IPv4/IPv6 Transition

Prof .Dr. Muzhir Shaban Al- Ani [1] & Rola A.A.Haddad [2]
Anbar University – Iraq Amman Arab University – Jordan
Muzhir_Shaban@yahoo.com, Rola2r@yahoo.com

Abstract

The new Internet Protocol (IPv6) has been developed to replace the current Internet Protocol (IPv4) and the transition from IPv4 to IPv6 is a necessary process in the realization of global Internet. The development of IPv6 technology and continuous increases in application, but this process will take long time so a transition methods will be needed. There are many IPv4/IPv6 transition methods already exist today, some of them applied in practice, the others still as proposed solutions. Tunneling and encapsulation methods are the most techniques that used until now, but all encapsulation mechanisms suffer from the increasing of the overhead traffic network as a result for either encapsulating IPv4 packet in the IPv6 packet or encapsulating IPv6 packet in the IPv4 packet. In this paper we proposed a system that make incompatible nodes; the first based IP4 the other based IPv6, communicate together without increasing packets size, this system is called Bi-Directional Transition System (BDTS). This system depends on understanding of the two environment of transmission , that is , received the source packet then converting the information header to be adaptable to the destination end. Our system has been implemented then we made a test by simulation tool called VMware ,during this simulation our system was studied in one scenario and the results shown that BDTS make two incomputable protocol hosts communicate together.

Keywords: IPv4,IPv6, IPV4/IPv6 transition, Dual Stack, Tunneling.

1. Introduction

The Internet Protocol (IP) was originally designed to facilitate connection of various organizations involved in the defense department's Advanced Research Project Agency (ARPA). Vinton G .Cerf and Robert E. Kahn in1974 presented IP as a protocol that supports the sharing of resources that exist in different packet switching networks. Now, the Internet Assigned Numbers Authority (IANA) administers the IP address space allocations on a universal basis. It also allows five Regional Internet Registries (RIR) to allocate IP addresses to local branches of internet registries or internet service providers [8]. The Internet Protocol is very simple in its functionality. It is only designed to handle the addressing and fragmentation of data-grams. Any additional functionality such as acknowledgement of received packets and retransmission of corrupted packets is passed off to the higher-level layers such as TCP [12]. An Internet Protocol address or IP address is a numerical label tagged to devices that take part in a local or wide area computer network that actively uses IP for communicating data and information. An IP address is a 32-bit number and this system is the Internet Protocol Version 4 or the IPv4 and most networks still use this format today, no one expected that the number of internet users will increase in this way so when IPv4 was designed it takes that the maximum numbers of devices that will have IP is (2^{32}). That means an IP address can provide a maximum (4,294,967,296) possible address , but in 1992 , the Internet Engineering Task Force (IETF) realized that current IP address space was running out as a result of rapid growth of Internet size and applications, so the need for a new protocol that has larger address space and improvement features was needed, because of that a solution for this problem was solved by IPv6 (internet protocol version 6) which offers a huge address space which will be more than enough ,but unfortunately IPv4 and IPv6 are incompatibles protocols and it is impossible to migrate from IPv4 to IPv6 in one day[10].Many transition mechanisms from IPv4 to IPv6 and vice versa had been proposed, some researchers divided these methods according to the techniques used in the transition to three transition methods : Dual-Stack method , Tunneling method and translation method as shown in figure 1[6] [2][13].

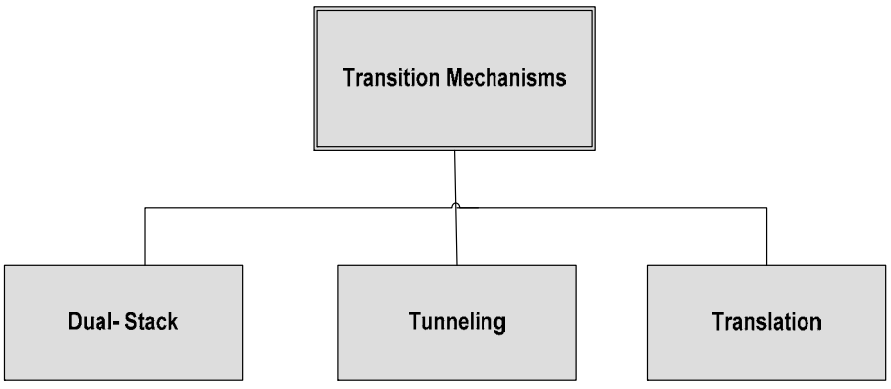

Figure 1 : IPv6/IPv4 transition mechanisms

In the dual –stack mechanism ; specified in IETF (RFC 2893) [14], a network node includes both IPv4 and IPv6 protocol stacks in parallel . Technical work mechanism of dual stack approach can be simply described as: parsing the received link layer packet data segment , open and check the header , if the first field that is the version number of IP packet is 4, the packet will handled by IPv4 protocol stack processing. But if the version number in the first field of the header is 6 , then it handled by IPv6 protocol stack processing. Dual stack mechanisms as explained include two protocol stacks that operate in parallel and allow network nodes to communicate either via IPv4 or IPv6 . they can be implemented in both end system and network node ,that means the network hardware runs IPv4 and IPv6 simultaneously. Usually, the IPv4/IPv6 dual-stack model is used for transition , but this approach requires that in order to use IPv6, hosts and infrastructure should be upgraded to dual-stack . the requirement cannot be met by old devices that don't support IPv6, and the upgrade of such device would induce a huge cost on the transition scheme, also it will increase the network complexity. On other hand there is a shortcoming , which is the most important reason for ISPs , is that for many users who have dual-stack by default , such as Win7 users , will get IPv4 and IPv6 name resolves at the DNS inquiry. Since IPv6 is prior to IPv4, IPv6 address is used to access the website first . for the reason that users do not have an IPv6 network environment , the result are often "Not Found" after a long time waiting for IPv6 time out. Obviously , this is not acceptable for ISP. Other shortcoming for dual stack approach is that servers can be visited from IPv4 and IPv6 , this result in firewall rules must be implemented both of IPv4 and IPv6 at the same time .if there is any change of a security policy , both IPv4 and IPv6 firewall rules must be re-considered carefully consistency, it is a hard work for security engineers in reality [7][9][6].

Encapsulation approach enables the connectivity between IPv6 islands by tunneling one protocol over another .In other words, Tunneling mean encapsulating IPv6 packets within the IPv4 packets and passing them through the native IPv4 domains. the tunnels are widely used in nowadays networks , this mechanism can transport IPv6 packets through IPv4 networks .Tunneling technology only requires both ends of the tunnel equipment to support both protocols , and each tunnel should be established between two endpoints manually or automatically. This mechanism will be used when two hosts that are using ipv6 want to communicate with each other and they intend to pass their packets through IPv4 zone ,so IPv6 packet will be as a data in IPv4 packet[1][3].

The advantages of this method that it enables the island IPv6 end systems and routers to communicate through an existing IPv4 infrastructure , and the IPv6 packets will be putted and transported over IPv4 network without being modified. But this method suffers from the increasing of the overhead traffic network , and the shortcoming is in its failure to direct communication between IPv4 and IPv6 nodes[5].

A translation method called NAT-PT was proposed ,it is a technique that allows the communication between only IPv6 and only IPv4 systems ,and it consists in translating the headers of the packets ,but only the common fields of IPv6 and IPv4 ,and for this reason NAT-PT is not so popular within the internet[1].

2. Internet Protocol Addresses (IP Addresses)

Every device connected to the public Internet is assigned a unique number known as an Internet Protocol (IP) address. The designers of the Internet Protocol defined an IP address as a 32-bit number and this system , known as Internet Protocol Version 4(IPv4),is still use today. Anew versions of IPs had been proposed ,some of these versions will discussed in this section .ICANN or Internet Community with Address Management and Governance tries to manage the address space in Internet and also they have designed different version of IP addresses after IPv4 . This list has IPv7 - (just an expansion of ipv4) IPV8 , IPv9 and none of them are operational now , this means they are in draft state[8] .

2.1 **IPv4**

An IPv4 address can provide a maximum of 4294967296 (2^{32}) possible address spaces out of which 18 million private network addresses and 270 million multi-cast addresses are reserved. A typical IP address comprises of dot-decimal notation. This notation has four decimal numbers, each one of which ranges from zero to 255, each separated apart by a dot (for example, 192.168.1.1) [8].

2.2 **IPv6**

In 1992, the Internet Engineering Task Force (IETF) realized the current IP address space was running out. To make address more readable, IPv6 specifies hexadecimal colon notation. In notation 128 bits are divided into eight sections, each 2 bytes in length. Two bytes in hexadecimal notation require four hexadecimal digits. Therefore address consists of 32 hexadecimal digits with every four digits separated by a colon. Although the IP address, even in hexadecimal format, is very long, many of the digits are zeros. In this we can abbreviate the address. The leading zeros of a section can be omitted .Only the leading zeros can be dropped, not the trailing zeros [4][8].

3. The Proposed Transition Process

In this paper a Bi-Directional Transition Mechanism (BDTS) will proposed , which is concentrated on translating and forwarding packets between the different network environments - IPv4 and IPv6 environments- .The proposed system deals with the deep understanding and analyzing the headers of both technologies IPv4 and IPv6 and the methods for managing the transformation between these technologies .There is many differences between the header structures for both protocols ,several fields has been removed as shown in figure 2[13].

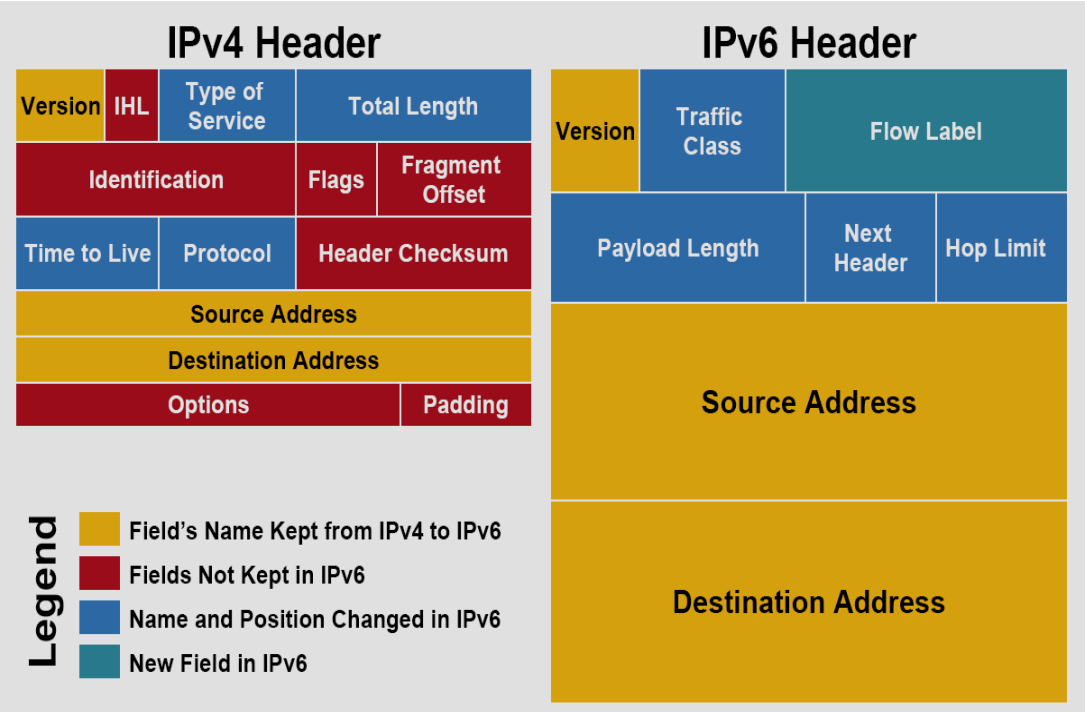

Figure 2: Comparison of IPv4 and IPv6 headers' structures [15]

As shown in figure 2, IPv6 header format is greatly simplified in comparison to the IPv4 format, this is due to the removal of several fields, these fields are: header length field, Identification field, Flags field, Fragment offset field, Header checksum field, Options field and Padding field.

Some fields are common to both protocols , these fields are:

- version field , in the case of IPv4 the " version" field will be equal to (4). while in the case of IPv6 the "version" field will be equal to (6).this field is important for routing since IPv6 message must be handled differently than IPv4 message.
- Source address field. It is expanded in IPv6 to be (128) bits ,while it is (32) bits in IPv4 . This change in size is due to the changes in addressing in IPv6.
- Destination address field. It is also expanded in IPv6 to be (128) bits, while it is (32) bits in IPv6.

Some fields have changes in name ,but they are the same function for both protocols, these fields are:

- Type of Service (IPv4) and Traffic class (IPv6) .
- Time to Live (IPv4) and Hop Limit (IPv6).
- Protocol (IPv4) and Next Header (IPv6).
- Total Length (IPv4) and payload (IPv6).

Flow label field is new in (IPv6) , if it is equal to zero then Traffic Class (IPv6) equal to Type of Service (IPv4) and if not then use different level of type of service. Extension headers (IPv6) , new way in IPv6 to handle option fields ,fragmentation , security , Some of the missing fields (e.g. fragmentation information) have been pushed into an extension packet header. These exist only in fragmented packets. Unfragmented packets do not have to carry the unnecessary overhead[8].

The proposed system depends on capturing the header , identifying the header, transformation the datagram to the destination environment and then transmitting the datagram to the destination address . this system deals with the bi-directional operation that leads to converting the received datagram to the destination environment.

3.1 Transition from IPv4 Header to IPv6 Header

The header processing proposed algorithm deals with the in-depth understanding of the two structures of the header fields .The process of transition from IPv4 to IPv6 are listed below:

Process 1: version transformation, inserting (0110) in the version field of IPv6 to denote that the IP version is 6.
Process 2 : computing payload length , it will be computed by subtracting the contents of the "header length " field of IPv4 header from the contents of the "total length " field of IPv4 , then , the resulted value will be saved in the "payload length" field in IPv6 [5].
Process 3 : inserting Flow Label field, this will done by copping the content of Identification Field of IPv4 in Flow Label field of IPv6.
Process 4 : filling the Traffic Class field of IPv6, by mapping the content of the TOS field of IPv4 to the TC field of IPv6 as shown in figure 3 [1]

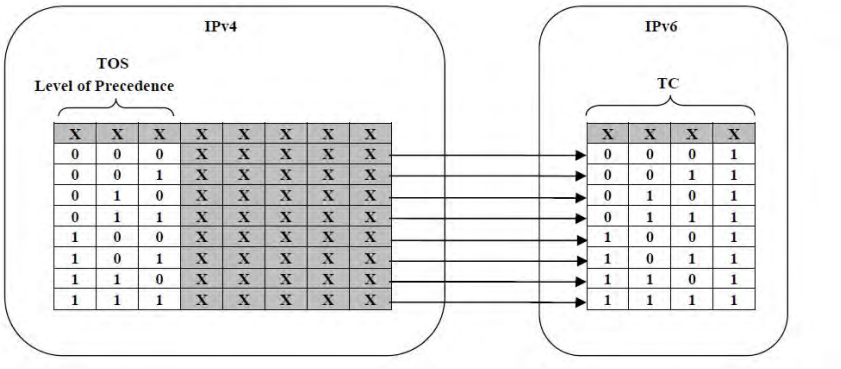

Figure 3 : Mapping the contents of the TOS to TC

Process 5 : checking the Fragment Offset field of IPv4 .However , if the Fragment Offset field is not equal zero then process 6 will done before process 7 and 8 .Else process 7 and 8 will done without doing process 6.
Process 6: coping the contents of the "Flag" and " Fragment Offset " fields of IPv4 header to the corresponding Fields in the " Fragment Extension Header " of IPv6.
Process 7 : copping the contents of "Time To Live" field of IPv4 header to the "Hop Limit " field of IPv6.
Process 8 : convert the" IPv4 Destination Address and Source Address" to "IPv6 Destination Address and Source Address " then save the result in IPv6 Destination Address and Source Address fields.

3.2 Transition from IPv6 Header to IPv4 Header

The main process of transition from IPv6 to IPv4 are listed below, some fields of the IPv4 header will contain the same values from the corresponding fields of the IPv6 header .

Process 1: version transformation, inserting (0100) in the version field of IPv4 to denote that the IP version is 4.
Process 2 : mapping the content of TC field in IPv6 header to the TOS field in IPv4 header as explained in figure 4 [1].

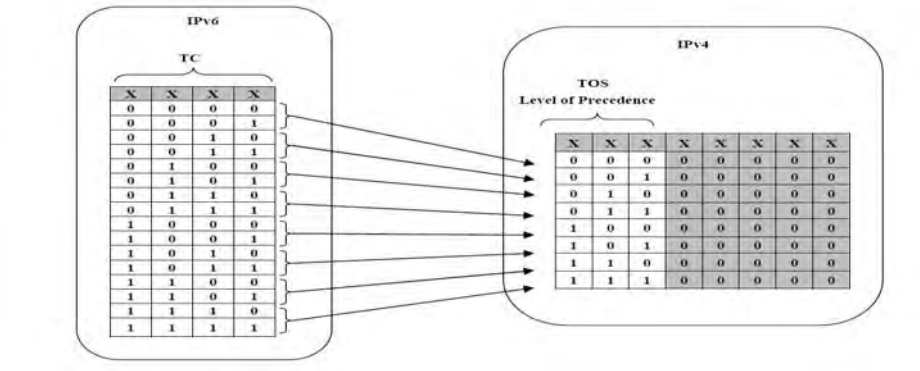

Figure 4: Mapping the contents of the TC to TOS

Process 3 : copping the content of Next Header field of IPv6 to the Protocol field in IPv4.
Process 4 : copping the contents of Hop Limit field in IPv6 header to the Time To Live field in IPv4 .
Process 5 : compute the header length and save the result in THL field in IPv4 header.
Process 6 : compute the Total Length for IPv4 header by adding the value of Payload Length of IPv6 header to the result that computing in process 5. Then save the result in Total Length field for IPv4.
Process 7 : convert the" IPv6 Destination Address and Source Address" to "IPv4 Destination Address and Source Address " then save the result in IPv4 Destination Address and Source Address fields.

4. Results and Simulation

As mentioned before our proposed system deals with the deep understanding and analyzing of the headers for both technologies IPv4 and IPv6 , our solution is a bi-directional translation system between IPv4 and IPv6 .In this section , a description of the architecture of the simulation environment will proposed. The scenario given in figure 5 depicts a conversation between two hosts , IPv4 host and IPv6 host.

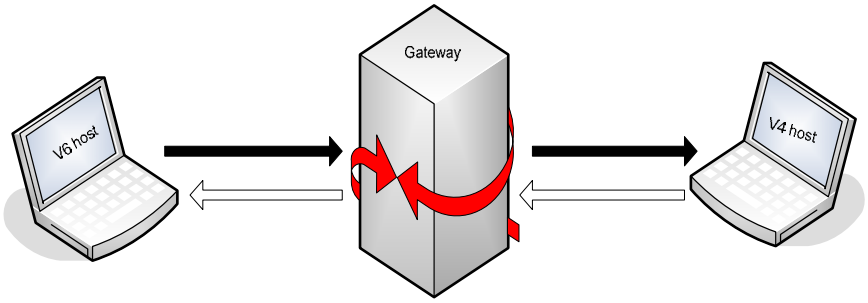

Figure 5: Simulation Scenario

As shown in figure 5, our virtual network contains three parts : two hosts and gateway machine .To test our system we used VMware software as a tools to perform the simulation experiments. We determined the operating system of the hosts as windows7, and the operating system of the gateway as Linux 2.6.x kernel. The test that has been done by order as below:

Step1: download VMware program.
Step2: identify (host 1) as IPv4 machine.
Step3 : identify (host2) as IPv6 machine by determining the IP address for the device in version 6.
Step4: download (BDTS) system in (host1) and (host2) as shown in figure 6.

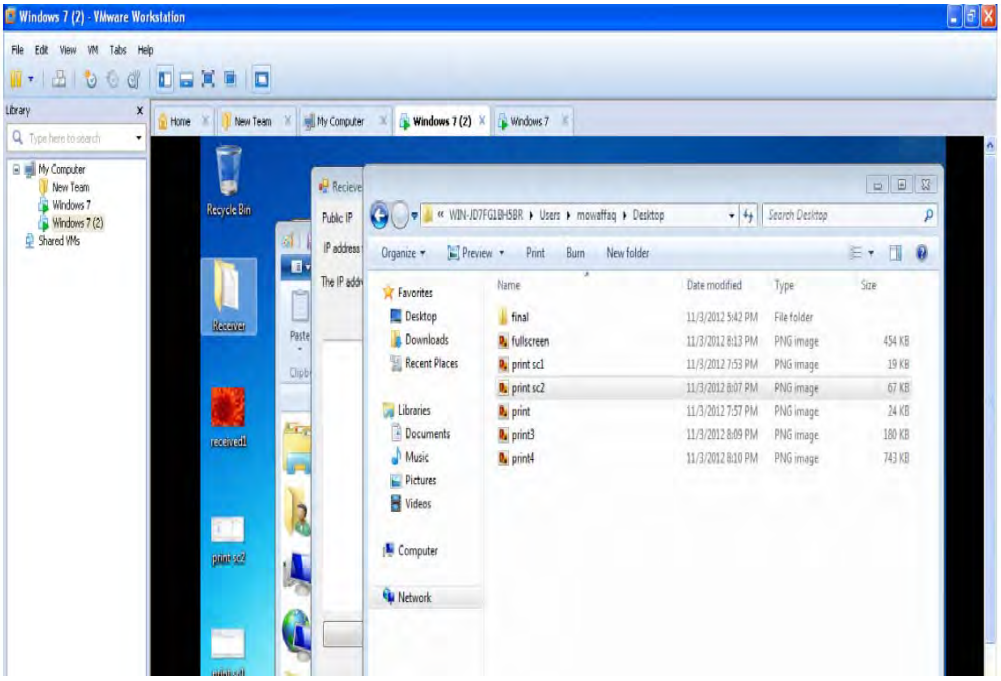

Figure 6: Full outside screen for VMware Workstation

Step5: run (BDTS) in (host1)- Main Screen will appeared- as shown in figure 7. The Main Screen contains the buttons to start Sender or Receiver applications, and Exit buttons to come out of the program.

Figure 7 : Main Screen of (BDTS)

Step6: select (sender) command from the Main Screen.
Step7: insert the IP address of (host2) –receiver- in the (IP of the receiver) in sender interface.
Step8 : select the file that will be send from (browse) command as shown in figures 8 and 9 .

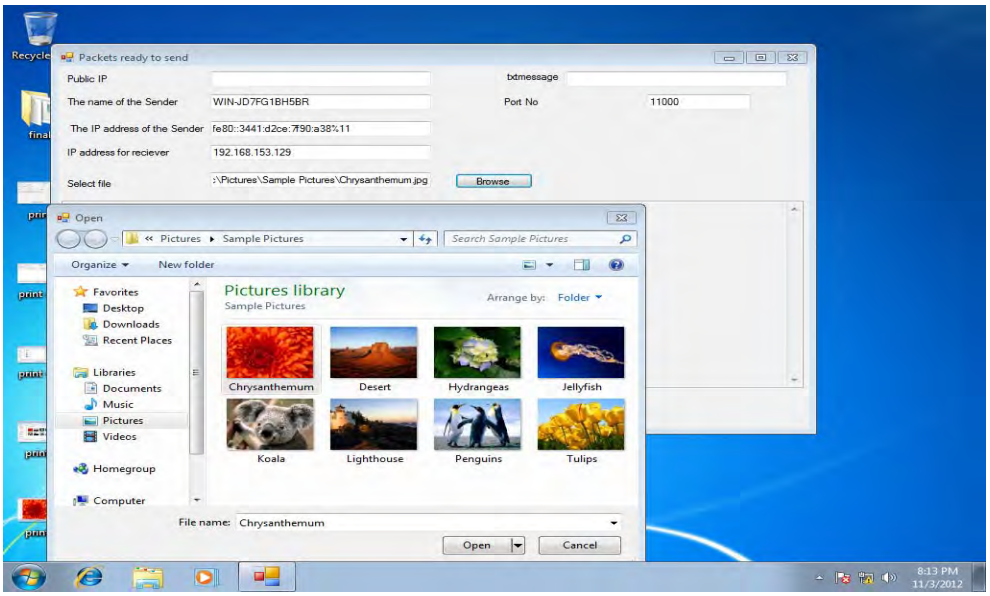

Figure 8 : Sending Operation

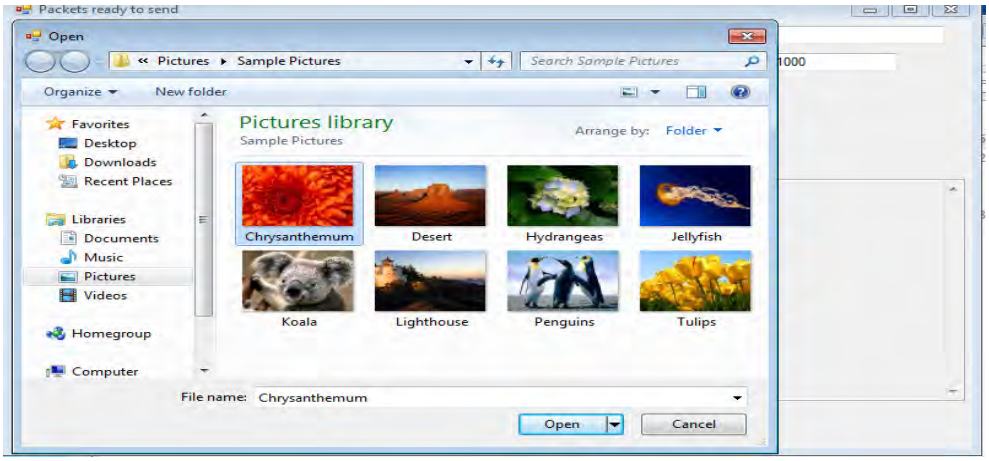

Figure 9 : Browsing for files

Step9:press (send) command from sender interface.
Step10: run (BDTS) in (host2).
Step11: select (receiver) command from the main menu.

Step 12: press (save) command from the receiver interface.
Step 13 : save the file in (host2) as shown in figures 10 and 11.

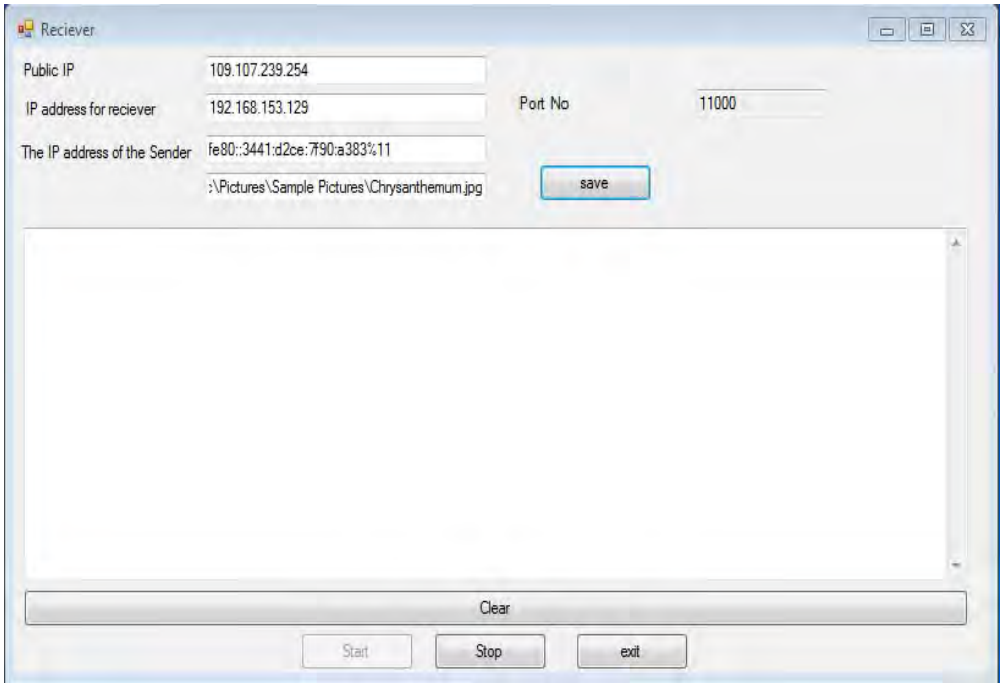

Figure 10 : Receiving Interface

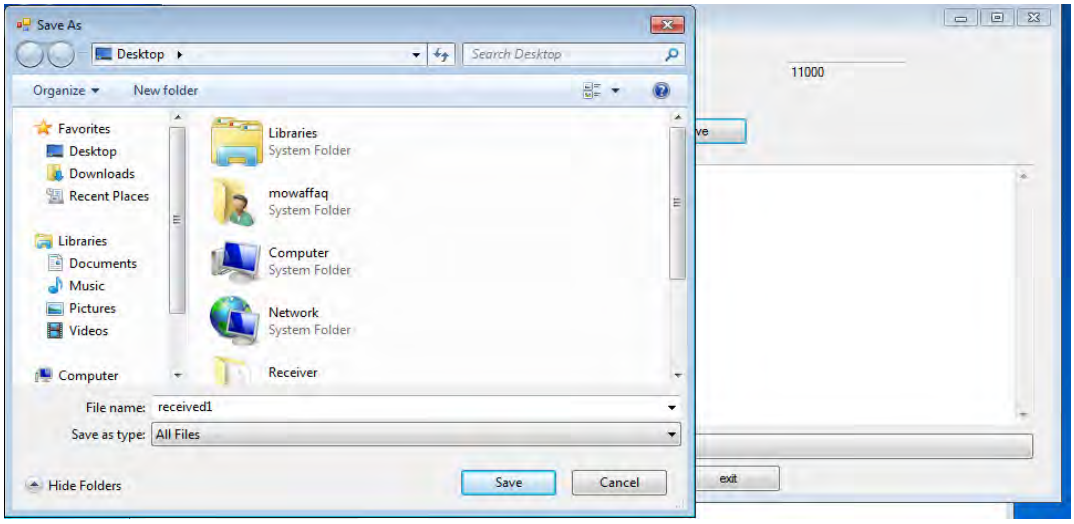

Figure 11 : Saving the received file

Step14: open the file to insure that it is the same file that has been send from (host1), then we could make a comparison between the properties of the files before sending them and their properties after receiving them to ensure that the receiving file is not corrupted.

5. Conclusions

It well understood that IPv6 has been designed to replace IPv4 . The migration over to IPv6 is a necessity in the long term, and because IPv4 and IPv6 are incompatible protocols , There are many IPv4/IPv6 transition methods already exist today, some of them applied in practice , the others still as proposed solutions .

Dual Stack and Tunneling are methods that applied in practice , but many challenges for the IPv6 migration have been mentioned in this paper , like changing or updating the infrastructure of the networks in using Dual Stack method or increasing the packet size that transmitted in using Tunneling method .

In this paper a transition mechanism has been proposed . The proposed algorithms deal with the method of transformation and adaptation between IPv4 and IPv6 that called Bi-Directional Transition System (BDTS) . This paper proposed algorithms that depend on understanding of the two environment of transmission , that is , received the source packet then converting the information header to be adaptable to the destination end in this

way no increasing in packet size will happened as in Tunneling method. The algorithms have been implemented and then a simulation test has been done by a network simulation tools called VMware.

6. Future Work

The work reported in this paper opens the way for continued research in a number of direction. A particularly interesting area for future research is implementing and evaluating the proposed mechanism in the real wireless Internet network.

References

[1] Al-Kasasbeh, Al-Qutaish,Muhairat, " Innovation Algorithms for the Header Processing Transition from IPv4 to IPv6 and Vice Versa", The International Arab Journal of Information Technology , Vol.7 , No 3 , July 2010.

[2] Muzhir Al-Ani , Basil Kasasbeh, "Efficient Header Processing Transition between IPv4 and IPv4 " ,International Journal of Science Engineering and Technology ,Vol.1 ,No.2 , 2008.

[3] J.Hanumanthappa and Manjaiah D.H, "Astudy on Comparison and Contrast between IPv6 and IPv4 Feature sets",International Conference on Computer Network and Security (ICCNS), 2008.

[4] Xianhuiche, Dylan Lewise, "IPv6 :Current Deployment and Migiration statuse", International Journal of Research and Reviews in Computer Science (IJRRCS), Vol.1,No.2, June 2010.

[5] Yuan-yuan LU, "Transition from IPV4 to IPV6 Network Application", International Conference on Intelligence Science and Information Engineering, 2011.

[6] Kuobin Dai, "IPv4 to IPv6 Transition Research Based on the Campus Network", International Symposium on Intelligence Information Processing and Trusted Computing, 2011.

[7] Li Zimu, Peng Wei, Liu Yujun, "An Innovative Ipv4-ipv6 Transition Way for Internet Service Provider", IEEE Symposium on Robotics and Applications(ISRA), 2012.

[8] Lawrence E. Hughes,"The Second Internet", Infoweapons , 2010.

[9] Yu Zhai,Congxiao Bao,Xing Li," Transition from IPv4 to IPv6 : A Translation Approach", Sixth IEEE International Conference on Networking ,Architecture ,and Storage ,2011.

[10] Norshakinah Bin Timd Nasir, "Performance Evaluation of IPsec Implementation in IPv4 and IPv6 Networks", University Utara Malaysia,July 2007.

[11] Khaldoun batiha, Khaled Batiha, Amer Abu Ali," The need for IPv6", International Journal of Academic Research, Vol.3. No.3.May 2011.

[12] RFC 791 ,"Internet Protocol DARPA Internet Program Protocol Specification" ,www.tools.ietf .org, 1981.

[13] Ra'ed AlJa'afreh , John Mellor , Mumtaz Kamala , Basil Kassasbeh, Muzhir Al-Ani , "A novel IPv4/IPv6 Transition Mechanism which Supports Transparent Connections" , ISBN: 1-9025-6016-7© 2007 PGNet.

[14] RFC 2893," Transition Mechanisms for IPv6 Hosts and Routers" , August 2000.

[15] http://www.pixmule.com/ipv6 acceded [11 November 2011]