ANALYSIS THE DUAL STACK, TUNNELING AND NAT PT USING GNS3 &JPERF BETWEEN IPV4&IPV6 NETWORKS

تحليل أداء آليات التوصيل بين شبكات IPv4 وشبكات IPv6 (DUAL STACK, TUNNELING AND NAT PT) باستخدام GNS3 &JPERF

Musab Ali Saleh El Nefati
mosabalnfatti@gmail.com

Essam Mohamed R Elosta
essamrtw@yahoo.com

RAMADAN M. A. KHALIFA
ramadanamharee@gmail.com

Abstract

Each node in the network needs an IP address to commute between hosts. The IPv4 address number in use so far is too restricted to even think of dealing with the new concerns of IP addresses، Whereas, version 4 of the network addresses currently in use is too limited to handle new requests from IP addresses.

Therefore, IPv6 is designed to provide sufficient address space for the current and future demand for the growth of the Internet, and for communication between networks whose addresses have been updated to IPv6 and networks with old IPv4 addresses, one of the three mechanisms must be used: Dual Stack, Tunneling, NAT-PT as it is impossible to communicate between networks IPv4. IPv6 without using these mechanisms.

This paper aims to analyze the mechanisms of Dual Stack, Tunneling and NAT-PT performance during communication between IPv6 network and IPv4 network analyzed using GNS3 and JPerf in emulation system closer to the working reality than any previous studies. The three mechanisms Dual Stack, The Tunneling and NAT-PT were tested to assess the complexity, advantages and disadvantages of each method in terms of response time (latency), packet loss and throughput. Implementation work is carried out according to similar scenarios and the conclusion of this study is that the Dual Stack mechanism is the most popular and simplest path between IPv6 and IPv4 freely without developing systems. The Dual Stack is suitable for specialized internet organizations, corporate systems, and home clients. While the Tunneling mechanism is suitable for Internet service providers, corporate systems and servers, while NAT-PT faces the most noticeable rates of packet misfortune due to the late response time of the packet as NAT-PT gives the maximum inactivity, while the Dual Stack mechanism gives moderate Tunneling mechanism is less inactivity. As for the recommendations, the Tunneling Mechanism technology includes some security issues that IP Security IPSec can understand. This is why we recommend using Tunneling with IPSec for the purpose of security advancement during communication between IPv4 and IPv6.

Keywords: IPv6, IPv4, dual stack, tunnel, translation

الملخص

تحتاج كل عقدة في الشبكة إلى عنوان IP للتنقل بين المضيفين. رقم العنوان الخاص بـ IPv4 المستخدم حتى الآن مقيد للغاية بحيث لا يمكن حتى التفكير في التعامل مع الاهتمامات الجديدة لعناوين

IP، حيث أن الإصدار الرابع من عناوين الشبكة المستخدم حاليًا محدود جدًا بحيث لا يمكنه التعامل مع الطلبات الجديدة من عناوين IP.

لذلك تم تصميم IPv6 لتوفير مساحة عنوان كافية للطلب الحالي والمستقبلي لنمو الإنترنت، وللتواصل بين الشبكات التي تم تحديث عناوينها لـ IPv6 والشبكات ذات العناوين القديمة IPv4 يجب استخدام احدى الاليات الثلاثة Dual Stack ,Tunneling , NAT–PT حيث أن من المستحيل التواصل بين الشبكات IPv4–IPv6 من غير استخدام هذه الاليات .

يهدف هذا البحث إلى تحليل آليات أداء Dual Stack ,Tunneling and NAT–PT اثناء الاتصال بين شبكة IPv6 وشبكة IPv4 التي يتم تحليلها باستخدام GNS3 و JPerf في نظام المحاكاة الأقرب لحقيقة العمل من أي دراسات سابقة.

تم اختبار الآليات الثلاثة The Tunneling and NAT–PT ،Dual Stack لتقييم مدى تعقيد ومزايا وعيوب كل طريقة من حيث ،وقت الاستجابة، فقدان الحزمة ، الإنتاجية. يتم تنفيذ أعمال التنفيذ وفقًا لسيناريوهات متشابهة واستنتاج هذه الدراسة هو أن آلية الـ Dual Stack هي أشهر وأبسط مسار بين IPv6 و IPv4 بحرية دون تطوير أنظمة. الـ Dual Stack مناسب لمنظمات الإنترنت المتخصصة وأنظمة الشركات والعملاء المنزليين. بينما آلية الـ Tunneling مناسبة لمقدمي خدمات الإنترنت وأنظمة الشركات والخوادم ، بينما تواجه آلية الـNAT–PT أكثر المعدلات الجديرة بالملاحظة من سوء حظ الحزمة بسبب وقت الاستجابة المتأخر للحزمة حيث تعطي آلية الـ NAT–PT أقصى درجات الخمول ، بينما تعطي آلية الـ Dual Stack المعتدل وتعطي آلية الـ Tunneling أقل سكون. بالنسبة للتوصيات ، تشتمل تقنية آلية الـ Tunneling على بعض مشكلات الأمان التي يمكن أن يفهمها (IP Security IPSec). لهذا نوصيَ باستخدام آلية الـ Tunneling مع (IPSec) لغرض التقدم الامني اثناء الاتصال بين الـIPv4 و IPv6 .

1. Background

IP version 4 is the dominant version for several years, but lately, it has experienced a number of limitations, including address space given the exponential growth of the Internet size and the number of devices currently connected. IPv6 , the new version of the protocol, has not only addressed all the issues related to its predecessor. But it has also added numerous new functions essential for the complex network environment of today, including the auto-configuration, a huge address space of 128 bits instead of 32 bits in IPv4, a better bandwidth management using multicast and anycast, a better quality of service support for all applications, in mobility, and an integrated security by default. In addition, the network infrastructure is currently still in IPv4, and therefore the transition to IPv6 is not an overnight project [1]. The subject of the translation to IPv6 is discussed for years given the limited address space problem in IPv4 because of the exponential growth of Internet size and number of connected equipment at the current time. In the first instance, we performed a comparative study of the mechanisms of transition from IPv4 to IPv6 [2] .Though previous works have been done on the comparison and the analyzing between these mechanisms, but by simulation tools not emulation tools and still many problems not resolved yet, calling for huge challenges on IPv6 transitions research. In this paper, the analysis has been done after implement the networks one by one for each performances [3] [4] [5] [6].

2. Problem Statement

Based on the description in the background above, the formulation of the problem of the research is the performance of Dual Stack, Tunneling and Translation between IPv6 Network and IPv4 Network using emulation system more than simulation system are analyzed:

How the performance of dual stack, tunneling, and translation are analyzed?

How the performance of dual stack, tunneling, and translation in emulation system?

Purpose of this study to analyze dual stack, tunneling, and translation performance that used to communicate with IPv6 and IPv4 nodes independently without changing networks. which is analyzed using GNS3 and JPerf in emulation system.

3. System Method

The transition between IPv4 Internet and IPv6 Internet will be a long process as long as the two protocols coexist. Various transition strategies can be divided into three categories, including dual stack, tunneling and translation mechanisms. In this research to analyzed the transition strategy IPv4 to IPv6 will use GNS3 and JPERF.

The Implementation agreements have been concluded between the head office and the branches of an enterprise through a public network (Internet Service Provider). Three model samples were tested in the laboratory to assess the complexity, advantages and disadvantages of each method. The implementation work is carried out according to two scenarios by applying three methods such as the 6to4 manual tunnel and the double stack.

- Method Scenario 1: 6to4 manual tunnel.
- Method Scenario 2: Dual stack.
- Method Scenario 3: Translation NAT-PT

- The equipment that will be used are:

- Router: Cisco 2800 Series with Cisco IOS Release 12.4 (4) T8.
- Client: Windows with a IP.

a. Scenario 1 6to4 manual tunnel

1) Physical connection

The network will be built as the (Figure 1).

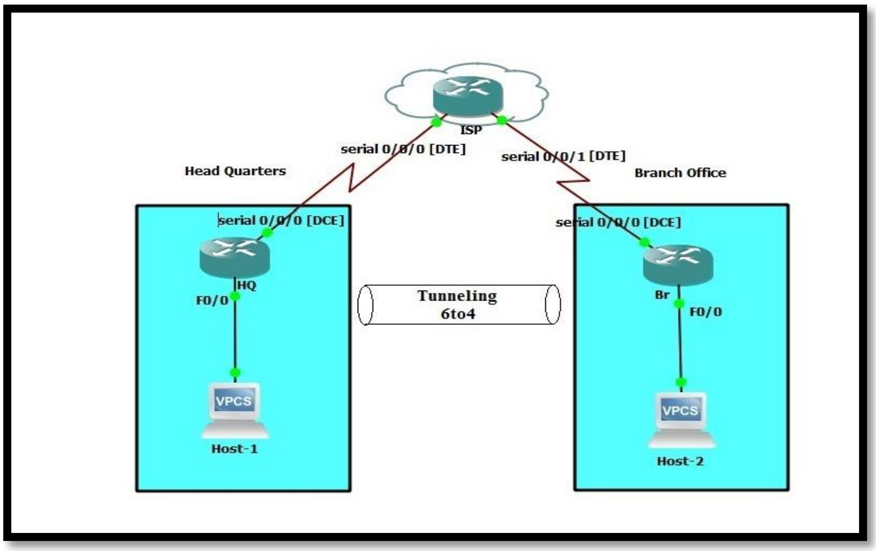

Figure1. Tunneling Topology

2) IP Address Scheme

Table 1. Host 1 and 2 IP Address [8]

Host	IPv6 address	IPv6 Gateway address
Host 1	FEC0:87:1:3::2/64	FEC0:87:1:3::1/64
Host 2	FEC0:87:1:4::2/64	FEC0:87:1:4::1/64

Table 2. Headquarters', ISP and Branch IP Addresses [8]

Criteria	Interface	IPv4 address	IPv6 address
Headquarter	FastEthernet 0/0	--	FEC0:87:1:3::1/64
	Serial 0/0/0	192.168.11.1/30	--
	Loopback 0	190.168.5.1/24	FEC0::11:1/128
	Tunnel 0	--	FEC0::12:1/128
ISP	Loop back 0	190.168.6.1/24	--
	Serial 0/0/0	192.168.11.2/30	--
	Serial 0/0/1	192.168.12.1/30	--
Branch	Loopback 0	190.168.7.1/24	FEC0::13:1/128
	Serial 0/0/0	192.168.12.2/30	--
	FastEthernet 0/0	--	FEC0:87:1:4::1/64
	Tunnel 0	--	FEC0::4:4/128

b. Scenario 2 (Dual stack)

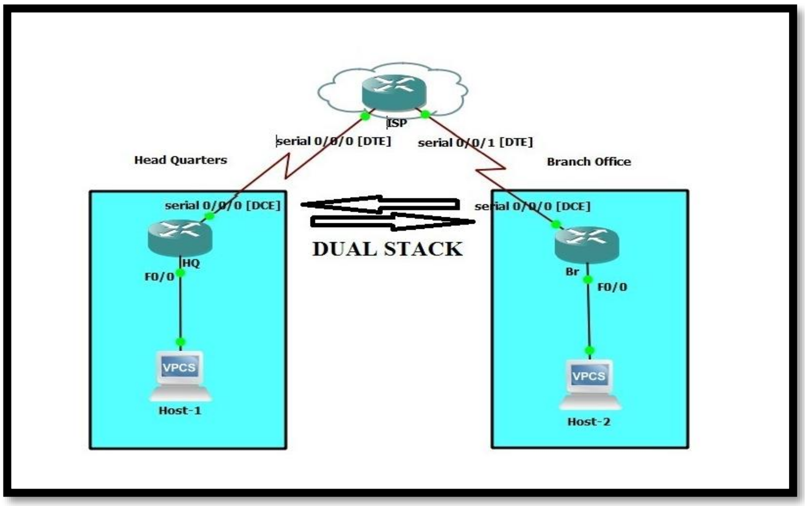

Figure 2. Dual Stack Topology

1) Physical connection
The physical settings of second Scenario have done by the same method as the first Scenario as the (Figure 2).
2) IP Address Scheme

Table 3. Host 1 and 2 IP Address [8]

Host	Criteria	IPv4 address	IPv6 address
Host 1	Ethernet	192.168.14.10/24	FEC0:87:1:3::2/64
	Gateway address	192.168.14.1/24	FEC0:87:1:3::1/64
Host 2	Ethernet	192.168.13.20/24	FEC0:87:1:4::2/64
	Gateway address	192.168.13.1/24	FEC0:87:1:4::1/64

Table 4. Headquarters', ISP and Branch IP Addresses [8]

Criteria	Interface	IPv4 address	IPv6 address
Headquarter	FastEthernet 0/0	192.168.14.1/24	FEC0:87:1:3::1/64
	Serial 0/0/0	192.168.11.1/30	2001:2:11::1/112
	Loopback 0	190.168.5.1/24	FEC0::11:1/128
ISP	Loopback 0	190.168.6.1/24	FEC0::12:1/128
	Serial 0/0/0	192.168.11.2/30	2001:2:11::2/112
	Serial 0/0/1	192.168.12.1/30	2001:22:11::1/112
Branch	Loopback 0	190.168.7.1/24	FEC0::13:1/128
	Serial 0/0/0	192.168.12.2/30	2001:22:11::2/112
	FastEthernet 0/0	192.168.13.1/24	FEC0:87:1:4::1/64

c. Scenario 3 (Translation)

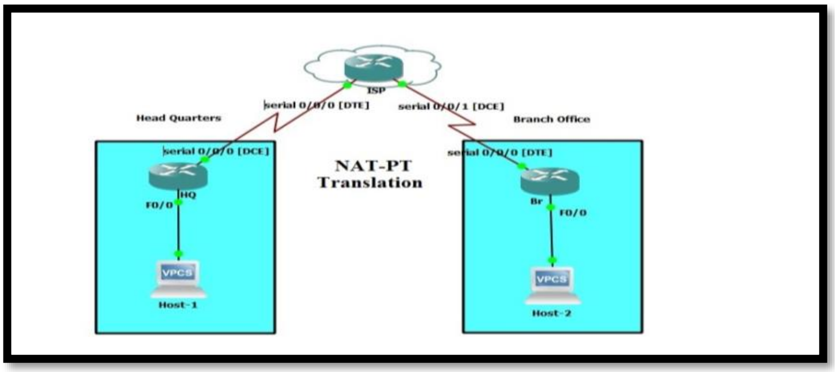

Figure 3.NAT-PT Topology

1) Physical connection
   The network will be built as (Figure 3).

   .

2) IP Address

Table 5. Host 1 and 2 IP Address [9]

Host	Criteria	IPv4 address	IPv6 address
Host 1	Ethernet	192.168.13.10/24	--
	Gateway address	192.168.13.1/24	--
Host 2	Ethernet	--	FEC0:87:1:4::2/64
	Gateway address	--	FEC0:87:1:4::1/64

Table 6. Headquarters', ISP and Branch IP Addresses [9]

Criteria	Interface	IPv4 address	IPv6 address
Headquarter	Fast Ethernet 0/0	192.168.13.1/24	--
	Serial 0/0/0	192.168.11.1/30	--
ISP	Serial 0/0/0	192.168.11.2/30	--
	Serial 0/0/1	--	2001:2:22::1/112
	ipv6 NAT v4v6 source	192.168.11.3	2001::960B:202
	ipv6 NAT v6v4 source	150.11.3.1	FEC0::13:1/128
	ipv6 nat prefix		2009::/96
Branch	Loopback 0		FEC0::13:1/128
	Serial 0/0/0	--	2001:2:22::2/112
	Fast Ethernet 0/0	--	FEC0:87:1:4::1/64

3. Results and Analysis

3.1. Testing Result

3.1.1. Testing for 6to4 Tunnel (Scenario 1)

A ping test is a command to test the connections between two nodes of a network. The use of the latency ping command between two nodes will be explained. Ping results between host1 to host2 between host1 to host2 (IPv6:FEC0:87:1:4::2) to determine latency and packet loss over of 100 packages the following (Figure 4 and 5):

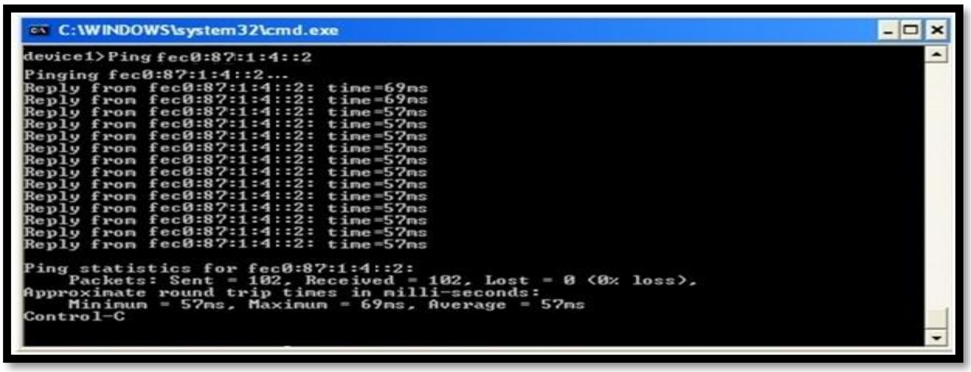

Figure 4. Ping Test Result of Scenario 1[a]

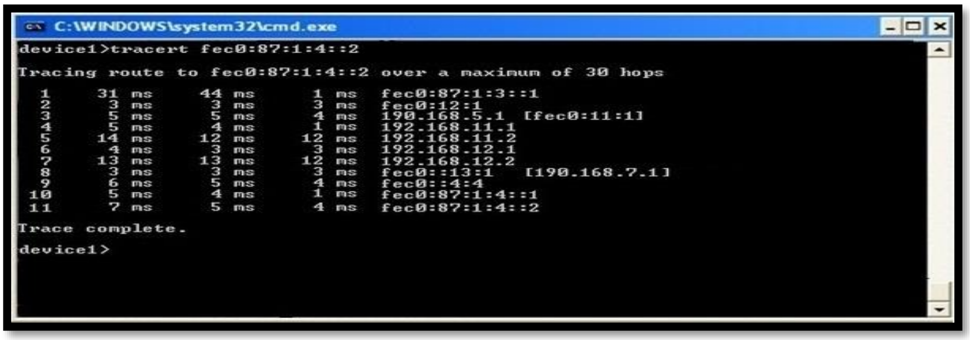

Figure 5. Ping Test Result of Scenario 1[b]

Table 7. Ping Test Result

Source Host 1	Destination Host 2
Packets Sent	102
Packets Received	102
Loss	0

Table 8. Latency Test Result

Level	Latency MS
Minimum	57
Maximum	69
Average	57

Here per a ping testing which in figure (4) we got the results in the table (7) the result got by send and receive packets of TCMP from node to node from IPv4 to IPv6 ,and the size of the packets created by the own network, Depending on the traffic and the number of the nodes , here sent 102 packets and received 102 packets so there is no Packet loss, but for the latency can see from the table (8) the time of the mechanism the highest time is 69ms and the lowest time is 57ms then the average is 57ms.

3.1.2. Testing for dual stack (Scenario 2)

Figure 6 and 7. below shows a ping test in scenario 2 between host1 to host 2 (FEC0:87:1:4::2) to determine the latency and the loss of packets made for more than 100 packages.

Here per a ping testing which in figure (6 and 7) we got the results in the table (9) the result got by send and receive packets of TCMP from node to node from IPv4 to IPv6 ,and the size of the packets created by the own network, Depending on the traffic and the number of the nodes , here sent 105 packets and received 105 packets so there is no Packet loss, but for the latency can see from the table (10) the time of the mechanism the highest time is 57ms and the lowest time is 57ms then the average is 46ms.

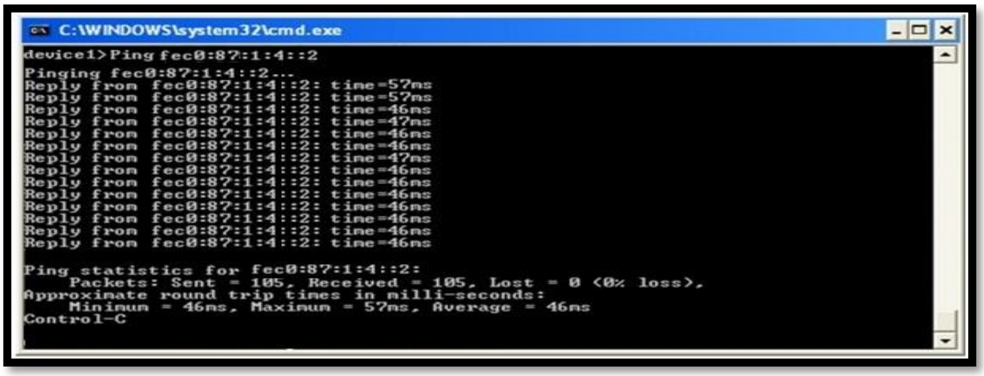

Figure 6. Ping Test Result of Scenario 2[a]

Figure 7. Ping Test Result

Table 9. Ping Test Result

Source	Destination
Packets Sent	105
Packets Received	105
Loss	0

Table 10. Latency Result

Level	Latency MS
Minimum	46
Maximum	57
Average	46

3.1.3. Ping Test Ping Test for Translation NAT-PT (Scenario 3)

Figure 8 and 9 below shows a ping test in scenario 3 between host1 to host 2 (IPv6:FEC0: 87:1:4::2) to determine the latency and the loss of packets made for more than 100 packages.

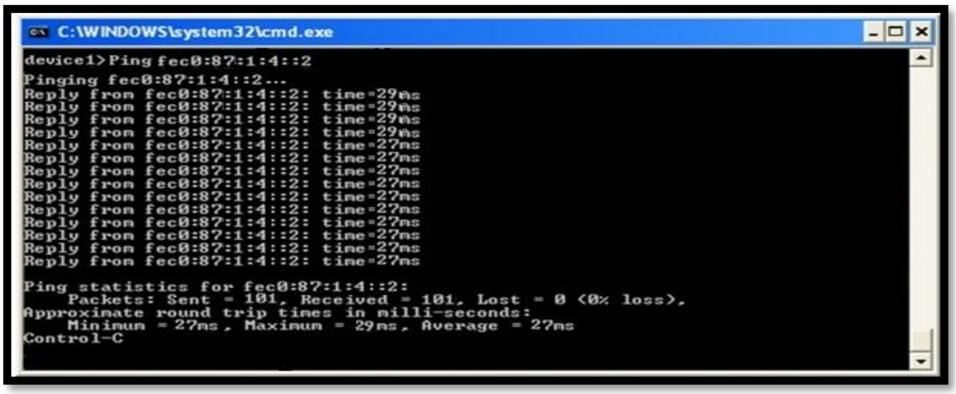

Figure 8. Ping Test Result

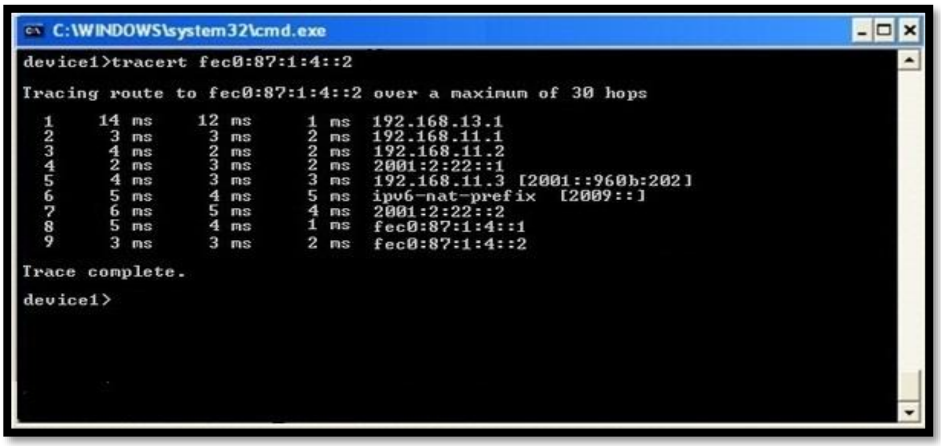

Figure 9. Ping Test Result

Table 11. Ping Test Result

Source Host 1	Destination Host2
Packets Sent	101
Packets Received	101
Loss	0

Table 12. Latency Result

Level	Latency MS
Minimum	27
Maximum	29
Average	27

Here per a ping testing which in figure (6) we got the results in the table (11) the result got by send and receive packets of TCMP from node to node from IPv4 to IPv6 ,and the size of the packets created by the own network, Depending on the traffic and the number of the nodes , here sent 101 packets and received 101 packets so there is no Packet loss, but for the latency can see from the table (12) the time of the mechanism the highest time is 29ms and the lowest time is 27ms then the average is 27ms.

3.2. Jperf Results

3.2.1.Latency Analysis of the transition mechanisms

This test is performed on the behavior of the TCP latency in the all scenarios, Host2 as client, and Host1 as the server listening to the client and The client generates ICMP (TCP) traffic using the Jperf tool.

As can be seen from figure (10). the latency can be appear on using the packet size (500) Bytes the time of transfer can be achieved in (200) msec in Translation Mechanism (NAT-PT), in dual stack can be seen that the time on the packet size (500) Bytes can be achieved (210) msec ,then the tunneling mechanism the time can be in (220) msec with same packet size bytes.

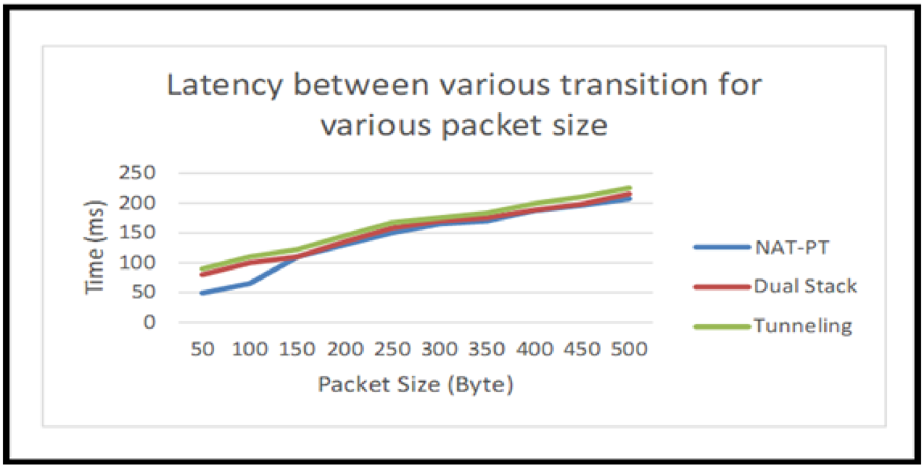

Figure 10. Latency Analysis of the transition mechanisms

3.2.2.Analysis of the Throughput

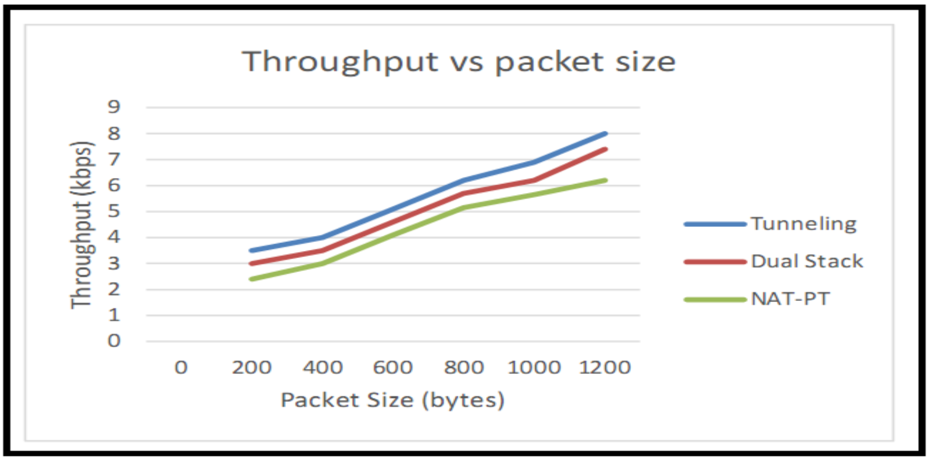

Figure 11. Analysis of the Throughput

This test are performed on the behavior of the TCP Throughput vs Packet size in the all scenarios, Host2 as client, and Host1 ICMP (TCP) traffic using the Jperf tool. As can be seen from figure (11). that on the packet size (1200) Bytes throughput can be achieved in Kbytes just under (7.2) Kbytes/sec in Translation Mechanism (NAT-PT) , in dual stack can be seen that the throughput increase is on packet size (1200) Bytes can be achieved (7.2) Kbytes/sec ,then the tunneling mechanism the throughput also seems to increase that can be seen on the same packet size (1200) Bytes throughput can be achieved in (6.1)Kbytes/sec.

3.2.3.Analysis of the Packet loss

This test are performed on the behavior of the TCP Packet loss in the all scenarios, Host2 as client, and Host1 as the server listening to the client and The client generates ICMP (TCP) traffic using the Jperf tool.

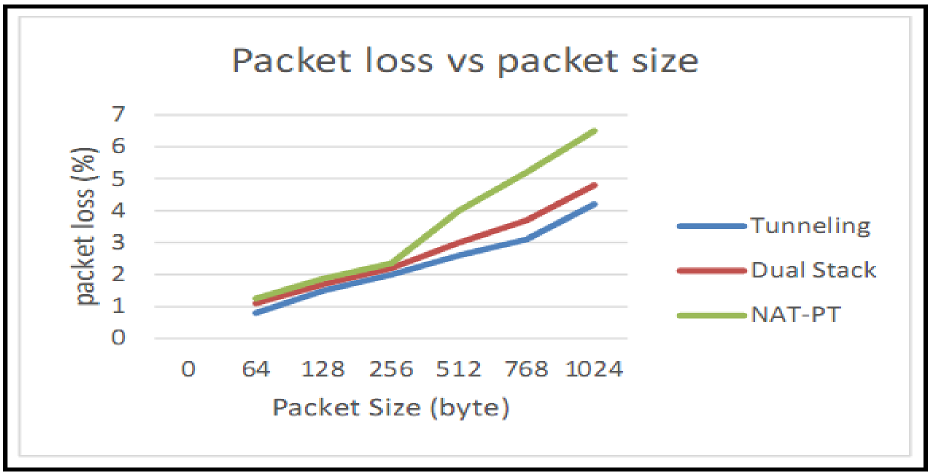

Figure 12. Analysis of the Packet loss

As can be seen from figure (12). that on an average of the packet size (1024) Bytes the Packet loss can be in percentage (4.2%) in the tunneling mechanism , in dual stack can be seen that the Packet loss increase is on the average of packet size (1024) Bytes can be achieved (4.9%) ,then the Translation Mechanism (NAT-PT) the Packet loss seems to be a high increase that can be (6.5%) with same packet size.

The reason to be the Translation NAT-PT mechanism expertise highest proportion of Packet loss because of it is time overwhelming limit . On the obverse part the tunneling got all-time low Packet loss expertise.

From this Results, the throughput, latency and the Packet loss analyzing have done. After implementation the previous designs of the IPv6-IPv4 mechanisms performance , some packets have been transmitted from HOST-1 to HOST-2. In this test and analysis, ICMP packets (TCP) have been transmitted with diverse duration time and sizes. After monitoring the packet transitions, the results below has been found:

As seen in the Figures (10),(11), it found that the Translation NAT-PT provides the elevated latency, while the Dual stack performance mechanism provides the moderate mode ,and about the Tunneling mechanism easy to see that it is provides the lowest latency and the Translation NAT-PT mechanism provides the highest latency , the tunneling has the highest throughput , and from the figure (12) it's found the Translation NAT-PT mechanism had the highest Packet loss and the Tunneling Mechanism had the lowest Packet loss.

.

Table 13.Comparative analysis of three transition mechanisms.

Features	Dual Stack	Tunneling	NAT-PT
Latency	Moderate	less	The Highest
Throughput	Moderate	The Highest	Lowest
Packet Loss	Higher than tunneling	less	The Highest

4. Conclusion

Based on the discussion above, the conclusions can be drawn as follows:

a. The dual stack progress instrument is the most well-known and simplest path for IPv6 and IPv4 hubs to speak with IPv6 and IPv4 hubs freely without evolving systems.

b. The dual stack is appropriate for Internet specialist organizations, corporate systems, and home clients.
c. Manual tunnel are appropriate for ISPs, corporate systems and server farms, yet not for home clients.
d. The progress system reacts to the issue of Internet development later on, however the decision of change components relies upon the foundation, security issues, spending plans, focal points and disservices of the instruments for an association.
e. The progress system NAT-PT change instrument encounters most noteworthy rates of bundle misfortune on account of its time overpowering confinement.
f. The progress system NAT-PT change gives the most elevated inertness, while Dual stack gives the moderate and the Tunneling component gives the least dormancy.
g. For the Recommendations, the Tunneling instrument technique has some of security issues that can will be understood by IP security (IPSec). that is the reason I prescribe to utilize tunneling mechanism mode with IP security (IPSec) for the most secure progress reason.

References

[1] R. Hinden, “Internet protocol, version 6 (IPv6) specification,” RFC 8200, 2017

[2] K. EL KHADIRI, O. LABOUIDYA, N. ELKAMOUN, and R. HILAL, “Etude comparative des mécanismes de transition de l’IPv4 à l’IPv6,” Mediterranean Telecommunications Journal, vol. 7, no. 1, Jan. 2017.

[3] Arafat, M., Ahmed, F. and Sobhan, M. On the Migration of a Large Scale Network from IPv4 to IPv6 Environment, International Journal of Computer Networks & Communications (IJCNC). 2014; 6(2): 111-126.

[4] M. A. Hossain, D. Podder, S. Jahan, and M. Hussain, “Performance Analysis of Three Transition Mechanisms between IPv6 Network and IPv4 Network: Dual Stack, Tunneling and Translation,” Int. J. Comput. IJC, vol. 20, no. 1, pp. 217–228, 2016.

[5] Ahmad, N. and Yaacob, A. IPSec over Heterogeneous IPv4 and IPv6Networks: Issues and Implementation, International Journal of Computer Networks & Communications (IJCNC). 2012; 4(5): 57-72.

[6] A. Salam and M. A. Khan, “Performance Analysis of VoIP over IPV4, IPv6 and 6-to-4 Tunneling Networks,” networks, vol. 14, no. 6, 2016.