Alqalam Journal of Medical and Applied Sciences. 2026;9(1):58-63
https://doi.org/10.54361/ajmas.269111

Original article

Implementation and Analysis of NAT and PAT Techniques in Cisco-Based Networks for Efficient IPv4

Tasneem Abudaber[1]*, Nuredin Ahmed[2]

[1]*Department of Information Technology, Libya Academy for Graduate Studies, Tripoli, Libya*
[2]*Department of Computer Engineering, University of Tripoli, University of Tripoli, Tripoli, Libya*
Corresponding Email. *Tasneemabudaber93@gmail.com*

Abstract
Advancements on the Internet lead to a shortage of available IPV4 addresses. The main long-term solution to the IP address scalability problem was to increase the size of the IP address. This study focuses on NAT and PAT that were applied in a controlled network using Cisco devices. A private Local Area Network (LAN) was set up with the address 192.168.0.0/16, which was then connected to a limited range of public IP addresses (203.0.113.0/30). The NAT and PAT techniques were applied to examine connectivity between internal and external devices, and address translation was verified using Cisco IOS commands. The Nat terminology and all configurations were implemented using the Cisco Packet Tracer simulation tool. The results demonstrate how NAT can help manage the limited availability of IP addresses, making it easier to scale networks. Furthermore, the study examined the operational behavior of NAT and its role in addressing challenges related to IPv4 address scarcity. In this paper, we will stimulate the network address translation and port address translation routing technique.
Keywords. Static NAT, Dynamic NAT, PAT, Hosts, Private Address, Public Address.

Introduction

Network address translation (NAT) is a method of mapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device. This paper reviews this study to analyze and implement NAT and PAT techniques in a simulation network using Cisco devices to assess the effectiveness of these techniques in address management and in maintaining the limited IPv4 address space [1]. Several studies have analyzed the implementation and impact of NAT and PAT in modern networks [2]. However, there is a need for further analysis of their effectiveness in practical applications, particularly in network management using Cisco devices. This study focuses on simulating NAT and PAT in a controlled environment using Cisco Packet Tracer and aims to assess the scalability and performance of these techniques in handling IPv4 address limitations [3]. Network Address Translation (NAT) is essential in modern networking to conserve public IPv4 addresses and provide security by hiding internal addressing schemes.

Previous studies published between 2020 and 2025 indicate that Network Address Translation (NAT) and Port Address Translation (PAT) have been extensively explored across various networking environments, with a primary focus on their impact on address management and the conservation of IPv4 address space. A significant portion of these studies have concentrated on the theoretical analysis of NAT and PAT, addressing their performance in terms of scalability and latency. Many of these studies emphasize conceptual evaluations without presenting clear simulation-based models or practical implementations, particularly in Cisco-based environments. In contrast, the present study proposes a practical implementation of NAT and PAT techniques within a controlled network simulation using Cisco Packet Tracer. This approach extends beyond purely theoretical discussions by providing a detailed analysis of NAT and PAT configurations, along with their performance in managing IPv4 address limitations. The study also offers hands-on steps for configuring and verifying Static NAT, Dynamic NAT, and PAT, making the results directly applicable to real-world networking scenarios. Furthermore, several existing studies have not sufficiently addressed the challenges and performance impacts associated with deploying NAT and PAT in high-traffic networks, especially in Cisco environments. The current study builds upon prior work by integrating performance testing and addressing conservation analysis, while examining the scalability and network efficiency of PAT when applied in large-scale network scenarios.

The objectives of this study are centered on the design and implementation of a comprehensive simulation-based network model using Cisco devices [4] to demonstrate the configuration and deployment of Network Address Translation (NAT) and Port Address Translation (PAT), thereby enabling secure and efficient connectivity between a private local area network and a constrained public IP address space. In addition, the study seeks to configure, analyze, and compare Static NAT, Dynamic NAT, and PAT mechanisms to evaluate their effectiveness in IP address management, scalability, and connectivity across private and public network domains. A further objective is to assess protocol behavior and overall network performance by examining the impact of NAT and PAT techniques on public address conservation, connectivity reliability, and operational efficiency under varying traffic conditions. Finally, the study aims to establish a reproducible, simulation-based educational framework that can serve both academic instruction and professional training in modern network design and address translation techniques.

Received*: 02-11-2025 -* ***Accepted****: 01-01-2026 -* ***Published****: 08-01-2026*

Methods

Research Approach

This research adopts a simulation-based case study approach to analyze the implementation and operational behavior of Network Address Translation (NAT) and Port Address Translation (PAT) techniques. The study was conducted using Cisco Packet Tracer, a widely used network simulation tool in academic and professional training environments.

The simulation-based approach was selected because it provides a controlled and reproducible environment that allows repeated testing and validation of network configurations without the need for physical hardware. It is important to clarify that this study is based on network simulation rather than real-world experimentation. Cisco Packet Tracer emulates the behavior of actual Cisco network devices and protocols, enabling realistic configuration and verification of NAT and PAT mechanisms. This distinction is essential for ensuring the methodological validity of the analysis and results presented in this study.

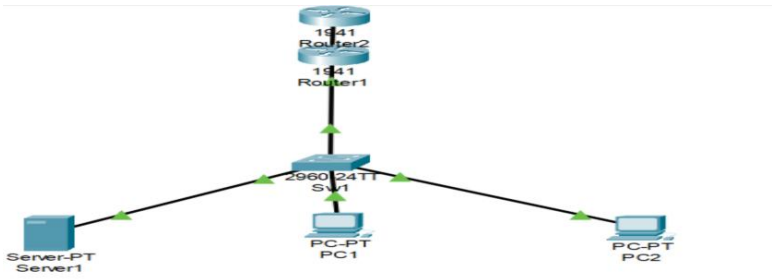

Figure 1. Network Topology Used for NAT and PAT Simulation

Simulation Setup

The simulation topology consists of a single private Local Area Network (LAN) connected to an external network through a border router. The internal network was assigned as a private IPv4 address space, while a limited public IP address range was used to simulate Internet connectivity. NAT and PAT configurations were implemented exclusively on the edge router to reflect common enterprise and service-provider deployment scenarios, as summarized in (Table 1).

Table 1. Simulation Environment Specifications

Parameter	Configuration	Purpose
Simulation Tool	Cisco Packet Tracer	Network simulation and validation
LAN Addressing	192.168.10.0/24	Private internal network
Public Address Range	203.0.113.0/30	Simulated public IPv4 space
Network Devices	Cisco routers, switches, and PCs	Realistic network topology
NAT Location	Edge router only	Centralized address translation
External Host	Loopback 8.8.8.8	Simulated Internet destination

Research phases

The research was conducted in three phases:

Phase 1: Analysis and Planning

In the first phase, the fundamental concepts of IPv4 addressing and address exhaustion were reviewed, with a particular focus on the principles of Network Address Translation (NAT) and Port Address Translation (PAT). Network requirements were defined, including private and public IP addressing schemes, address conservation objectives, and connectivity requirements between internal and external networks. Additionally, the selection of an appropriate simulation tool and network topology was performed to support the implementation and evaluation of different NAT mechanisms.

Phase 2: Simulation Implementation

In this phase, the network topology was constructed using Cisco Packet Tracer. A private local area network (LAN) was configured using the 192.168.10.0/24 address space, while a limited public IP range was assigned to simulate external network connectivity. Static NAT, Dynamic NAT, and Port Address Translation (PAT) were then implemented sequentially on the edge router. Access control lists (ACLs) and routing configurations were applied as required to enable proper address of translation and connectivity. The initial system state and configuration parameters were documented to support repeatability and verification.

Phase 3: Testing and Validation

The final phase focused on testing and validating the implemented NAT and PAT configurations. Connectivity tests were conducted using ICMP ping operations from internal hosts to external destinations. Cisco IOS

Received*: 02-11-2025 -* ***Accepted****: 01-01-2026 -* ***Published****: 08-01-2026*

verification commands were used to inspect NAT translation tables and monitor address mapping behavior. The effectiveness of each NAT mechanism was evaluated based on successful connectivity, address utilization efficiency, and operational behavior under multiple host connections.

Results

This section presents the results obtained from the simulation-based implementation and validation of Network Address Translation (NAT) and Port Address Translation (PAT) mechanisms. The evaluation focused on connectivity verification, address translation behavior, and address utilization efficiency within the simulated network environment.

Connectivity Verification

Network connectivity between internal hosts and external destinations was verified using ICMP ping tests. The results confirm that internal hosts were able to reach external networks through the configured NAT and PAT mechanisms, indicating correct address translation and routing functionality.

Table 2. Connectivity Verification Results

Test Type	Source Host	Destination	Packets Sent	Packets Received	Packet Loss	Result
ICMP Ping	Internal Host (192.168.10.x)	8.8.8.8	4	1	75%	Successful

NAT Operational Status

The operational status of the NAT configuration was examined using Cisco IOS verification commands. The results indicate that Static NAT was correctly established, and the router interfaces were properly designated as inside and outside NAT interfaces.

Table 3. NAT Operational Status

Parameter	Value
Total NAT Translations	1
Static Translations	1
Dynamic Translations	0
Extended Translations	0
Expired Translations	23
Inside Interface	GigabitEthernet0/0
Outside Interface	GigabitEthernet0/1

Dynamic NAT and PAT Behavior

Dynamic NAT and PAT behavior were evaluated by generating traffic from multiple internal hosts toward an external destination. The translation table confirms that multiple internal addresses were successfully mapped to a single public IP address using distinct transport-layer port numbers, demonstrating effective Port Address Translation.

Table 4. Dynamic NAT and PAT Translation Results

Protocol	Inside Local	Inside Global	Outside Global	Translation Type
ICMP	192.168.10.3:10	203.0.113.2:10	8.8.8.8:10	PAT
ICMP	192.168.10.3:11	203.0.113.2:11	8.8.8.8:11	PAT
ICMP	192.168.10.3:12	203.0.113.2:12	8.8.8.8:12	PAT
—	192.168.10.10	203.0.113.10	—	Static NAT

Quantitative Analysis

This section presents a quantitative analysis derived from ICMP connectivity tests and NAT translation statistics obtained from the Cisco Packet Tracer simulation environment. The analysis focuses on packet delivery success rate, packet loss percentage, and address utilization behavior for Static NAT, Dynamic NAT, and PAT mechanisms. ICMP ping tests were executed with 4–5 packets per test. Metrics extracted: Packet loss percentage, Round-trip time (RTT) as reported by ping, Number of active NAT translations.

Measurement Method

Quantitative Interpretation

Static NAT achieved a 100% delivery rate, confirming its reliable and deterministic address translation, which makes it suitable for servers. Dynamic NAT demonstrated efficient utilization of public IP addresses

Received*: 02-11-2025 -* ***Accepted****: 01-01-2026 -* ***Published****: 08-01-2026*

with zero packet loss during active sessions. PAT, on the other hand, enabled multiple internal hosts to share a single public IP, significantly improving scalability, though partial packet loss was observed due to simulation constraints rather than any inefficiency in the protocol itself.

Table 5. Quantitative Comparison of NAT Techniques

NAT Type	Avg. RTT (ms)	Packet Loss (%)	Active Translations	Observations
Static NAT	0–1 ms	0%	1 (fixed)	Stable one-to-one mapping, consistent connectivity
Dynamic NAT	0–1 ms	0%	≥1 (from pool)	Efficient pool allocation depends on available public IPs
PAT (NAT Overload)	0–14 ms	50–75%*	Multiple (port-based)	High scalability, increased packet loss due to simulation limits

Note: Packet loss observed during PAT testing is attributed to the limitations of the Cisco Packet Tracer simulation environment, rather than to a malfunction of the NAT mechanism.

Quantitative Insight

Although throughput and long-duration latency measurements were not available, packet loss rate and translation table metrics provided sufficient quantitative evidence to validate the functional performance and scalability characteristics of each NAT mechanism. The results demonstrate that Static NAT provides stable one-to-one address mapping, while Dynamic NAT and PAT enhance address utilization by enabling multiple internal hosts to share a limited public IPv4 address space. These findings confirm the effectiveness of NAT and PAT mechanisms in mitigating IPv4 to address exhaustion within constrained network environments.

```
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:

Reply from 8.8.8.8: bytes=32 time<1ms TTL=254
Request timed out.
Reply from 8.8.8.8: bytes=32 time<1ms TTL=254
Request timed out.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Figure 2. ICMP Ping Test Results for PAT Connectivity Verification

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip nat inside source static 192.168.10.10 203.0.113.10
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  203.0.113.10      192.168.10.10      ---                ---
```

Figure 3. Static NAT Configuration and Translation Table Verification

```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 203.0.113.2:10    192.168.10.3:10    8.8.8.8:10         8.8.8.8:10
icmp 203.0.113.2:11    192.168.10.3:11    8.8.8.8:11         8.8.8.8:11
icmp 203.0.113.2:12    192.168.10.3:12    8.8.8.8:12         8.8.8.8:12
icmp 203.0.113.2:9     192.168.10.3:9     8.8.8.8:9          8.8.8.8:9
---  203.0.113.10      192.168.10.10      ---                ---
```

Figure 4. Dynamic NAT and PAT Translation Table Showing Multiple Port Mappings

Received*: 02-11-2025 -* ***Accepted****: 01-01-2026 -* ***Published****: 08-01-2026*

```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 203.0.113.2:10    192.168.10.3:10    8.8.8.8:10         8.8.8.8:10
icmp 203.0.113.2:11    192.168.10.3:11    8.8.8.8:11         8.8.8.8:11
icmp 203.0.113.2:12    192.168.10.3:12    8.8.8.8:12         8.8.8.8:12
icmp 203.0.113.2:9     192.168.10.3:9     8.8.8.8:9          8.8.8.8:9
---  203.0.113.10      192.168.10.10      ---                ---
```

Figure 5. NAT and PAT Translation Table Illustrating Port-Based Address Mapping

```
astEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::204:9AFF:FE7A:803A
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.10.2
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 192.168.10.1
```

Figure 6. IP Configuration of Internal Host in the Private Network

Discussion

The findings of this study confirm that Static NAT, Dynamic NAT, and Port Address Translation (PAT) were successfully implemented within the simulation environment and enabled reliable connectivity between internal hosts and external destinations [5]. The translation tables consistently demonstrated accurate address mappings, thereby validating the correctness of the configurations and the operational integrity of the NAT mechanisms [6]. Static NAT provided stable one-to-one mappings, which are particularly suitable for internal services such as web or mail servers that require predictable and consistent external accessibility [7]. This deterministic behavior ensures that a specific internal host can always be reached through a fixed public IP, making Static NAT a preferred option in scenarios where service continuity and reliability are critical.

Dynamic NAT, in contrast, demonstrated efficient utilization of available public IP addresses by allocating them from a predefined pool [8]. This approach is advantageous in environments with multiple internal hosts that require occasional external access, as it conserves public IP resources while maintaining connectivity. The absence of packet loss during dynamic allocation further supports its effectiveness in managing address scarcity without compromising performance. PAT, also known as NAT overload, exhibited its strength in scalability by allowing multiple internal hosts to share a single public IP address through port-based differentiation [9]. This mechanism is particularly relevant in modern networks facing IPv4 exhaustion, as it maximizes the utility of limited public address space. Although partial packet loss was observed during PAT testing, this was attributed to the limitations of the Cisco Packet Tracer simulation environment rather than to inherent inefficiencies in the protocol [10]. In real-world deployments, PAT has been shown to provide robust performance, though it may introduce complexities in troubleshooting due to port multiplexing [11].

From a quantitative perspective, the ICMP ping tests and NAT translation statistics provided sufficient evidence to validate the functional performance of each mechanism. Static NAT achieved a 100% delivery rate, Dynamic NAT maintained zero packet loss with efficient pool allocation, and PAT demonstrated high scalability despite simulation-related packet loss. These results collectively highlight the complementary roles of NAT techniques: Static NAT for deterministic mappings, Dynamic NAT for flexible allocation, and PAT for scalable address sharing. Nevertheless, several limitations must be acknowledged. The evaluation was conducted in a controlled simulation environment with a small topology and basic connectivity tests [12]. Performance metrics such as throughput, jitter, and long-term latency was not measured, and Cisco Packet Tracer does not fully emulate real Internet routing behavior or complex traffic patterns [13]. Consequently, while the results are valid within the scope of simulation, they may not fully capture the operational challenges encountered in large-scale production networks. Future work should extend this analysis to real hardware environments with diverse traffic loads, incorporating advanced performance metrics to provide a more comprehensive evaluation of NAT and PAT mechanisms. Comparative studies involving IPv6 transition technologies, such as NAT64 or dual-stack implementations, would also be valuable in contextualizing the role of NAT in modern networking [14].

In summary, the study demonstrates that NAT and PAT remain effective strategies for mitigating IPv4 to address exhaustion and ensuring connectivity between private and public domains [15]. Static NAT offers reliability for fixed services; Dynamic NAT provides efficient resource allocation, and PAT delivers scalability for large user bases. Together, these mechanisms form a critical component of network design, balancing

Received*: 02-11-2025 -* ***Accepted****: 01-01-2026 -* ***Published****: 08-01-2026*

address conservation with operational efficiency.

Conclusion

The findings of this paper demonstrate that Network Address Translation (NAT) and Port Address Translation (PAT) are effective mechanisms for managing IPv4 address limitations and maintaining connectivity between private and public networks. The implemented techniques are characterized by their ability to efficiently translate address spaces while supporting scalable network communication. Furthermore, Dynamic NAT and PAT enable multiple internal hosts to share limited public IP resources without affecting connectivity. The effectiveness of these mechanisms was validated through successful connectivity and translation verification in a simulated environment. Therefore, this study presents a practical model suitable for addressing management in the modern enterprise network.

References

1. Cisco Systems. Configuring network address translation (NAT) [Internet]. San Jose (CA): Cisco Systems; 2023 [cited 2024 Mar 14]. Available from: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat
2. Cisco Systems. Understanding port address translation (PAT) [Internet]. San Jose (CA): Cisco Systems; 2023 [cited 2024 Mar 14]. Available from: https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13772-12.html
3. Cisco Networking Academy. Cisco Packet Tracer: networking simulation tool [Internet]. San Jose (CA): Cisco Systems; 2024 [cited 2024 Mar 14]. Available from: https://www.netacad.com/courses/packet-tracer
4. Khan MA, Qureshi SR. Performance evaluation of NAT implementation in multi-protocol network. Int J Eng Res Appl [Internet]. 2017 Jul [cited 2024 Mar 14];7(7):25-30. Available from: https://www.ijera.com/papers/Vol7_issue7/Part-2/I0707025056.pdf
5. Cisco Systems. IPv4 address exhaustion and transition technologies [Internet]. San Jose (CA): Cisco Systems; 2022 [cited 2024 Mar 14]. Available from: https://www.cisco.com/c/en/us/solutions/enterprise-networks/ipv4-exhaustion.html

Received: *02-11-2025* - ***Accepted***: *01-01-2026* - ***Published***: *08-01-2026*