Journal of Theoretical and Applied Information Technology
10th February 2013. Vol. 48 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A NEW KIND OF IPV6 TUNNEL DESIGN TO SUPPORT NAT

[1]JUNYUN WU, [2]CAIYUN XIE
Lecturer, School of Information Engineering, Nanchang University. Nanchang. China
Assistant, Department of Information Science, Nanchang Teachers College. Nanchang. China
E-mail: [1]wujunyun@ncu.edu.cn , [2]xiecaiyun2005@163.com

ABSTRACT

In the process of building IPv6 transition network, there are three commonly used methods of transition: double-stack technology, tunnel technology and address translation. But none of them can traverse NAT. Considered this condition, this paper advances a new solution based on Client / Server technology for traversing NAT. It summarizes the technological challenges and analyzes possible scenarios during the transition from IPv4 to IPv6, and proposes a new protocol based on tunnel technology. This new technology needs less equipment and can greatly facilitate users. The result of the experiment shows it obtains better effect.

Keywords: *IPv4, IPv6, Tunnel, NAT Traversal*

1. INTRODUCTION

Recently, there are some IPv6 tunnels applied in the IPv6 transition strategy, but they almost can't go through the NAT. Teredo technology is relatively mature for NAT tunneling protocol designed for users, but it also has some disadvantages: users can not assign a fixed IPv6 address, the type of NAT does not support symmetry, and it can not help users to prevent unauthorized access getting into the IPv6 network. It introduced the whole tunnel system, repeaters, servers and other equipment, so that it increased the costs of transition to IPv6 equipment and technology. This paper presents a way how to implement IPv6 based on the NAT. This tunnel technology only uses one tunnel server, without any other equipment. You can assign an IPv6 address for client and establish long-side connection between IPv6 server and clients through this new tunnel. Using this method we only require a tunnel server with IPv6 and IPv4 protocol stacks of network routing / relaying device, then other tasks related to the tunneling protocol will be completed by software[1-2].

2. SCENE DESCRIPTION AND ANALYSIS

A Scene Description

In order to understand easily, it gives a brief description of the scene which we need to realize and a prerequisite for achieving. In the process of transition from IPv4 to IPv6, it is a typical scenario in the next generation of Internet. In this scene, IPv4 and IPv6 networks exist simultaneously. If there are two different networks: C (Campus) and the network H (Home), and net H only supports IPv4 currently, net C can support IPv6. Internet between network H and network C includes a number of IPv4 networks. From the hardware point of view, the two networks are isolated by a number of intermediate routers. At the same time, there is NAT equipment in net H, so workstation HW1 in net H can visit Internet. The workstation CW1 in network C also needs to access the Internet across NAT device. The basic structure of the scene is shown in Figure 1.

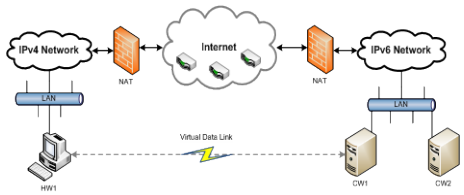

Figure 1. Description The Environment

From the Figure 1, we can see that under the present IPv4 network environment, it is difficult for HW1 to visit CW1. If using the collocation method to solving this problem, we need to bind the port of the router of the CW1 IPv4 address and the corresponding port. But in this way, HW1 only can visit CW1 indirectly. How can we realize under this scene:

Journal of Theoretical and Applied Information Technology
10th February 2013. Vol. 48 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

1、Assign a IPv6 address for HW1, enable HW1 to become a part of IPv6 network.

2、The mutual visit which HW1 "turning on" to network C, cause HW1 to send out IPv6 package and CW1 can access.

3、Establish the stable long connection between HW1 and CW1, then form the virtual data link used for the stable data stream transmission.

B Scene Analysis

Our goal is to establish a tunnel server as well as visiting this tunnel service based on the specific protocol of the client program, when we lay this tunnel server at some specific positions, the machine between net H and net C can use the IPv6 protocol to correspond mutually. Position deposited according to the tunnel server is different as well as whether the net C machine uses the server. Usually, there are the following two kinds of location state.

● Scene one: The tunnel server is laid at some positions in Internet. In this kind of situation, machines in net H and net C need to install the client program, and register the tunnel server. And the tunnel server is placed in both sides of NAT. Therefore, the tunnel server needs to process IPv4 packages of penetration which come from the net H and net C, but the way of processing is basically consistent. At this time the tunnel server is not only a part of IPv6 network, but has the ability of processing the double protocol stack of IPv6 and IPv4, and needs to deploy alone the tunnel server in Internet and assigns an independent IPv4 address for it. As is shown in Figure 2.

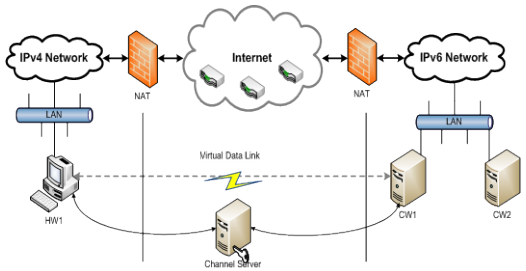

Figure 2.Tunnel Server Deployed In Internet

● Scene two: We can also choose to lay the tunnel server in the net C, it becomes an equipment in the IPv6 network environment. Therefore tunnel server has IPv6 and IPv4 protocol stack, it can visit any IPv6 equipment in the net C. But in order to make the tunnel server to provide the access tunnel service, we need to place the tunnel server in NAT, so its monitored IP and the port are exposed in Internet. In addition, tunnel monitor is still established in the IPv4 protocol. Therefore we need the NAT equipment in net C simultaneously, and this equipment can support the double stack of IPv4 and IPv6. As is shown in Figure 3.

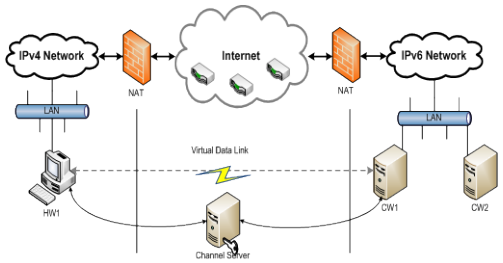

Figure 3 .Tunnel Server Deployed In The Ipv6 Net

C NAT Independency of Scene Two

Under the client /server pattern, client and server establish tunnel. Client sends IPv6 data which has been packaged as IPv6-in-UDP to the goal node by the server breaking and retransmits. In order to make the goal node return the package, IPv6-in-UDP must be sealed to return to the client unties by the same package breaking module when it obtains the IPv6 data packet. During this process, the tunnel server and the goal node (CW1) donot have NAT. Between tunnel server and client, the NAT mapping (exterior address + exterior port) is always fixed, the tunnel server can use this NAT mapping data packet normally and send out to client[3-4]. Therefore, between the client and server, correspondence has nothing to do with NAT.

Because scene two uses the client/server pattern tunnel, tunnel's establishment has nothing to do with the NAT type. Therefore there may be willfully the multi-NAT equipment between HW1 and the tunnel server. Simultaneously this method causes to simplify through the part collocation method on the tunnel server's work load, for the full implementation of ipv6 network, this tunnel server depositing needn't take the independent IPv4 address in the interior network. Its opposite of Internet is deployed an equipment, which is simple, convenient and has the low cost tunnel. Therefore we take the scene two as the key point to realize.

3. TUNNEL SERVER PROTOCOL

A Overview of the Basic Protocol

By the last section of the scene description, we can simply divide the process of building and completing the IPv6 communication channel into four parts [5-8]:

1. The login authentication. At first client must dispose IPv4 address on the tunnel server, and then

Journal of Theoretical and Applied Information Technology
10th February 2013. Vol. 48 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

send out the UDP message of requesting login authentication through the tunnel server. The UDP message carries the user's name and password of client. The tunnel server will return a confirmation package which includes an encryption public key generated by the server after verifying. The client will use this public key in the next process of encryption communication, which can effectively prevent the middle attacking. As is shown in Figure 4.

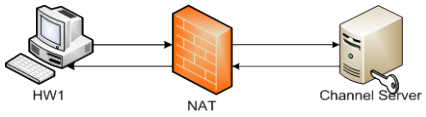

Figure 4 .Login Authentication Graph

2. The address assignment. The client transmits the IPv6 address requesting message to the tunnel server, the tunnel server obtains client's tunnel parameter from this message, then returns the IPv6 response address message to the client. There are some kinds of strategy of assigning the IPv6 address: sending a request IPv6 address to the DHCP server of the IPv6 network; generating the IPv6 address according to the network rule; assigning IPv6 address of related client by the network administrators, and so on. As is shown in Figure 5.

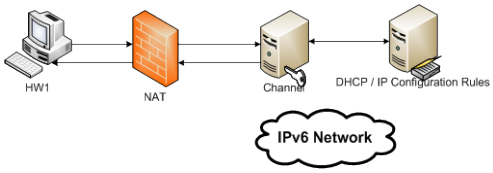

Figure 5. Address Distribution Diagram

3. The tunnel establishment. The client disposes its own IPv6 address according to the content of the message, then sends the message for requesting establishing tunnel to the tunnel server, in the message including the goal IPv6 address. The tunnel server sends a PING message to IPv6 goal address after receiving the request. When goal address returns the response, the tunnel mapping will be established in the end of the tunnel server, so that the client will be accessed. At this time, the client can send IPv6 message carrying actual service date to the goal server. As is shown in Figure 6.

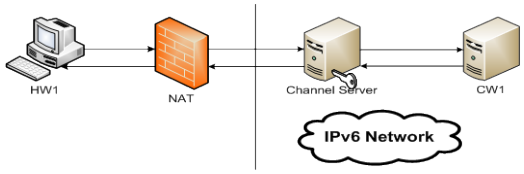

Figure 6 .Tunnel Establishment Chart

4. The tunnel maintenance. After tunnel establishment, because NAT will delete the mapping of UDP data packet which is outdate, to maintain tunnel's existence, the client needs to send the BUBBLE message to the tunnel server periodically. The BUBBLE message is IPv6-IN-UDP message which doesn't have data loading. As is shown in Figure 7.

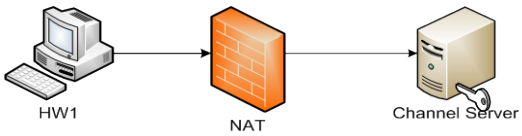

Figure 7. Tunnel Maintenance Chart

B Tunnel Management Protocol

A major function of the tunnel server is realizing the double package of the head of the IPv6 and the UDP in the IPv6 package of the client in the destination before they are transmitted. This process is realized through establishing the mapping relationship between the IPv6 address of client and the tunnel's parameters.

IPv6 address requesting message is a UDP package which has the content of an identifier for the client. The tunnel server will obtain its parameter of tunnel after that the client A receives this address requesting package. It also transforms after NAT source IPv4 address IPv4A and source UDP port number UDPA is a construct IPv6 according to the client side connection identifier address IPv6A, establishes IPv6A and between the IPv4A \ UDPA mapping relations. Therefore, the tunnel server needs to maintain one mapping table, in which we increase a user every time, it will increase one new table item, indicates that founds a new tunnel. After receiving the data message from the IPv6 connection, the tunnel server obtains the IPv4 address and the UDP port through querying the table, then it sends the package which is sealed and sealed again to the client.

The mapping table will grow larger gradually along with the increasing of the number of users; the tunnel server's expenses also increase. So we need to manage these tunnels. We can delete the tunnels which are no longer used, and then the tunnels on the server are all active. There are two

Journal of Theoretical and Applied Information Technology
10th February 2013. Vol. 48 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ways to manage: first, client procedure sends notice when exiting, then the tunnel server will delete this tunnel after receiving the notice; second, the client sends notice to the tunnel server periodically to prove its existence, otherwise this tunnel will be deleted if the server can't receive the notice with certain amount of time.

The IPv6-IN-UDP tunnel is established on the foundation of UDP conversation. To ensure the effectiveness of the tunnel, the NAT equipment will delete the UDP conversation which has no data stream in a long time. The client needs to transmit the BUBBLE data packet unceasingly to the tunnel server, the tunnel server happens to regard the package as the notice, therefore we will use the second tunnel mode. The tunnel server designs a timer for each user, after receiving the BUBLLE data packet, the timer will be reset. Once the timer is overtime, the mapping table which is related to this user will be deleted.

4. SYSTEMS REALIZATION

Usually, there are two kinds of realization of tunnel in the client: realizing in the system kernel space and the user space realizes. In the user space realization, the client and the application server are both an operating system's application, they are both realized by socket programming. If the realization is in the system essence space, it will be Independent in the upper formation application. The application procedure sends the IPv6 package to the goal address. Tunnel is in the bottom of the stack of IPv6 protocol. IPv6 packets take their own packets as the UDP packets, then use the IPv4 protocol stack interface and the tunnel server to communicate; On the contrary, the tunnel client procedure will split the IPv6 package out according to the protocol when receiving the IPv6-in-UDP package sent by tunnel server. Then the package will be transmitted to the upper application. Therefore, this approach does not require any modifications in the upper application, it is transparent for IPv6. We use this way to realize the function of the client tunnel. The IPv6-in-UDP packets sent by the client split out the IPv6 package, and then transmit to the target IPv6 network in the forwarding process. Therefore the most direct way is to make the tunnel server implemented as application based on a IPv4/IPv6 double-stack, and transmit the IPv6 package sent by the tunnel client by using IPv6 protocol in the IPv6 network. So in a sense point of view, the tunnel server is similar to a proxy IPv6 server[9-12]. As is shown in Figure 8.

5. PERFORMANCE TEST

Performance test is intended primarily for the tunnel server packet forwarding capability and concurrent processing. Tunnel server runs on the network center of our campus,Ipv4 address is 222.204.23.20, IPV6 prefix can be assigned to 2001:250:6 C00:: / 48, 4-core CPU clocked at 3.2G, memory for the 4G, Linux kernel version 2.6.30.5. By gradually increasing the number of address requesting packet, the forwarding efficiency test server, we can see from Figure 9 the efficiency of packet forwarding.

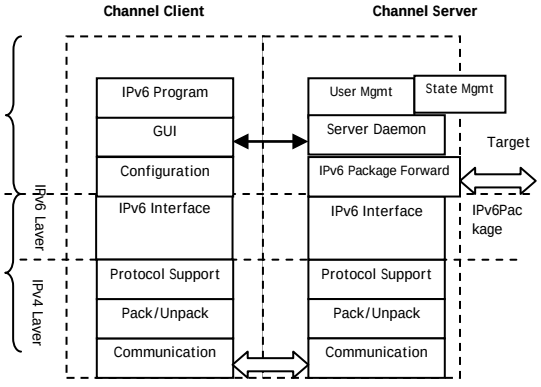

Figure 8 The Tunnel System Structure

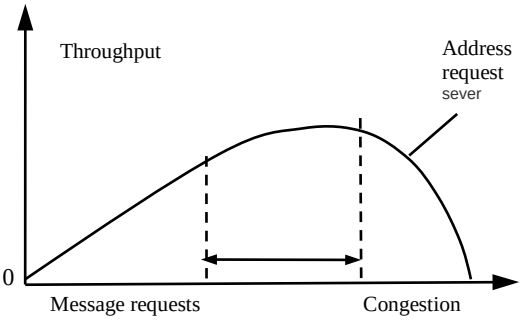

Figure 9 The Efficiency Of Packet Forwarding

It can be seen from Figure 9, at the beginning, the system forwarding the requesting packets is increasing in the number. But up to a certain data, the rate of forwarding will drop dramatically, and even causes the system collapsing. The reason is that the server's concurrent processing capabilities are limited. Therefore, this system needs gradual incensement in the number of users to upgrade and optimize the server.

6. CONCLUSION

The method is relatively simple in structure, using less equipment, and getting higher efficiency. In addition, the design also indicates that the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

existing tunnel proxy mechanism can not support NAT users. This current system has been tested in the laboratory of the network center, and will be put into practical application soon.

ACKNOWLEDGMENTS

The project is supported by the Foundation of Jiangxi Provincial Education Department (No. GJJ12048) and Jiangxi Provincial Department of Science Technology (No. 20122BBE500049).

REFRENCES:

[1] S.FLu ,W.Q.Hu. "Passing NAT of VPN by improving UDP based on Agent", *Compter Application*, vol24, No.10, 2004, pp.50-51.

[2] X.F.YZhang, F.Y.Xia. "A solution for symmetric NAT traversal in P-Teredo", *Application of Electronic Technique(China)*, No.2, 2007, PP.113-115, 2007.

[3] [DRAFT] C. Huitema. "Teredo: Tunneling IPv6 over UDP through NATs", *http://www.rfc-editor.org/rfc/rfc4380.txt*, February 6 ,2002.

[4] Z.Wang, Y.Guo, Y.Zhang. "NAT traversal solution based on host identity protocol", *Computer Engineering and Design(China)*, vol.29,No.10 , 2008,pp.2435-2438.

[5] G.Y.Zhang, Z.W.Ye and L.J.Qu. "Novel Solution of Using UDP to Traverse NAT". *Computer Engineering(China)*, vol.34, No.122008, pp.112- 114.

[6] Iflikli. Cebrail C, Gezer. Ali and Ozsahin. Abdullah Tuncay. "Packet traffic features of IPv6 and IPv4 protocol traffic". *Turkish Journal of Electrical Engineering and Computer Sciences*, Vol.20, No.5, 2012, p.727-749.

[7] X.G.Wu. "Research on the IPv6 Tunnel Technology Designed for Network Address Translator Users", *Institute of Computer Technology Chinese Academy of Sciences(China)* , 2006.

[8] Risdianto. Aris Cahyadi, Rumani. R. "IPv6 Tunnel Broker implementation and analysis for IPv6 and IPv4 interconnection", *Proceedings of 2011 6th International Conference on Telecommunication Systems, Services, and Applications*, TSSA 2011, pp.139-144.

[9] Narayanan. A. Sankara, Mohideen. M. Syed Khaja and Raja. M.Chithik. "IPv6 Tunneling Over IPv4". *International Journal of Computer Science Issues*, Vol.9, No.22-2, 2012, p.599-604.

[10] Y.J.Wu, X.Q.Zhou. "Research on the IPv6 performance analysis based on dual-protocol stack and tunnel transition". *ICCSE 2011-6th International Conference on Computer Science and Education, Final Program and Proceedings*, 2011, pp.1091-1093.

[11] X.G.Wu, M.Liu. "Design and Implementation of the IPv6 Tunnel Broker to Support NAT Users", *Computer Engineering. (China)*, Vol.32, No.23, 2006, pp.62-68.

[12] G.T.Si, F.F.Ren. "Design and Implementation of IPv4/IPv6 Campus Network". *Microcomputer Application(China)*, Vol.27, No.4, 2011, pp.37-39.