

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).

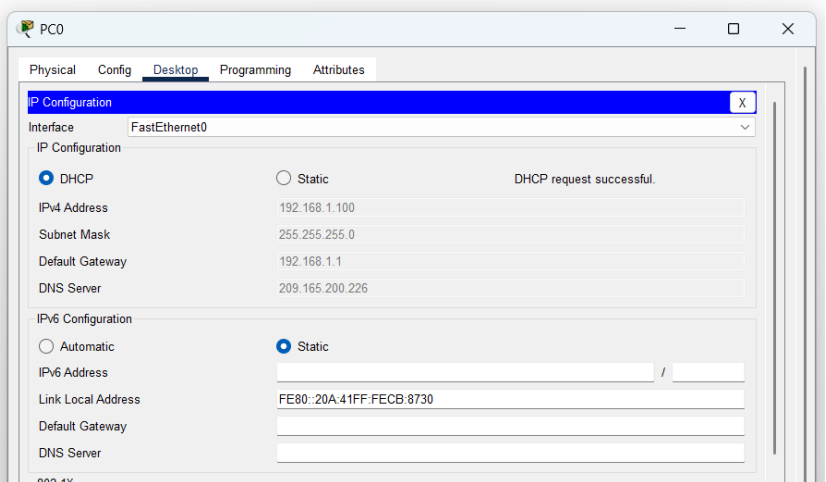
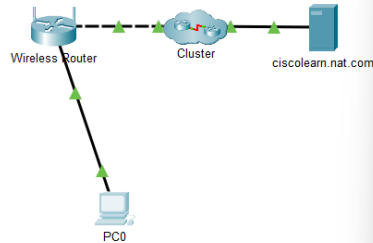
Internal devices use private IP addresses which cannot be routed across the Internet.

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

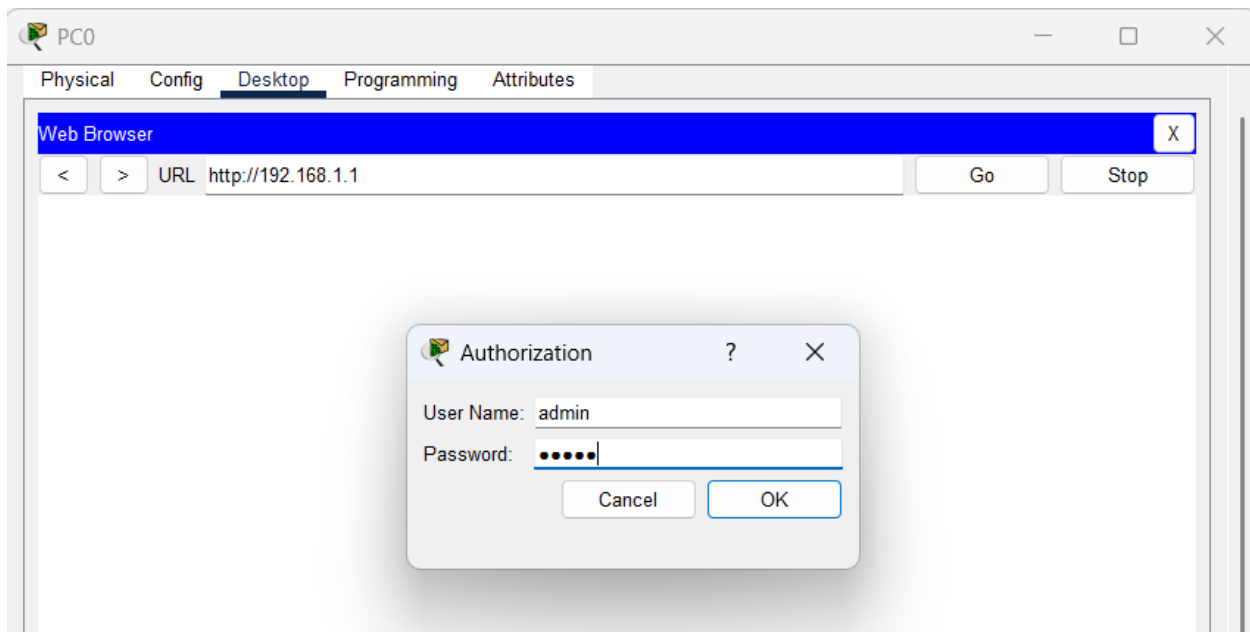


3. Part 1 – Examine External Network Configuration

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.



PC0

Physical Config **Desktop** Programming Attributes

Web Browser

< > URL http://192.168.1.1/Status_Router.asp

Wireless Tri-Band Home Router

Firmware Version: v0.9.7

Status Setup Wireless Security Access Restrictions Applications & Gaming Administration Status

Router Router Local Network Wireless Network

Router Information

Firmware Version:	v0.9.7
Current Time:	Not Available
Internet MAC Address:	0040.0B2D.0601
Host Name:	
Domain Name:	

Internet Connection

Connection Type:	Automatic Configuration - DHCP
Internet IP Address:	209.165.200.227
Subnet Mask:	255.255.255.224
Default Gateway:	209.165.200.225
DNS1:	209.165.200.226
DNS2:	209.165.200.226
DNS3:	
MTU:	1500
DHCP Lease Time:	1 days 0:0:0

IP Address Release IP Address Renew

Help...

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.

Status		Wireless Tri-Band Home Router					HomeRouter-PT-AC
Setup	Wireless	Security	Access Restrictions	Applications & Gaming	Administration	Status	
Router		Local Network				Wireless Network	
Local Network						Help...	
	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				
	<div>DHCP Client Table</div>						

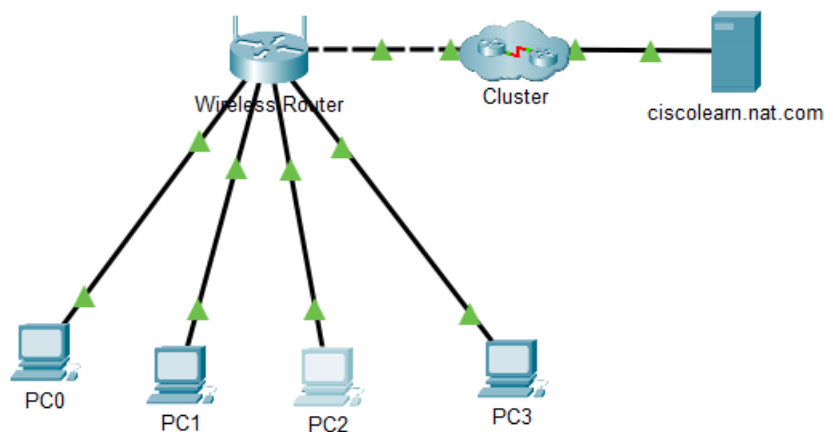
Figure 2: Local Network & DHCP Pool

Are these internal network addresses private or public?

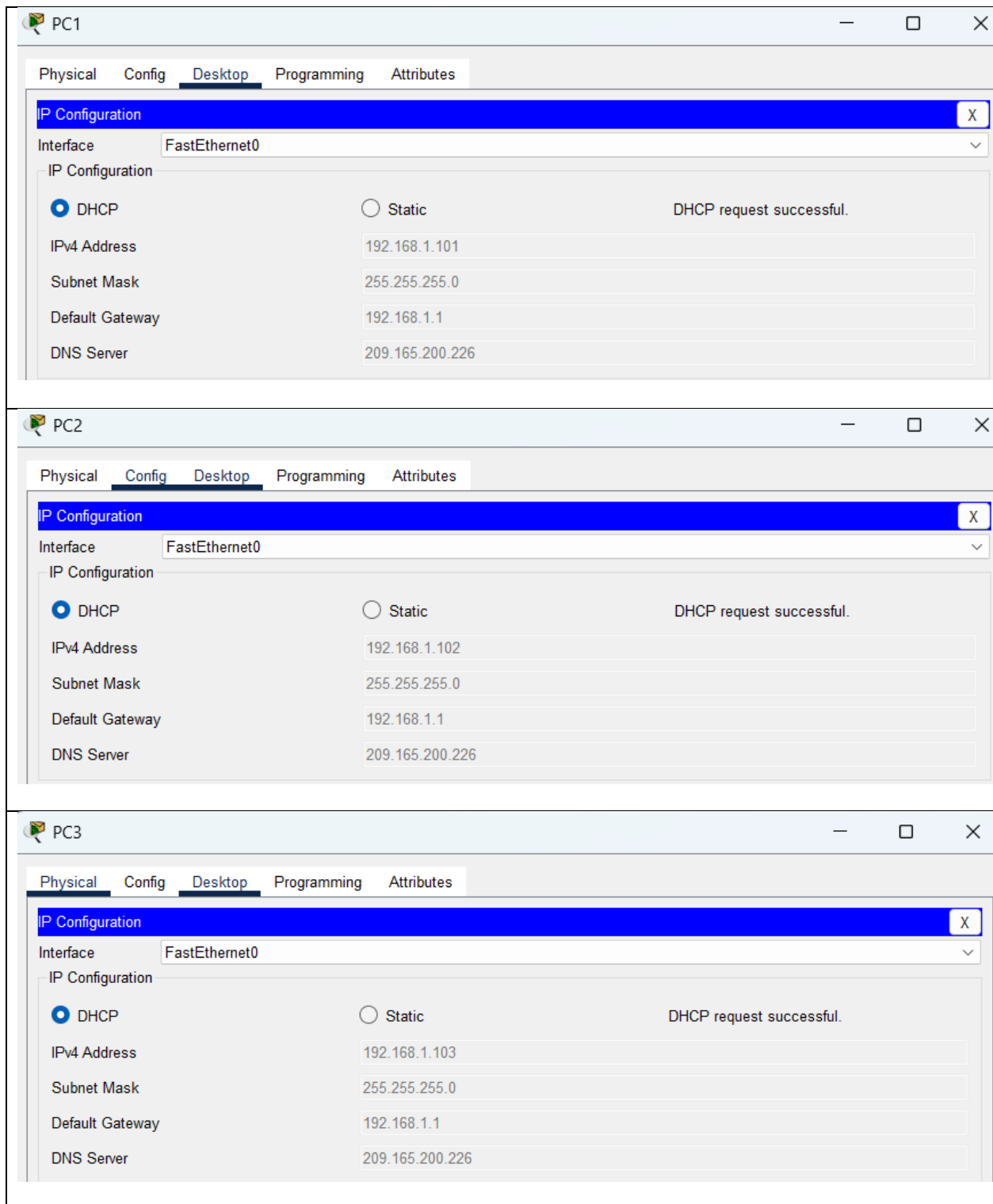
The internal IP addresses are private, used only inside the LAN

5. Part 3 – Connect Additional PCs

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

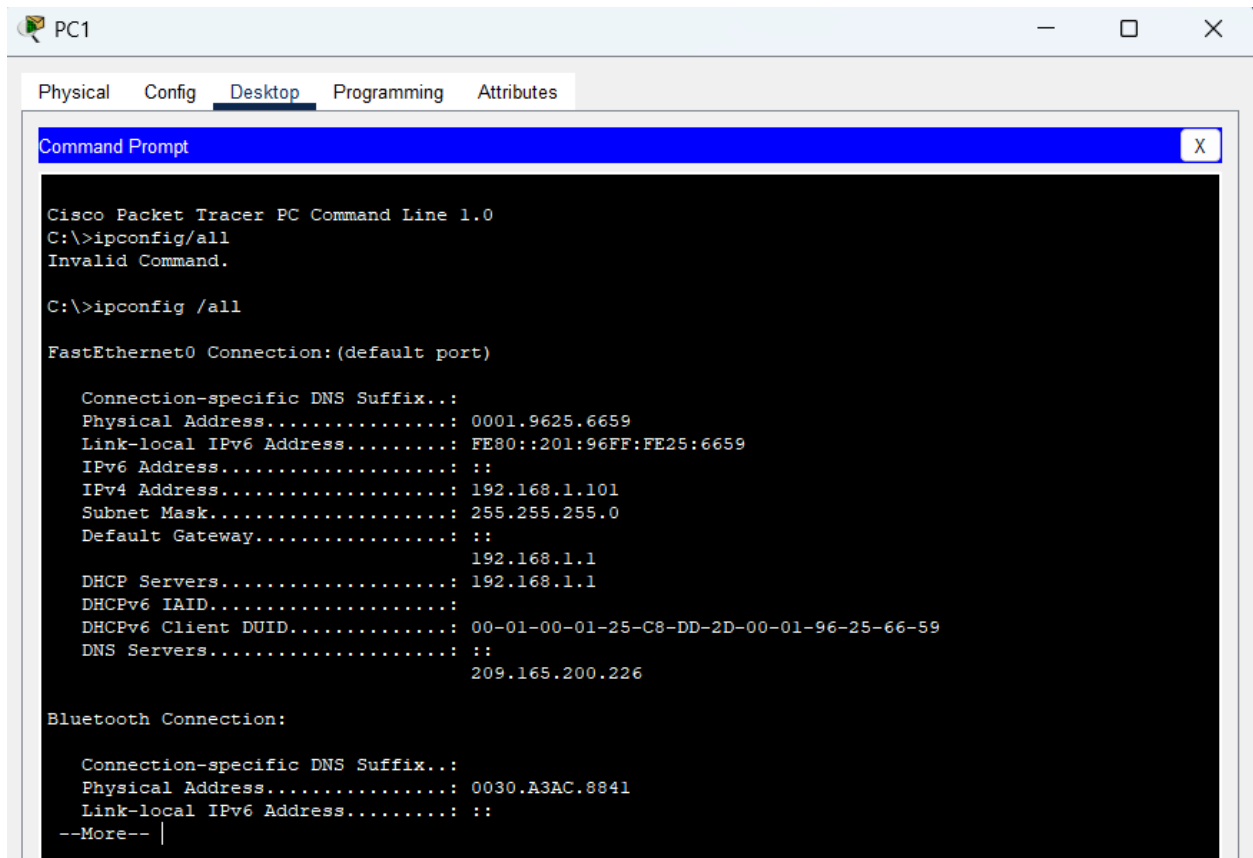


2. Configured each PC to use DHCP.



3. Verified IP configurations using:

`ipconfig /all`



The screenshot shows a window titled "PC1" with tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active, displaying a "Command Prompt" window. The Command Prompt shows the output of the `ipconfig /all` command, which displays network configuration details for both FastEthernet0 and Bluetooth connections. The FastEthernet0 connection shows an IPv4 address of 192.168.1.101 and a subnet mask of 255.255.255.0. The Bluetooth connection shows a physical address of 0030.A3AC.8841.

```
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

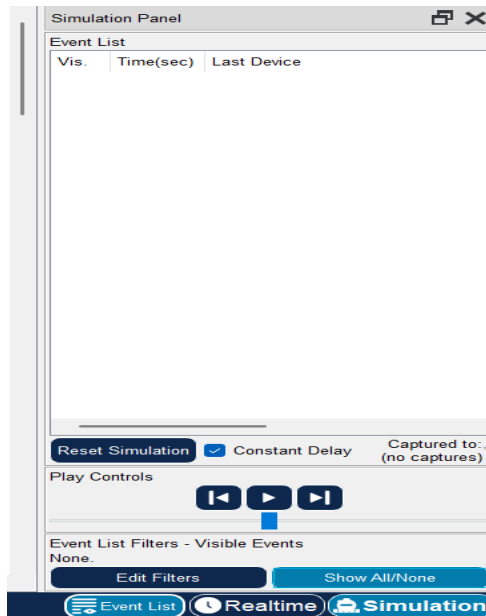
Bluetooth Connection:

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

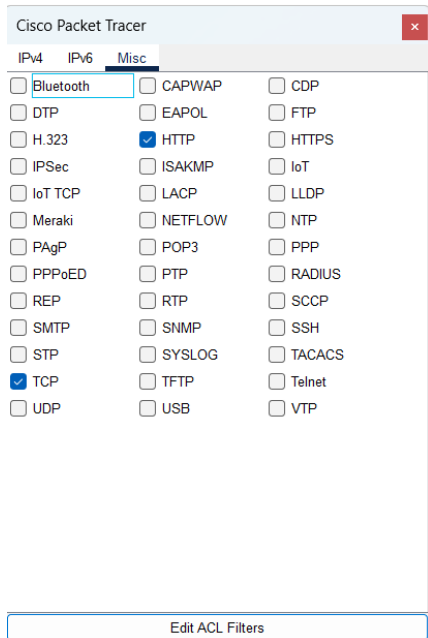
Figure 3: PC IP Config Results

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



Create Complex PDU

Source Settings

Source Device: PC0
Outgoing Port:
FastEthernet0 ☐ Auto Select Port

PDU Settings

Select Application: HTTP
Destination IP Address: 209.165.200.228
Source IP Address:
TTL: 32
TOS: 0
Starting Source Port: 1000
Destination Port: 80
Size: 0

Simulation Settings

☐ One Shot Time: 120 Seconds
☒ Periodic Interval: 120 Seconds

Create PDU

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

The image shows a 'Simulation Panel' window with a close button (X) in the top right corner. It contains an 'Event List' table, 'Reset Simulation' and 'Constant Delay' controls, 'Play Controls' with play/pause/stop buttons, 'Event List Filters - Visible Events' showing 'HTTP, TCP', and buttons for 'Edit Filters' and 'Show All/None'. At the bottom are three tabs: 'Event List' (selected), 'Realtime', and 'Simulation'.

Vis.	Time(sec)	Last Device
	0.002	--
	0.003	PC0
	0.304	--
	0.305	PC0
	0.306	Wireless Router
	0.307	Switch0
	0.308	ciscolearn.nat.com
	0.309	Switch0
	0.310	Wireless Router
	0.310	--
	0.311	PC0
	0.311	--
	0.312	PC0
	0.312	Wireless Router
	0.313	Wireless Router
	0.313	Switch0
Visible	0.314	Switch0

Reset Simulation ☒ Constant Delay Captured to: 0.314 s

Play Controls

Event List Filters - Visible Events
HTTP, TCP

Edit Filters Show All/None

Event List Realtime Simulation

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.

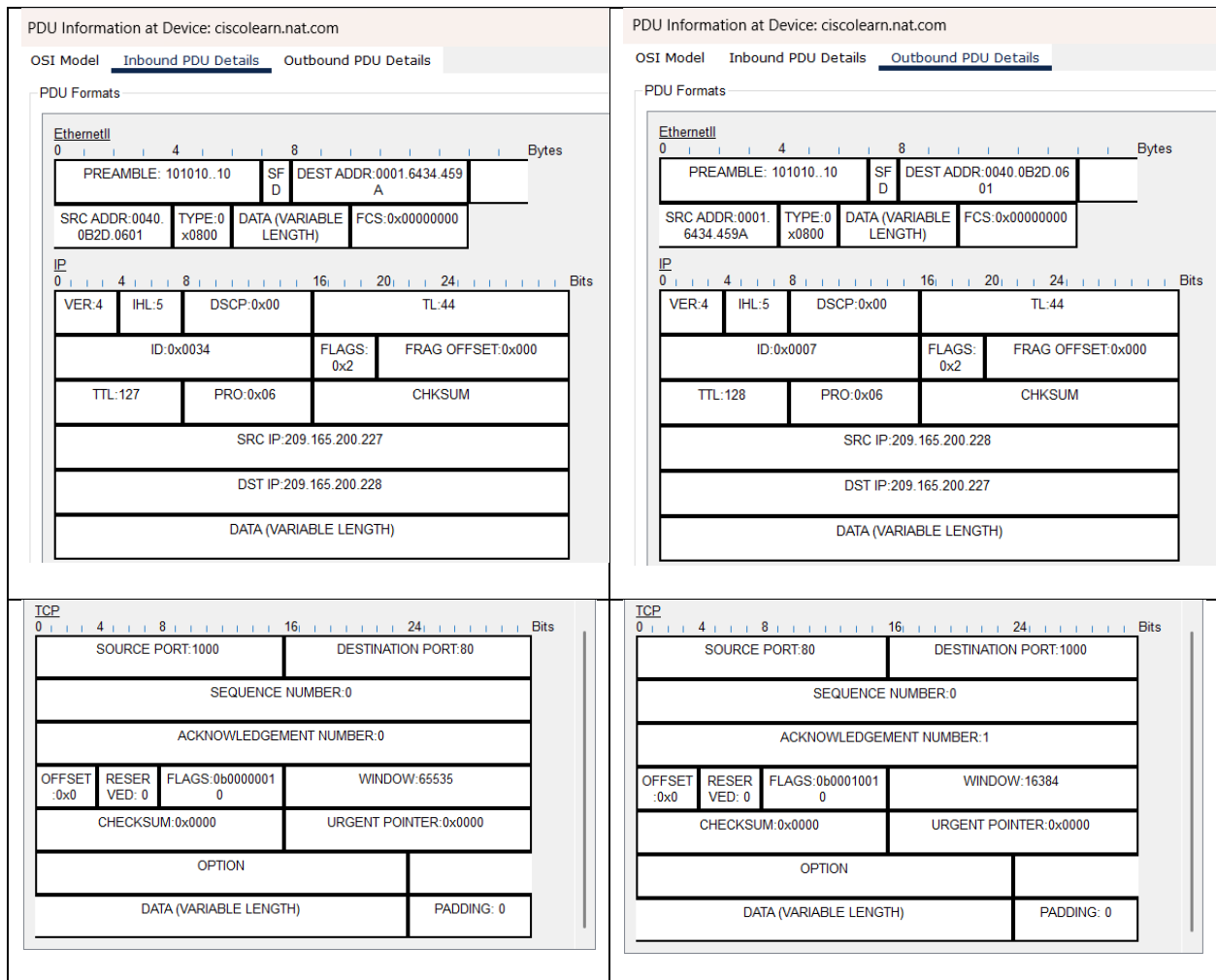


Figure 5: Inbound / Outbound PDU Header Comparison

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