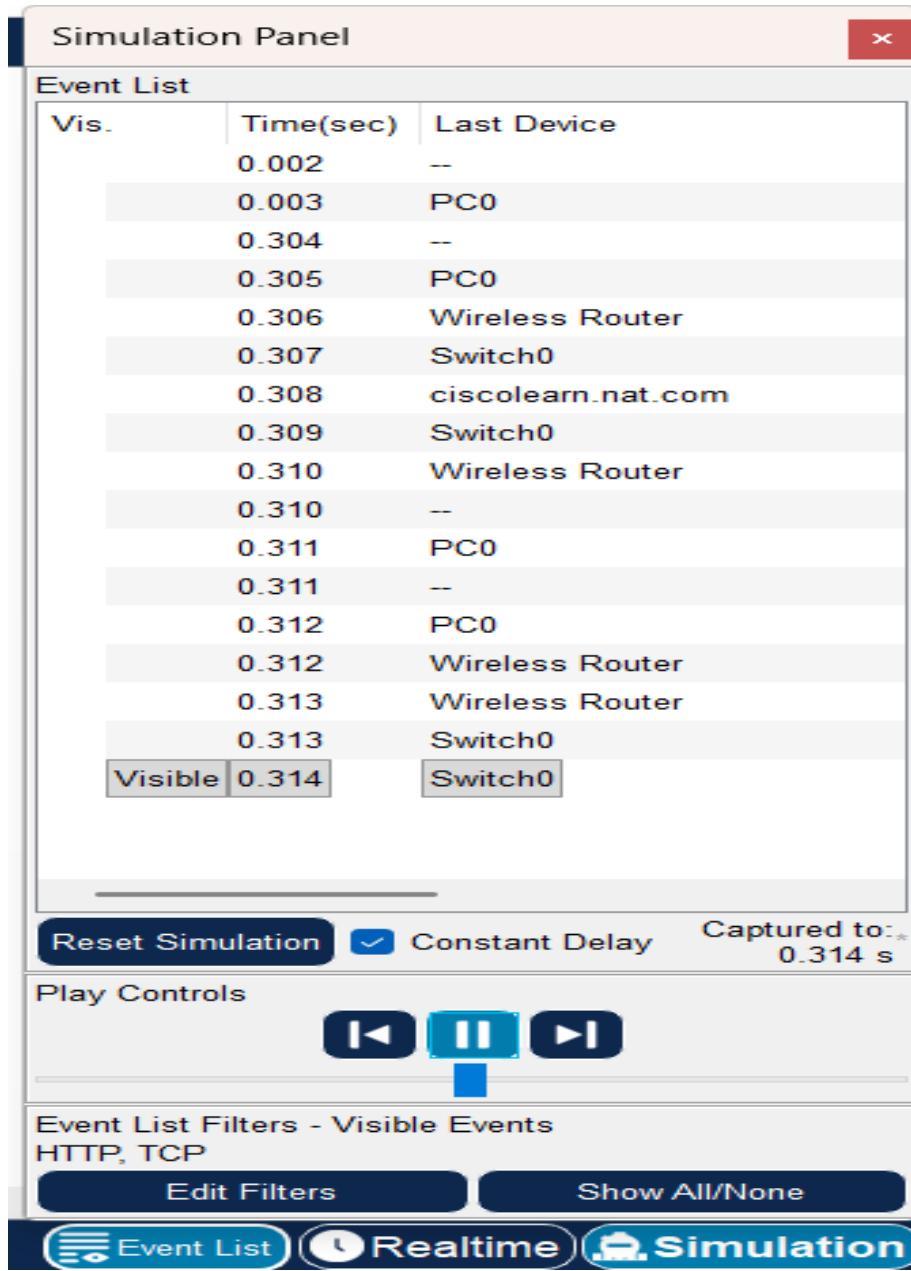


Figure 4: Packet Traversal Animation

7. Part 5 – Packet Header Inspection

1. Viewed packet event details in Simulation mode.
2. Compared Inbound vs Outbound PDU Details on the router.

Key Observations:

Packet Direction	Source IP	Destination IP
Inbound to Router	Private IP (e.g., 192.168.x.x)	Web Server IP
Outbound to Internet	Public WAN IP	Web Server IP

This confirms NAT translation is occurring, changing the source IP from internal private to external public.

PDU Information at Device: ciscolearn.nat.com

OSI Model Inbound PDU Details Outbound PDU Details

At Device: ciscolearn.nat.com Source: PC0 Destination: 209.165.200.228	
In Layers Layer7 Layer6 Layer5 Layer 4: TCP Src Port: 1000, Dst Port: 80 Layer 3: IP Header Src. IP: 209.165.200.227, Dest. IP: 209.165.200.228 Layer 2: Ethernet II Header 0040.0B2D.0601 >> 0001.6434.459A Layer 1: Port FastEthernet0	Out Layers Layer7 Layer6 Layer5 Layer 4: TCP Src Port: 80, Dst Port: 1000 Layer 3: IP Header Src. IP: 209.165.200.228, Dest. IP: 209.165.200.227 Layer 2: Ethernet II Header 0001.6434.459A >> 0040.0B2D.0601 Layer 1: Port(s): FastEthernet0

1. FastEthernet0 receives the frame.

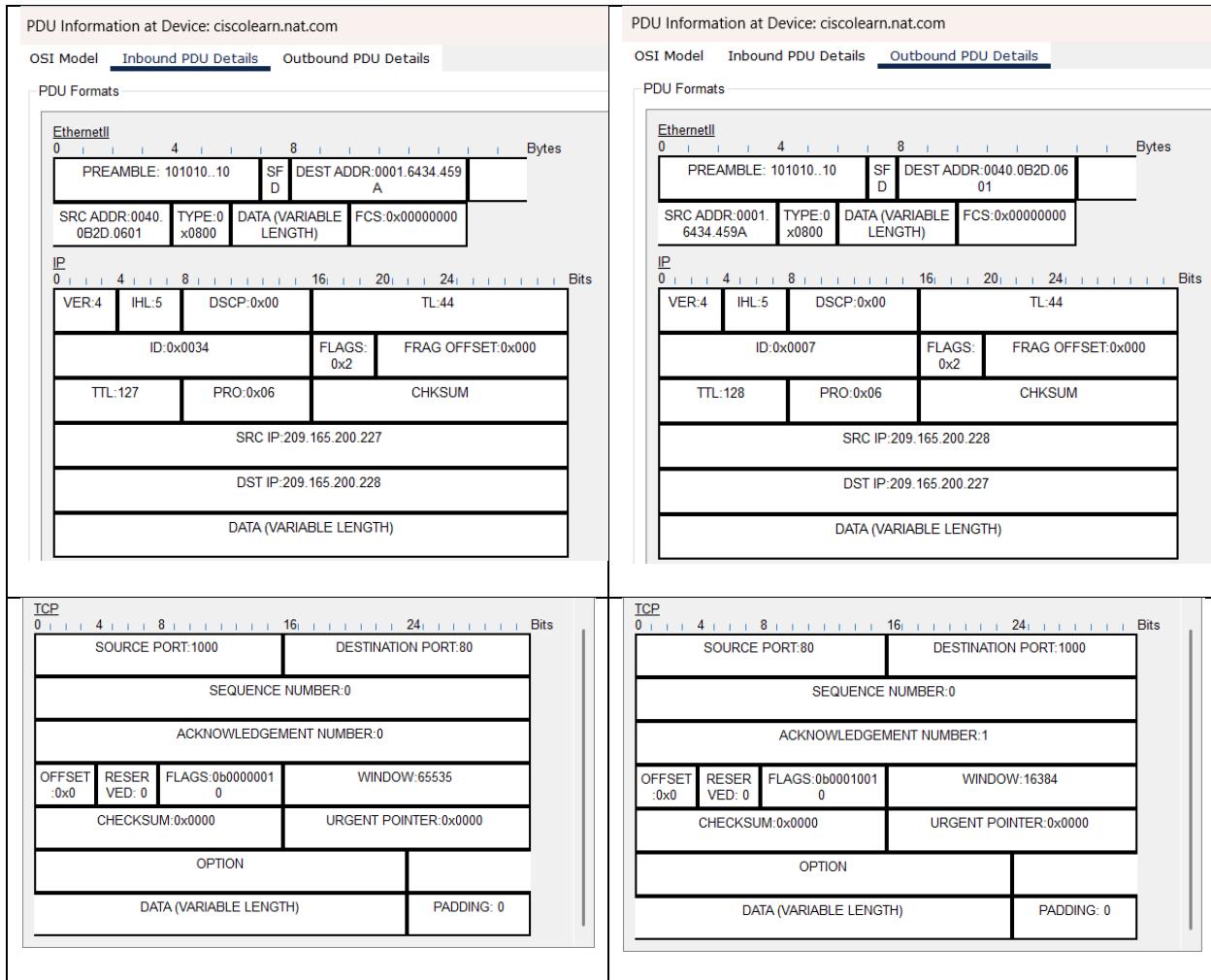


Figure 5: Inbound / Outbound PDU Header Comparison

8. Reflection and Conclusion

This lab demonstrated how NAT enables private internal devices to communicate with external networks by translating private source addresses into a public IP address. I also observed how DHCP automatically configures devices in the LAN and verified network flows using Packet Tracer's Simulation Mode. Understanding NAT is critical for securing and scaling modern networks.

Sign-Off

Prepared by:

Kudzaishe Majeza

Junior Network Engineer – VxLEARN Networks

Reviewed by:

Titus Majeza

Senior Network Engineer