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

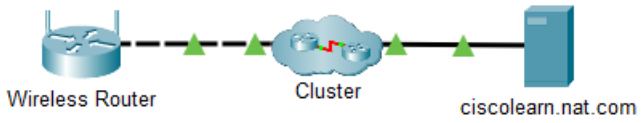
This lab demonstrates how Network Address Translation (NAT) is used on a wireless router to allow private internal devices to access external networks. The lab also uses DHCP to automatically assign IP addresses to internal hosts and examines packet header changes during NAT translation.

2. Background / Scenario

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

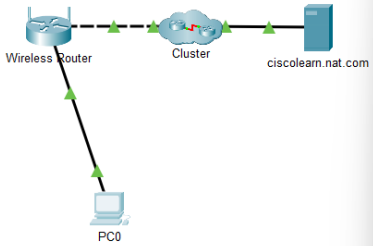
Internal devices use private IP addresses which cannot be routed across the Internet.

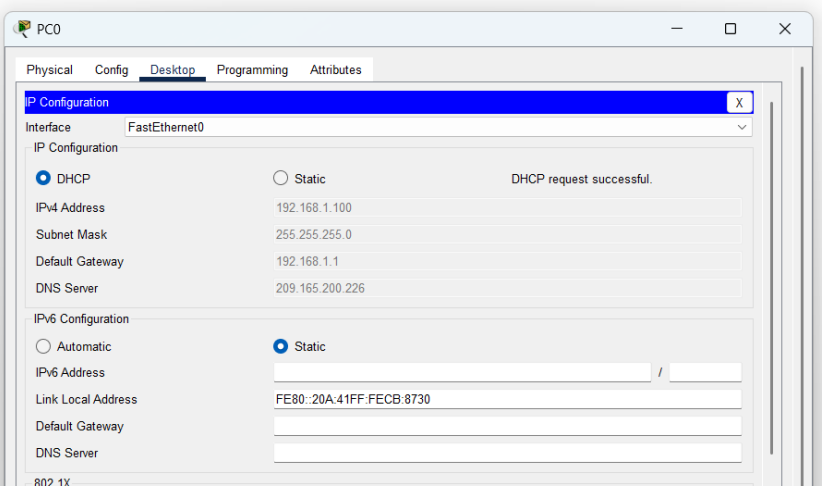
NAT translates these private addresses into a single public address so external communication can occur.



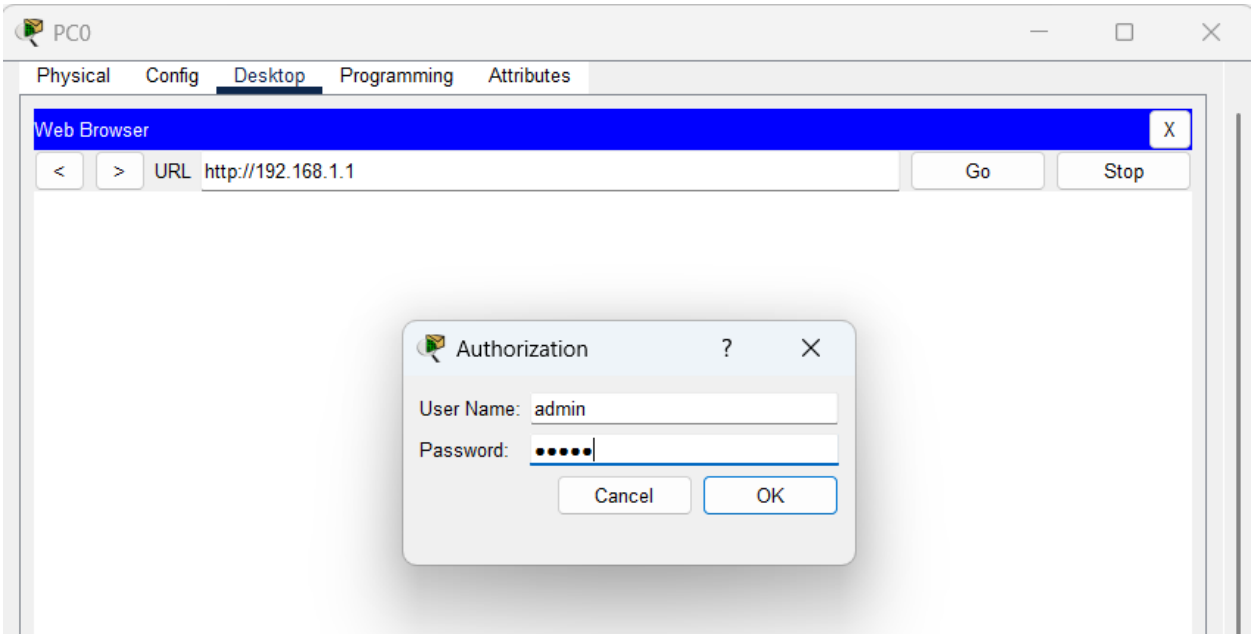
3. Part 1 – Examine External Network Configuration

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.



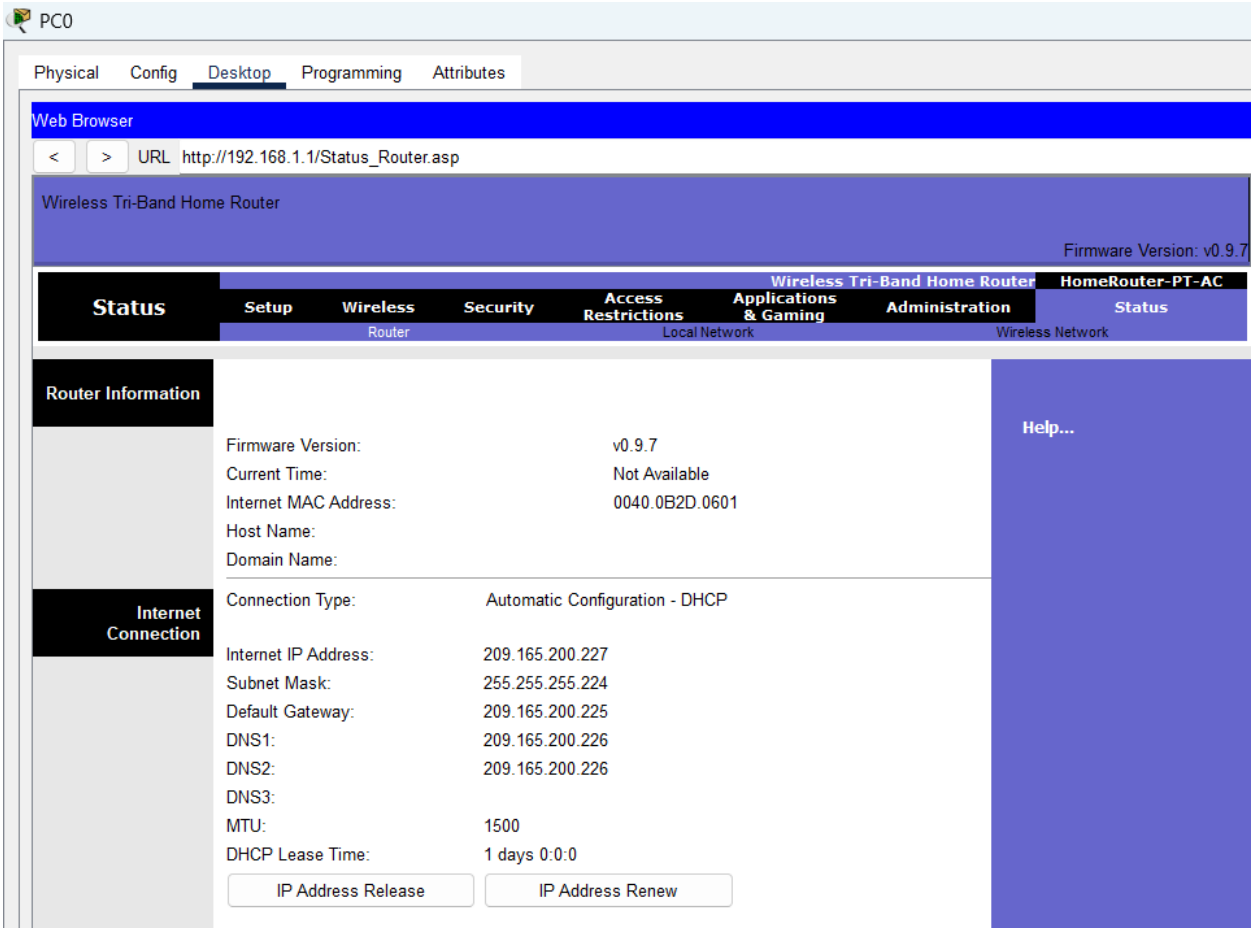


Figure 1: Router WAN Status

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.

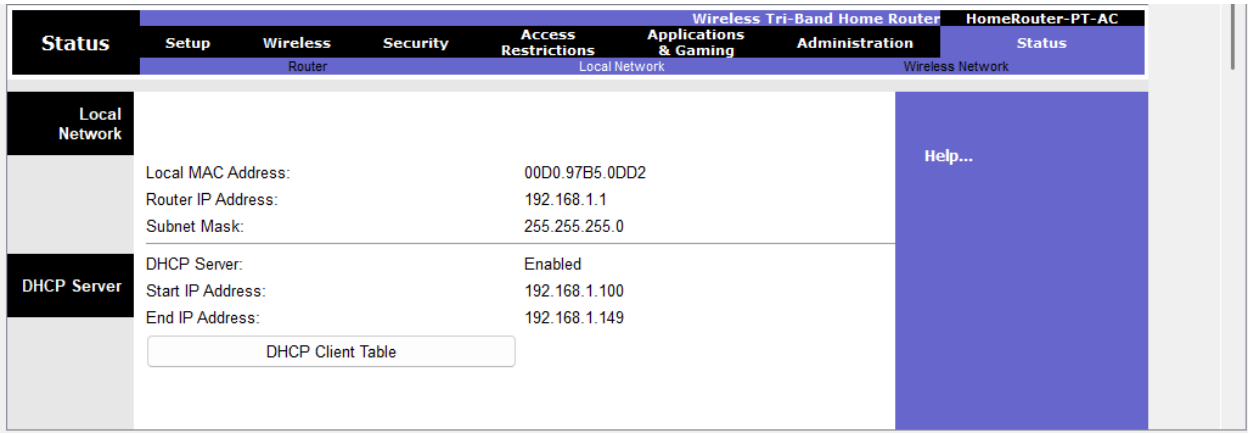


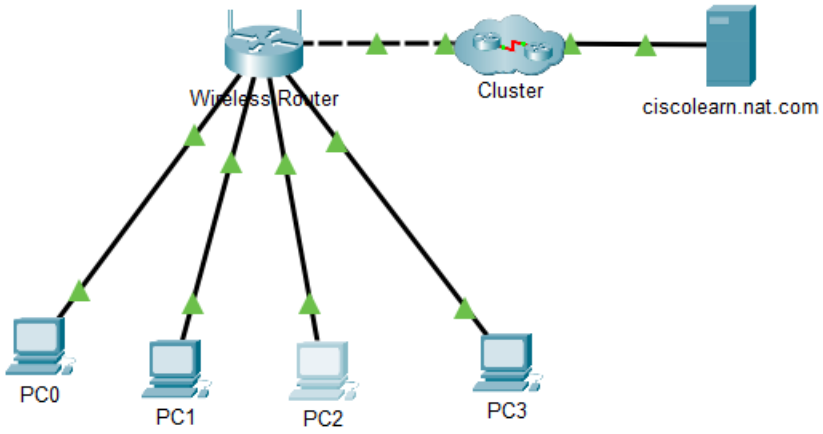
Figure 2: Local Network & DHCP Pool

Are these internal network addresses private or public?

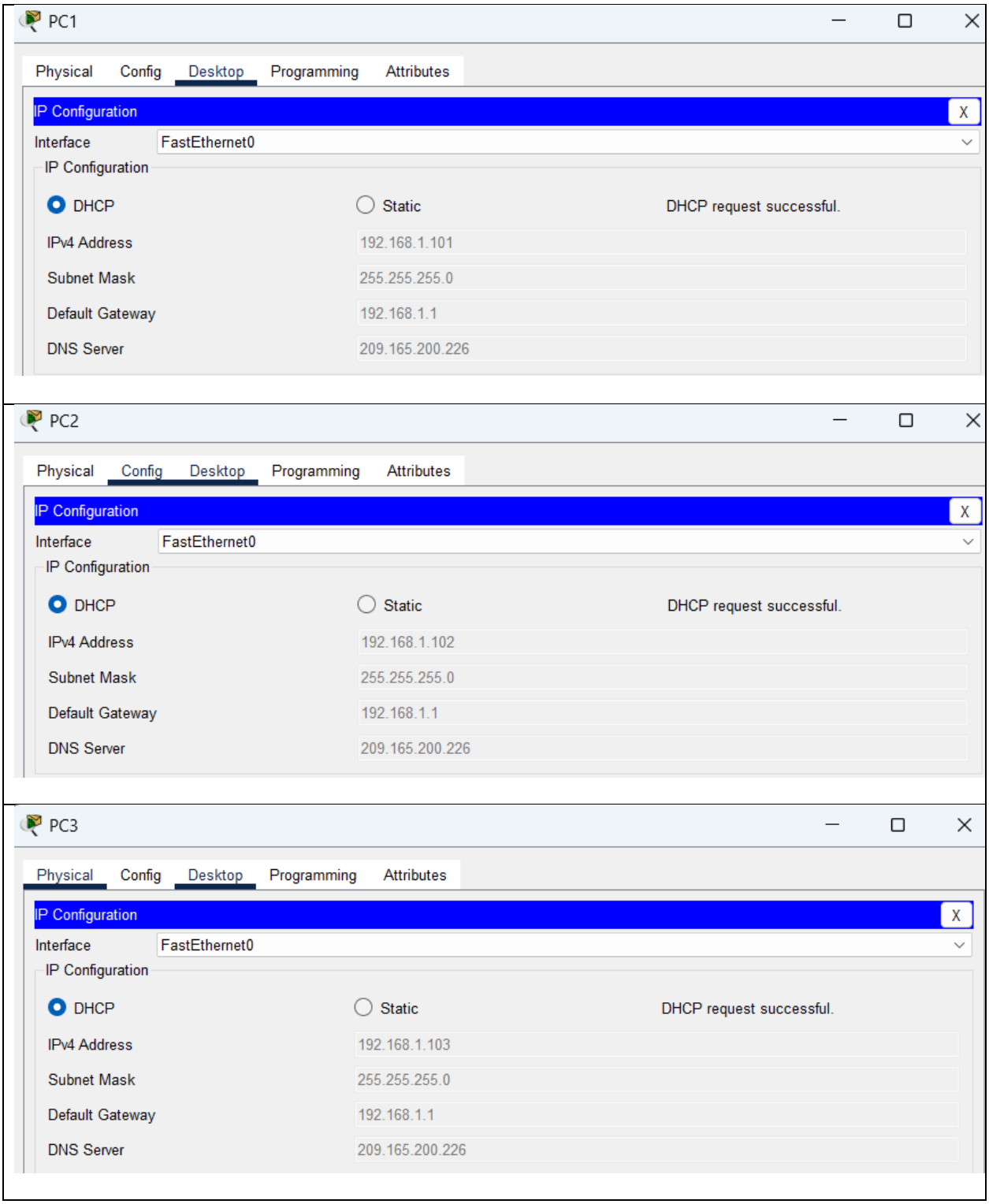
The internal IP addresses are private, used only inside the LAN

5. Part 3 – Connect Additional PCs

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



2. Configured each PC to use DHCP.



3. Verified IP configurations using:

ipconfig /all

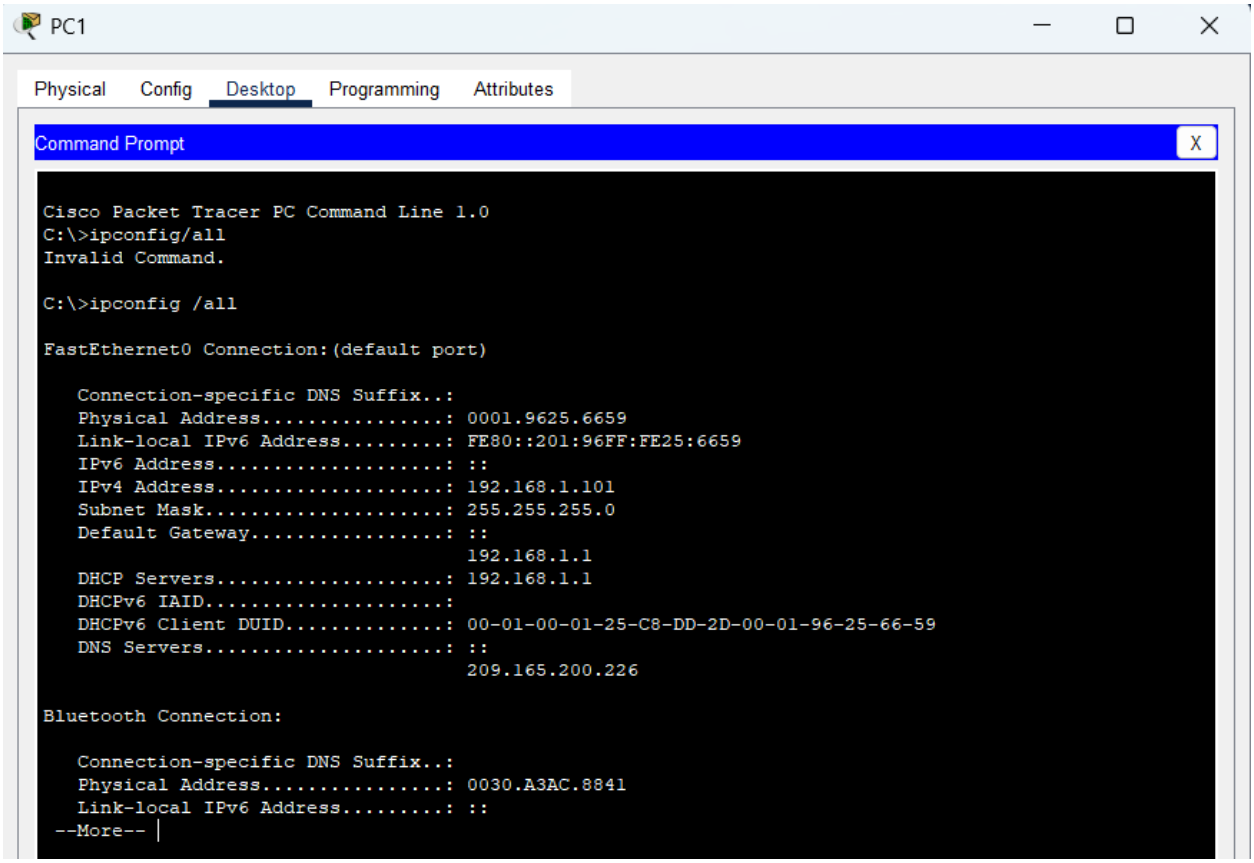
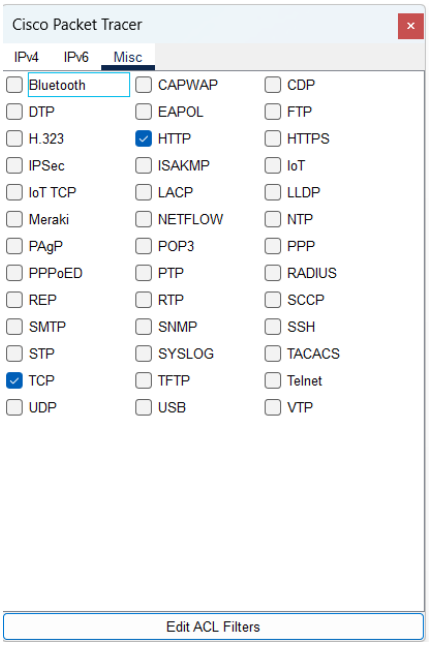


Figure 3: PC IP Config Results

6. Part 4 – Observe NAT Translation

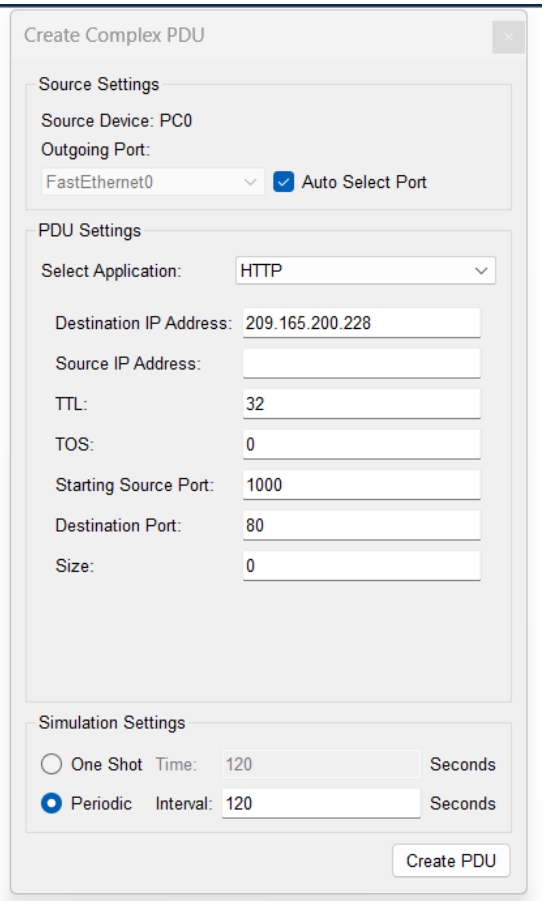
1. Switched to Simulation Mode.

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.

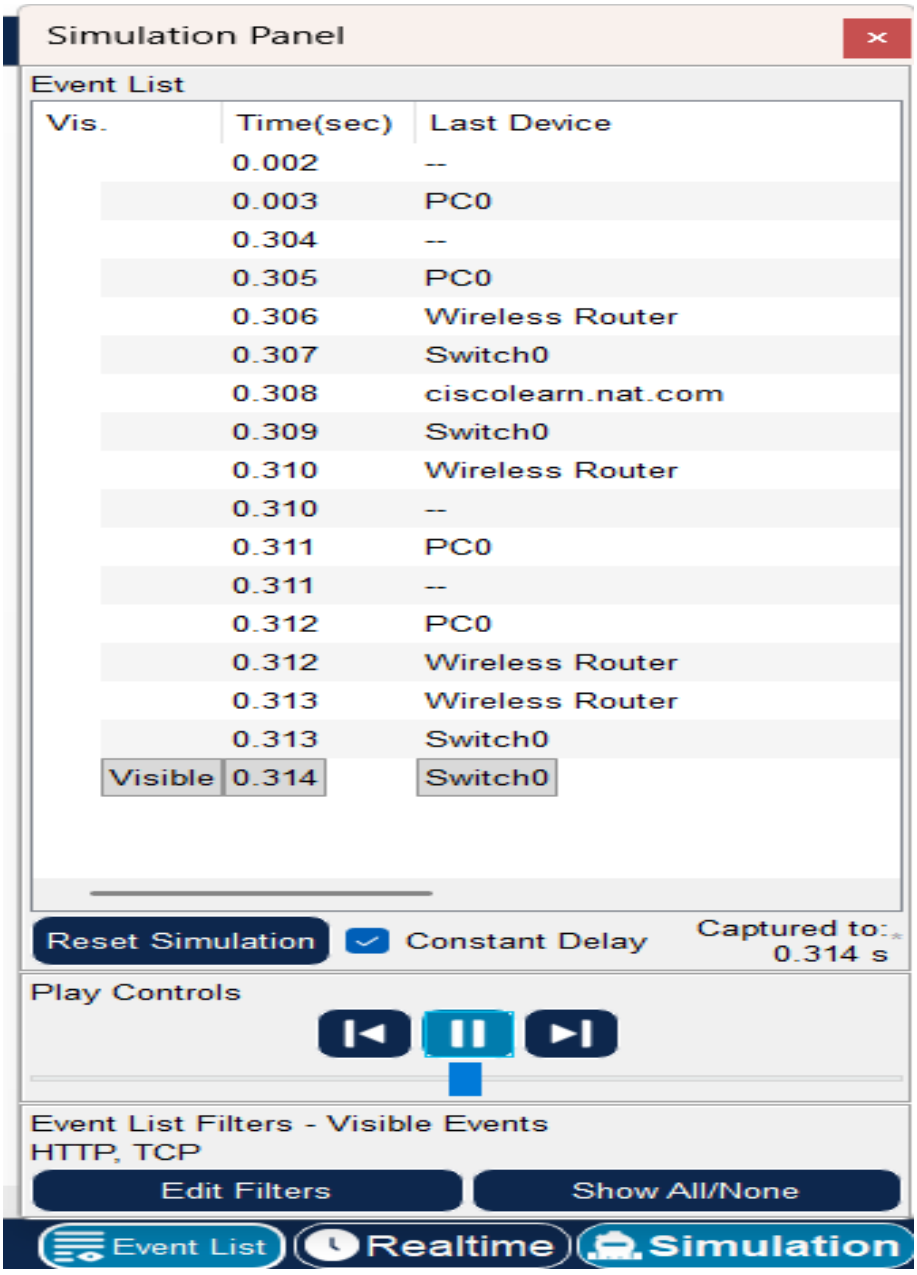


Figure 4: Packet Traversal Animation

7. Part 5 – Packet Header Inspection

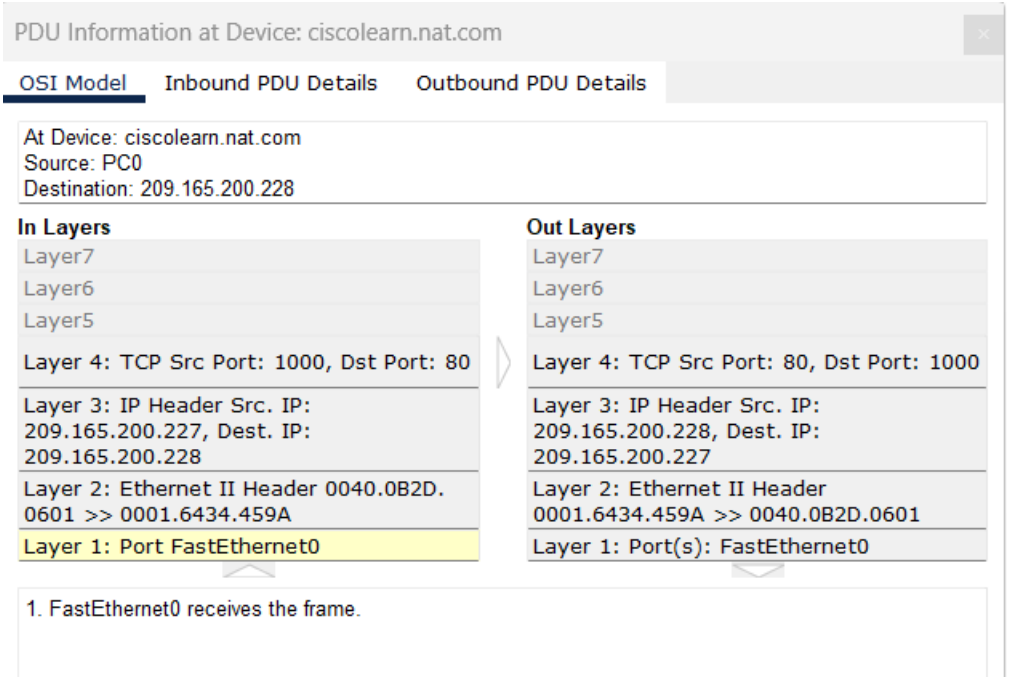
1. Viewed packet event details in Simulation mode.

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.



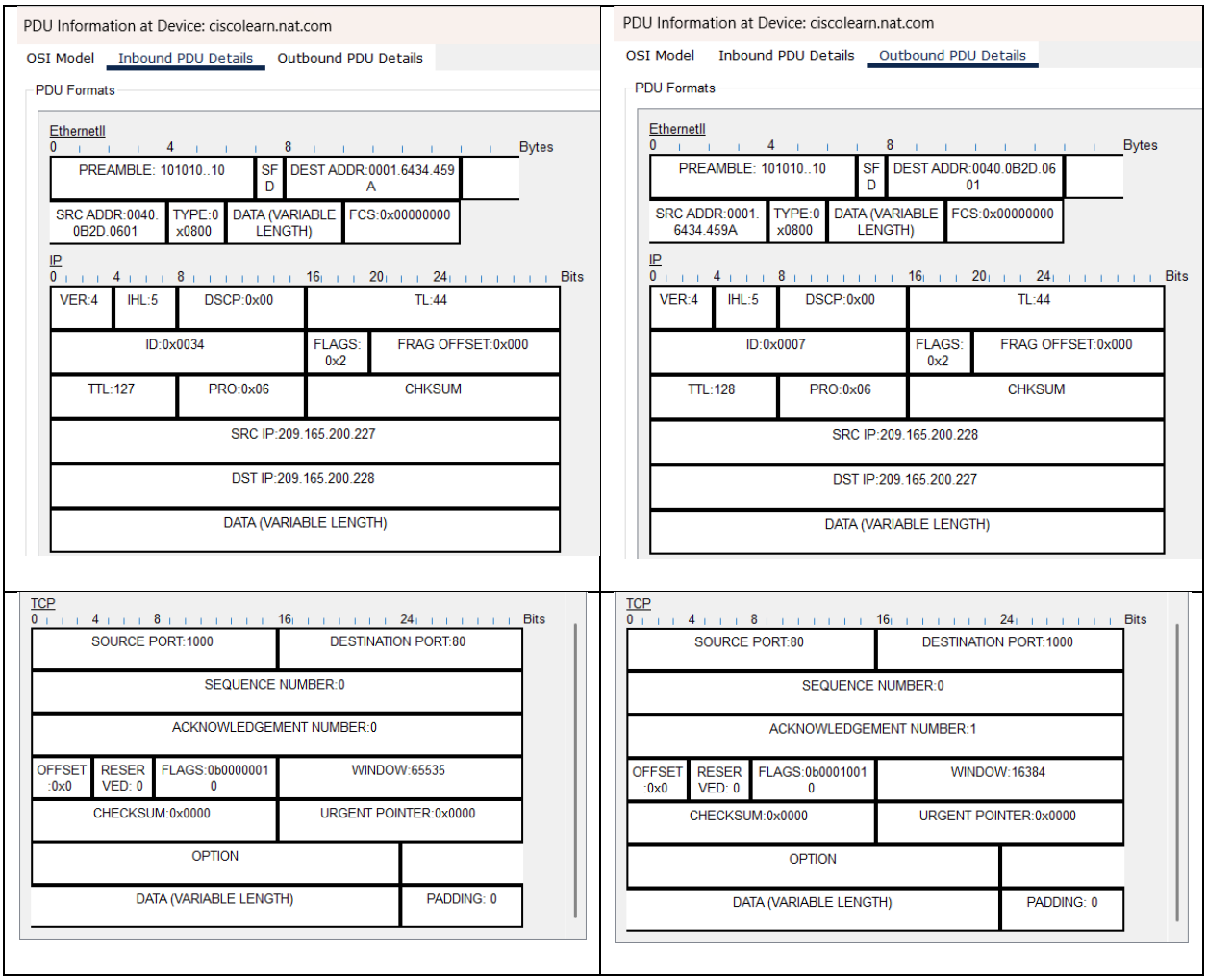


Figure 5: Inbound / Outbound PDU Header Comparison

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