



EXPERT TRANSLATION BUREAU, LLC

Telephone: (312) 759-9999 Facsimile: (312) 283-1071

18001 North Bay Road, Suite 506, Sunny Isles, FL 33160

www.Expert-Translation.com

CERTIFICATE OF TRANSLATION

December 12, 2023

I, Xing Zhong, hereby certify that I am competent in both the English and the Chinese languages.

I further certify under penalty of perjury that translation of the aforementioned patent document:

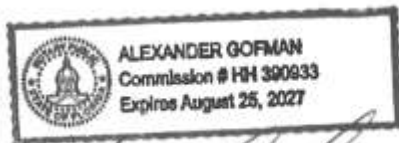
[CN 1525699 A_English.pdf]

from the Chinese language into the English language is accurate and correct to the best of my knowledge and proficiency.

Xing Zhong

Xing Zhong

Professional Translator



Alex Gofman
12.12.2023



[12] Patent Application Publication

[21] Application No.: 03158973. 1

[43] Publication Date: September 1st, 2004

[11] Patent NO.: CN 1525699A

[22] Application Date: September 17th, 2003

[21] Application No.: 03158973. 1

[71] Applicant: The Institute of Computing Technology of
the Chinese Academy of SciencesAddress: No.6, Kexueyuan South Road,
Zhongguancun, Haidian District, Beijing
100080[72] Inventor: WU Xianguo, LIU Min, ZHANG Tianle,
SHI Jinglin, LI Zhongcheng[74] Patent agency: China Science Patent &
Trademark Agent Ltd.
Agent: ZHOU Guocheng

Claims: 6 pages

Specification: 8 pages

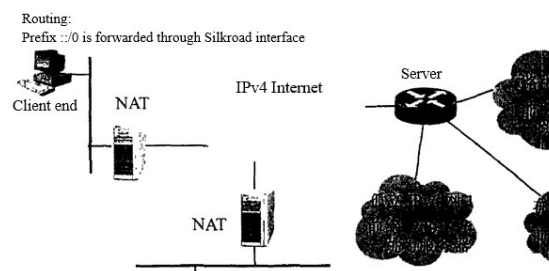
Drawings: 5 pages

[54] Title of Invention

An automatic tunnel method capable of traversing
network address translation

[57] Abstract

The present invention involves the field of Internet technology, a kind of automatic tunnel method capable of traversing NAT (Network Address Translation), i.e. this tunnel technology allows the tunnel body to have any type and any number of NAT, it is a kind of new tunnel technology in the transition period from IPv4 Internet to IPv6 Internet. The aim is to make the IPv6/IPv4 dual-stack nodes within NAT field to obtain the global end-to-end IPv6 connection. By using this tunnel technology, the IPv6/IPv4 dual-stack nodes within NAT field will communicate with the IPv6 nodes outside NAT field through the intermediate server, and will communicate with other the IPv6/IPv4 dual-stack nodes within NAT field.



ISSN 1008-4274

1. A kind of automatic tunnel method capable of traversing network address translation, wherein it is characterized in that a tunnel technology for encapsulating IPv6 data packet in UDP load is proposed, such a tunnel is known as SilkRoad Tunnel, SilkRoad is not affected by that the main body of tunnel has any type and any number of NAT, which can deliver the IPv6 data packet from the head node of tunnel to the end node of tunnel.

2. According to the method mentioned in Claim 1, it is characterized in that this tunnel technology defines 3 communication entities which are used to realize the above-mentioned method:

Silkroad client end represents the IPv6/IPv4 dual-stack node in the NAT field, supports the Silkroad tunnel function, it has one aggregate global unicast IPv6 address and one private IPv4 address;

Silkroad server is outside NAT field, which represents that it assigns IPv6 address and the IPv6/IPv4 dual-stack node with the routing function for client end, it supports Silkroad tunnel function, has one public IPv4 address, which can have the route leading to IPv6 backbone network, also can have the route leading to isolated IPv6 network;

Ordinary IPv6 node represents other IPv6 nodes besides the client end and the server.

3. According to the method mentioned in Claim 1, it is characterized in that the IPv6 address adopted when the client end communicates is a kind of address with prescribed form, it includes 64-bit IPv6 address prefix and 64-bit interface ID, the interface ID is composed of pseudo external port field, NAT type zone bit field, Silkroad address zone bit field and pseudo external address field, the descriptions of each part are as follows:

◆ IPv6 prefix:

The aggregate global unicast address prefix or the “site-local” address prefix formally assigned by IANA, which shouldn’t be the “link-local” address prefix or multicast address prefix;

◆ Pseudo external port:

External port is the port mapped by NAT and 0xFFFF and/or the subsequent 16-bit numerical value, the SilkRoad client end sends an initialized data packet to the server after it is started, its UDP port is mapped to a different port when the packet passes NAT, we call it as an external port; the server obtains this port from the received initialized data packet, considering that NAT will delete the expired mapping relation, the client end or the server will periodically send data packets to NAT to maintain such mapping relation, thus, the NAT translation table always keeps this mapping relation, the aim of conducting the operation on the external port is to prevent some NAT from translating the external ports in UDP data packet load, i.e. IPv6 header + IPv6 load;

◆ NAT type zone bit:

The length is 2 bits, it is used to represent the type of NAT where the client end is located, 00 represents that the client end is in the “cone” NAT field, 10 represents that the client end is in the “Restricted” NAT field, and 11 represents that the client end is in the “Symmetric” NAT field;

◆ Silkroad address zone bit:

The length is 14 bits, it is set as 0, representing that this address is a Silkroad address, the aim of putting this field in the middle of interface ID is to avoid conflicting with other addresses, because at present, as long as it is not an interface ID randomly assigned, the middle 16 bits are FFFE;

◆ Pseudo external address:

External address is the address mapped by NAT and 0xFFFFFFFF and/or the subsequent 32-bit numerical value, the client end sends an initialized data packet to the server after it is started, its private IPv4 address is mapped to a public IPv4 address when the packet passes NAT, we call it as an external address, the server obtains this address from the received initialized data packet, considering that NAT will delete the expired mapping relation, the client end or the server will periodically send data packets to NAT to maintain such mapping relation, thus, the NAT translation table always keeps this mapping relation, the aim of conducting the operation on the external address is to prevent some NAT from translating the external ports in UDP data

packet load, i.e. IPv6 header + IPv6 load.

4. According to the method mentioned in Claim 1, it is characterized in that when the client end and other IPv6 nodes are communicating, the data packets sent or received are composed of IPv4 header, UDP header, IPv6 header and IPv6 load;

The detailed description is as follows:

- IPv4 header:

The source IPv4 address is the IPv4 address of the client end, a private address, the destination IPv4 address is the IPv4 address of the server, if the destination is the ordinary IPv6 node or the external address of the client end mapped by NAT, if the destination is another client end;

- UDP header:

The source port is 5188, the destination port is 5188, if the destination is the ordinary IPv6 node or the external port of the client end mapped by NAT of the counterparty, if the destination is another client end;

- IPv6 header:

It includes the IPv6 address and the destination IPv6 address, wherein at least one is the SilkRoad Earth Ground;

- IPv6 load:

It is composed of 0 or several IPv6 extension headers and upper layer Protocol Data Unit, i.e. PDU;

In order to maintain the mapping relation in NAT, e.g. "cone" NAT's <source address, source port, destination address, destination port>, the client end needs to periodically sends data packets to NAT, which are called maintaining packet, in the IPv6 header of maintaining packet, the next-hop field is set as 59, representing that there is no IPv6 load.

5. According to the method mentioned in Claim 1, it is characterized in that the client end sends or receives data packets through the SilkRoad tunnel, the SilkRoad tunnel interface is a logic interface, it will automatically encapsulate the IPv6 data packet in the UDP load to send directly, similarly, the data packet received by Silkroad tunnel interface must be a encapsulated UDP data packet of IPv6 message, the client end has one default route (::/0), it deems all IPv6 addresses as the address on the same link and uses the SilkRoad tunnel interface to forward, the next-hop address of the default route is the destination address in IPv6 data packet, the next-hop interface is the SilkRoad tunnel interface, the server has the route leading to IPv6 backbone network and each isolated IPv6 network, also has the route leading to each client end, for any one data packet sent by IPv6 node in the IPv6 backbone network and each isolated IPv6 network, as long as the destination address prefix is the address prefix assigned to the client end by the server, it will be routed to the server, take the address prefix 2001:*/64 as an example, the server then forwards the data packet to the client end through the route to the client end; similarly, the client ends can realize reciprocal visits through the server, IPv6 backbone network and any one IPv6 node in each isolated IPv6.

6. According to the method mentioned in Claim 1, it is characterized in that the client end firstly registers with the server to obtain a SilkRoad address after it is started every time, so as to establish the communication with other IPv6 nodes, this process is called as the initialized configuration of client end;

The initialized configuration of client end is completed by sending a series of routing requests messages to the server, the server responds with router advertisement message, the router advertisement message contains the external address and external port information mapped by NAT, through this process, the client end obtains a SilkRoad address and judges which type of NAT field it is located;

The process of initialized configuration of client end is as follows:

1. The client end sends a route request message to the preferred server, i.e. Server 1, the source IPv6 address of the message is a "link-local" address, and its F field value is 00;

2. Server 1 sends a router advertisement message as a response after receiving the route request message, as the route request message displays that the client end is located in the "cone" NAT field (F field is set as 00),

it selects a different IPv4 address as the source address to send the router advertisement message, if the client end can receive this message, it represents that the client end is actually located in the “cone” NAT field;

3. If the client end fails to receive this router advertising message, it will resend a route request message to Server 1, the source IPv6 address of the route request message is another “link-local” address, and its F field value is 10;

4. Server 1 sends a router advertisement message as a response after receiving the route request message, as the route request message displays that the client end is located in the “Restricted” NAT field, it will take the destination IPv4 address in the route request message as the source IPv4 address to send the router advertisement message, if the client end can receive this message, it represents that the client end is actually located in the “Restricted” NAT field.

5. In order to clarify whether it is located in the “Symmetric” NAT field, the client end will resend the route request message to another server i.e. Server 2. After receiving the route request message, Server 2 sends a router advertisement message as a response;

6. The client end compares the received router advertisement message with the originally received router advertisement message, if the information for constructing the SilkRoad address contained in the messages is the same, representing that the mapping relation of NAT address port is one-to-one correspondence; if it is different, representing that NAT has mapped the same internal addresses and ports to different external addresses and ports, the mapping relation is one-to-many, thus the client end considers that it is located in “Symmetric” NAT field;

For the router advertisement message received according to Step 2, Step 4 or Step 6, the client end constructs a SilkRoad address as per the following:

- The first 64 bits of the address are set as the “prefix information option” in the router advertisement message, e.g. 2001:***/64;
- The next 16 bits are set as the external port contained in the router advertisement message;
- The subsequent 2 bits are set as 00, if the client end is located after “cone” NAT or at 10, if the client end is located after “Restricted” NAT or at 11, if the client end is located after “Symmetric” NAT;
- The next 14 bits are set to 0;
- The last 32 bits are set as the external address contained in the router advertisement message;

7. According to the method mentioned in Claim 1, it is characterized in that the communication situation between the Client end and other IPv6 nodes has the following 3 kinds:

I. The communication counterparty is the client end on the same link;

For data packets with destinations on the client end of the same link, the SilkRoad tunnel interface adopts the exchange of SilkRoad maintaining packet to substitute the address resolution process found by the neighbor, the exchange of SilkRoad maintaining packets is to obtain the IPv4 address of the communication counterparty on this link, so as to conduct direct communication;

In order to judge whether the host corresponding to the destination address is located on the same link, the client end will check its SilkRoad neighbor cache, each client end will send the SilkRoad maintaining packet to the IPv4 link connecting with it to show its existence on the link, all the client ends which have received these SilkRoad maintaining packets will put the SilkRoad address and the IPv4 address into its SilkRoad neighbor cache; therefore, if some destination SilkRoad address is located in the SilkRoad neighbor cache, the host corresponding to this address must be located on the same link, the communication between client ends on the same link is shown as the following:

1. Client end 1, i.e. the host sends a maintaining packet, its IPv4 destination address is one reserved IPv4 multicast address 224. 0. 0. 1 that is assigned by IANA, the destination IPv6 address of the IPv6 header of the maintaining packet is Client end 2, i.e. the destination host SilkRoad address;

2. After receiving the SilkRoad maintaining packet, Client end 2 judges whether the IPv4 addresses of

Client end 1 belong to the same link, whether the UDP port is 5188, if all the address ports are confirmed, Client end 2 responds by sending a maintaining packet to Client end 1, Client end 1 obtains the IPv4 address of Client end 2 after receiving this packet, and this address is the private address in the NAT field;

3. Then, Client end 1 directly sends data to Client end 2 without the need to pass NAT, further without the need to pass the Server;

II. Client end of another NAT field of communication counterparty;

This situation can be further subdivided into three situations:

1. This host is located in “cone” NAT field or “Restricted” NAT field, the destination host is located in “cone” NAT field

The communication between them can be conducted directly, as the “cone” NAT will not limit any source IPv4, Client end 1 can directly send data packets to Client end 2 to create the address port mapping relation in the NAT translation table of the counterparty, if Client end 1 is located in “Restricted” NAT, as after it has sent data to Client end 2, NAT1 has established the mapping relation with the destination of NAT2, thus the data packets of Client end 2 can pass NAT1;

2. The destination host is located in “Restricted” NAT field

The SilkRoad tunnel interface adopts the exchange of maintaining packets to substitute the address resolution process found by the neighbor, making the NAT where the counterparty is located to create the necessary address port mapping relation for communication, then the two client ends can directly exchange data packets, the specific communication process is as follows:

- Client end 1, i.e. the host sends a maintaining packet to Client end 2, i.e. destination host, the aim is to create the mapping relation with the destination of NAT2 in “Restricted” NAT1, so that the data from NAT2 can pass NAT1, if NAT1 is the “cone” type, this step can be omitted;

- Then Client end 1 sends a maintaining packet to Server 1, i.e. the server registered by Client end 1, the destination IPv4 address is the public IPv4 address of Server 1, and the destination IPv6 address is the address of Client end 2;

- After receiving this packet, Server 1 strips the IPv4 header and UDP header, the new data packet only has one IPv6 header, it forwards the new data packet to Server 2 through IPv6 network, i.e. the server registered by Client end 2, the dotted line represents that the packet operates in the IPv6 network;

- After receiving this packet, Server 2 extracts the external address and external port from the destination IPv6 address, and sends to Client end 2 after encapsulating this packet in UDP, the destination port of UDP is the extracted external port, the source port is 5188, the source address of IPv4 header is the IPv4 address of Server 2, the destination address is the extracted external address;

- After receiving the data packet from Server 2, Client end 2 extracts the external address and external port from the source IPv6 address, and learns from the address of Client end 1 that it isn't located in “Symmetric” NAT field, then send a maintaining packet to Client end 1, wherein, IPv4 source address is the private address of Client end 2, the IPv4 destination address is the extracted external address, the UDP source port is 5188, the destination port is the extracted external port, even though NAT1 is the “Restricted” type, as NAT1 has established the mapping relation of NAT2 in Step 1, this packet can pass NAT1;

Then Client end 1 can directly send data packets to Client end 2 without the need of forwarding by intermediate server. Before sending, it extracts the external address and external port from the destination IPv6 address which is also the SilkRoad address of Client end 2, then encapsulate the data packet in UDP, the destination IPv4 address is the extracted external address, the source IPv4 address is the private IPv4 address of the host, the destination port is the extracted external port, the source port is 5188, Client end 2 un-encapsulates this packet after receiving this packet, if it sends data packets to Client end 1, it must execute the same encapsulating process with Client end 1;

3. This host or the destination host is located in “Symmetric” NAT field

The data packets of communication between them must be forwarded through the server, the detailed process is as follows:

- The Client end 1, i.e. the host encapsulates the data packet to be sent in UDP, the destination IPv4 address is the public IPv4 address of the Server 1, the source IPv4 address is the private IPv4 address of this host, both the destination port and the source port are 5188.
- Server 1, i.e. the server registered by Client end 1 strips IPv4 and UDP header, forwards the un-encapsulated IPv6 data packets to Server 2 through IPv6 network, the dotted line represents that this packet operates in the IPv6 network;
- Server 2, i.e. the server registered by Client end 2 extracts the external address and external port from the destination IPv6 address after receiving this packet, encapsulates this packet in UDP, and then sends to Client end 2, i.e. the destination host, the destination port of UDP is the extracted external port, the source port is 5188, the source address of IPv4 header is the IPv4 address of Server 2, the destination address is the extracted external address;
- After Client end 2 receives a data packet from Server 2, if it wants to send a data packet to Client end 1, it will encapsulate the packet in UDP, the destination IPv4 address is the public IPv4 address of the Server 2, the source IPv4 address is the private IPv4 address of this host, both the destination port and the source port are 5188.

III. The communication counterparty is an ordinary IPv6 node

The communication data packet between the client end and ordinary IPv6 node must be forwarded through the server, the client end and the server adopt the “SilkRoad” tunnel to transfer the data flow, the data flow between the server and ordinary IPv6 node directly utilizes the IPv6 network to transfer or uses the IPv4 network to transfer through IPv6-over-IPv4 tunnel;

The communication process diagram from the client end to the ordinary IPv6 node is as follows:

- The client end encapsulates the data packet to be sent in the UDP, the destination IPv4 address is the public IPv4 address of the server, the source IPv4 address is the private IPv4 address of the host, both the destination port and the source port are 5188;
- The server strips the IPv4 and the UDP header, forwards the un-encapsulated IPv6 data packet to IPv6 node through IPv6 network, the dotted line represents that this packet operates in the IPv6 network;
- The data packet sent back by IPv6 node is routed to the server finally, the dotted line represents that this packet operates in the IPv6 network;
- The server extracts the external address and external port from the destination IPv6 address after receiving this packet, and encapsulates this data packet in the UDP, its source IPv4 address of IPv4 header is the public IPv4 address of the server, the destination address is the extract external address, the source port is 5188, and the destination port is the extracted external port;

The communication process diagram from ordinary IPv6 node to the client end is as follows:

- The IPv6 node sends data packets to the client end, the destination IPv6 address is the SilkRoad address of client end, the dotted line represents that this packet operates in the IPv6 network;
- This data packet will be routed to the server finally, the server extracts the external address and external port from the destination IPv6 address, and encapsulates this data packet in UDP, the source IPv4 address of IPv4 header is the public IPv4 address of server, the destination address is the extracted external address, the source port is 5188, the destination port is the extracted external address, then sends the encapsulated data packets to the client end;
- The client end encapsulates the data packet to be sent in the UDP, the destination IPv4 address is the public IPv4 address of server, the source IPv4 address is the private IPv4 address of the host, both the destination port and the source port are 5188;
- The server strips the IPv4 and the UDP header, forwards the un-encapsulated IPv6 data packet to IPv6

node through IPv6 network, the dotted line represents that this packet operates in the IPv6 network.

An automatic tunnel method capable of traversing network address translation

Field of the Invention

The present invention involves the field of Internet technology, especially a kind of automatic tunnel which can traverse NAT (Network Address Translation). This method utilizes the existing IPv4 network routing system to transfer the IPv6 data packet, it is a tunnel technology in the transition period from IPv4 to Ipv6, so as to realize the transition from IPv4 to IPv6.

Background technology

NAT (Network Address Translation) technology is an effective method for solving the insufficient IPv4 addresses, it is extremely widely deployed in China. According to the different mapping relations, NAT is divided into 3 types: “cone” NAT, “Restricted” NAT and “Symmetric” NAT.

When receiving the data packet from the internal network, NAT translates the IPv4 source address (private address) of the data packet into another address (public address), we call this address as the external address, it translates the TCP or UDP source port number into another port number, we call this port number as the external port, then sends the translated data packet to the external network. And it adds the mapping relation between the source address, source port and the external address, external port in the translation table it maintains. After the external network receives the data packet, if it sends back the data packet, it sets the external address as the destination address of data packet, and the external port as the destination port of data packet. When NAT receives the data packet from the external network, according to the mapping relation in the translation table, it translates the IPv4 destination address and TCP or UDP destination port (i.e. the original external address and external port) of data packet into the source address and source port, and then sends to the internal network.

In “cone” NAT, the mapping relation of the translation table is <source address, source port, external address, external port>. As long as the <destination address and destination port> in the data packet from the external network comply with the <external address and external port> in the mapping relation, it will translate them into the <source address and source port> in the mapping relation, then sends this data packet to the internal network.

In “Restricted” NAT, the mapping relation of the translation table is <source address, source port, external address, external port, destination address and destination port> or <source address, source port, external address, external port and destination address>. If the <destination address, destination port, source address and source port> comply with the <external address, external port, destination address and destination port> or <external address, external port and destination address> in the mapping relation, it will translate the <destination address and destination port> of the data packet into the <source address and source port> in the mapping relation, then sends this data packet to the internal network.

The mapping relation of the above-mentioned two kinds of NAT is one-to-one, i.e. as long as the preimage <source address and source port> doesn't change, the mapped image <external address and external port> also doesn't change. “Symmetric” NAT is different, its mapping relation is one-to-many, for the same preimage <source address and source port>, according to the different destination addresses of data packet, it will be mapped to different images <external address and external port>.

NAT destroyed the end-to-end feature of IP protocol while solving the insufficient IPv4 addresses, and IPv4 Protocol itself has many deficiencies in aspects of address assignment strategy, security, access, Qos and mobility, IPv6 is designed for solving these problems. With the increase of IPv6 Internet research and operation investment by the governments and enterprises, the transformation of IPv4 Internet to IPv6 Internet is

imperative. But this transformation is not accomplished in an action, it needs a long process. At present, IETF has proposed the 3 kinds of main migration mechanism transiting from IPv4 to IPv6: dual-stack, protocol translation and tunnel.

The dual-stack node realizes IPv4 Protocol and IPv6 Protocol at the same time, which can establish the communication with IPv4 or IPv6. The node decides to adopt IPv4 Protocol or IPv6 Protocol to send or receive data packets according to the destination IP address. At present, the dual-stack is the most extensive migration mechanism. But the dual-stack only allows the communication between the same IP version.

Protocol translation is to translate the data packets from one protocol to another protocol transparently. Thus, the communication between the pure IPv6 node and pure IPv4 node can be established without modifying any software. The most famous protocol translation mechanism is NAT-PT. NAT-PT adopts SIIT (Stateless IP/ICMP T router advertisement translator) to conduct protocol translation, when the IPv6 node and the IPv4 node need to establish communication, NAT-PT assigns a provisional IPv4 address to IPv6 node, and maintains the mapping relation between IPv4 address and Ipv6 address during the session. Meanwhile, it also can provide the application layer gateway function, and execute the translation of IPv4 and IPv6 DNS request and response.

The essence of tunnel technology is to encapsulate the IPv6 (IPv4) data packets in the IPv4 (IPv6) data packets, utilizes the existing IPv4 (IPv6) routing system to transfer, so as to solve the problem of mutual communication between the nodes adopting the same IP version and separated by incompatible network. In the early transition period, the IPv4 network plays a dominant role, IPv6 network is like isolated islands in the whole IPv4 ocean, and the communication among these islands can adopt IPv6-over-IPv4 tunnel to realize. In the later transition period, the IPv6 network plays a dominant role, similarly, the communication among each IPv4 island can adopt the IPv4-over-IPv6 tunnel to realize.

Generally, the tunnel is composed of 3 parts: The head node of tunnel, which encapsulates the data packets; the end node of tunnel, which un-encapsulates the data packets; the body of tunnel, which actually is a IPv6 or IPv4 pat, transferring the encapsulated data packets from the head node of tunnel to the end node of tunnel. According to the difference of implementation methods of each part, the tunnel technologies include 6to4, ISATAP, 6over4, Tunnel Broker and DSTM.

At present, most tunnel technologies adopt the method of encapsulating the IPv6 data packets in the IPv4 load to solve the communication problem between the two IPv6 nodes separated by the IPv4 network. However, these tunnel technologies cannot support between the IPv6 node and other IPv6 nodes in the NAT field, i.e., these tunnels don't allow the NAT in the body of tunnel. The reason is that the present NAT basically doesn't allow IPv6-in-IPv4 data packets (i.e. the protocol type field of IPv4 header is the data packet of 41) to pass. NAT discards it after receiving the IPv6-in-IPv4 data packet due to incognizance.

Summary of the Invention

The present invention proposes a kind of method for automatic tunnel which can traverse NAT, it aims to solve the mutual communication problem between the IPv6 node and other IPv6 nodes (which can be inside or outside NAT field) within NAT field.

Technical solution of the present invention:

Therefore, a kind of tunnel technology encapsulating the IPv6 data packet in the UDP load is proposed, we call it as "SilkRoad", correspondingly, we call such tunnel as SilkRoad Tunnel, SilkRoad isn't affected by any type and any number of NAT on the body of tunnel, which can transfer the IPv6 data packet from the head node of tunnel to the end node of tunnel.

SilkRoad Tunnel defines 3 communication entities, which are used to realize the above-mentioned method:

1. Silkroad client end (hereinafter referred to as the client end) represents the IPv6/IPv4 dual-stack node in the NAT field, it supports the Silkroad tunnel function, has an aggregate global unicast IPv6 address (we call it as SilkRoad address) and a private IPv4 address.

2. Silkroad server (hereinafter referred to as the server) is outside the NAT field, representing that it assigns IPv6 address and the IPv6/IPv4 dual-stack node with the routing function for the client end, it supports the Silkroad tunnel function, has a public IPv4 address, can have the route leading to IPv6 backbone network, also the route leading to the isolated IPv6 network.

3. Ordinary IPv6 node represents other IPv6 nodes besides the client end and the server.

Brief Description of the Drawings

Fig. 1 is the form diagram of SilkRoad address assigned to the client end by the server.

Fig. 2 is the form diagram of the data packet defined by SilkRoad.

Fig. 3 is the form diagram of the maintaining packet defined by SilkRoad.

Fig. 4 is the routing system diagram of SilkRoad.

Fig. 5 is the process diagram of initialization configuration after the client end is started.

Fig. 6 is the communication diagram between the client ends on the same link.

Fig. 7 is the diagram of the first communication situation between client ends of different NAT fields.

Fig. 8 is the diagram of the second communication situation between client ends of different NAT fields.

Fig. 9 is the diagram of the third communication situation between client ends of different NAT fields.

Fig. 10 is the communication process diagram from the client end to the ordinary IPv6 node.

Fig. 11 is the communication process diagram from ordinary IPv6 node to the client end.

The IPv6 address adopted by client ends during communication is a kind of address with prescribed form, it includes the 64-bit IPv6 address prefix and 64-bit interface ID, the interface ID is composed of the pseudo external port field, NAT type zone bit field, Silkroad address zone bit field and pseudo external address field, as shown in Attached Fig. 1. The description of each part is as follows:

◆ IPv6 prefix:

The aggregate global unicast address prefix or the “site-local” address prefix formally assigned by IANA shouldn’t be the “link-local” address prefix or multicast address prefix.

◆ Pseudo external port:

The external port (NAT-mapped port) and 0xFFFF and/or the subsequent 16-bit numerical value. The SilkRoad client end send an initialized data packet to the server after it is started, the UDP port of this packet is mapped to a different port when it passes NAT, we call it as the external port.

The server obtains this port from the received initialized data packet. Considering that NAT will delete the expired mapping relation, the client end (or server) will periodically send data packets to NAT to maintain such mapping relation, thus, the NAT translation table always keeps this mapping relation. The aim of the operation conducted on the external port is to prevent some “smarty-pants” NAT to translate the external port of UDP data packet load, i.e. IPv6 header + IPv6 load.

◆ NAT type zone bit:

The length is 2 bits, it is used to represent the type of NAT where the client end is located. 00 represents that the client end is located in the “cone” NAT field, 10 represents that the client end is located in the “Restricted” NAT field, and 11 represents that the client end is located in the “Symmetric” NAT field.

◆ Silkroad address zone bit:

The length is 14 bits, it is set as 0, representing that this address is a Silkroad address. The aim of putting this field in the middle of interface ID is to avoid conflicting with other addresses, because at present, as long as it is not an interface ID randomly assigned, the middle 16 bits are FFFE.

◆ Pseudo external address:

External address is the address mapped by NAT and 0xFFFFFFFF and/or the subsequent 32-bit numerical value, the client end sends an initialized data packet to the server after it is started, its private IPv4 address is mapped to a public IPv4 address when the packet passes NAT, we call it as an external address, the server obtains this address from the received initialized data packet, considering that NAT will delete the expired mapping relation, the client end (or the server) will periodically send data packets to NAT to maintain such mapping relation, thus, the NAT translation table always keeps this mapping relation, the aim of conducting the operation on the external address is to prevent some “smarty-pants” NAT from translating the external ports in UDP data packet load, i.e. IPv6 header+IPv6 load; The sent or received data packet when the client end communicates with other IPv6 nodes is called as the Silkroad data packet, it is composed of the IPv4 header, UDP header, IPv6 header and IPv6 load, as shown in Attached Fig. 2. The detailed description is as follows:

- IPv4 header:

The source IPv4 address is the IPv4 address of the client end (private address), the destination IPv4 address is the IPv4 address of the server (if the destination is the ordinary IPv6 node) or the external address of the client end mapped by NAT (if the destination is another client end).

- UDP header:

The source port is 5188, the destination port is 5188 (if the destination is the ordinary IPv6 node) or the external port of the client end mapped by NAT of the counterparty (if the destination is another client end).

- IPv6 header:

It includes the source IPv6 address and the destination IPv6 address, wherein at least one is the SilkRoad address.

- IPv6 load:

It is composed of 0 or several IPv6 extension headers and upper layer Protocol Data Unit (PDU).

In order to maintain the mapping relation in NAT, e.g. “cone” NAT’s <source address, source port, destination address, destination port>. The client end needs to send data packet to NAT periodically, we call such data packet as the maintaining packet, as shown in Attached Fig. 3. In the IPv6 header of the maintaining packet, the next-hop field is set as 59, representing that there’s no IPv6 load.

The routing system of Silkroad is as shown in Attached Fig. 4. The client end sends or receives data packet through the SilkRoad tunnel interface, SilkRoad tunnel interface is a logic interface, it will automatically encapsulate IPv6 data packet in the UDP load for sending. Similarly, the data packet received by the Silkroad tunnel interface must be a UDP data packet encapsulated with IPv6 message. The client end has a default route (:::0), it deems all IPv6 addresses as the addresses on the same link and uses the SilkRoad tunnel interface for forwarding. The next-hop address of the default route is the destination address in the IPv6 data packet, and the next-hop interface is the SilkRoad tunnel interface. The server has the route leading to the IPv6 backbone network and each isolated IPv6 network, also the route leading to each client end. For the data packets sent by the IPv6 backbone network and any IPv6 node in each isolated IPv6 network, as long as the destination address prefix is the address prefix assigned to the client end by the server, will all be routed to the server (take the address prefix 2001:*/64 as an example in the figure), the server will forward the data packets to the client end through the routing to the client end. Similarly, the client end can realize reciprocal visits through the server, the IPv6 backbone network and any IPv6 node in each isolated IPv6 network.

The client end firstly registers with the server to obtain a SilkRoad address after it is started every time, so as to establish the communication with other IPv6 nodes, this process is called as the initialized configuration of client end, as shown in Attached Fig. 5.

The initialized configuration of client end is completed by sending a series of route request messages to the server, the server responds with router advertisement message, the router advertisement message contains the external address and external port information mapped by NAT. Through this process, the client end obtains a SilkRoad address and judges which type of NAT field it is located.

The process of initialized configuration of client end is as follows:

1. The client end send a route request message to the preferred server (Server 1 in the figure), the source IPv6 address of the message is a “link-local” address with the F field value of 00.

2. Server 1 sends a router advertisement message as a response after receiving the route request message, as the route request message displays that the client end is located in the “cone” NAT field (F field is set as 00), it selects a different IPv4 address as the source address to send the router advertisement message, if the client end can receive this message, it represents that the client end is actually located in the “cone” NAT field.

3. If the client end fails to receive this router advertising message, it will resend a route request message to Server 1, the source IPv6 address of the route request message is another “link-local” address, and its F field value is 10.

4. Server 1 sends a router advertisement message as a response after receiving the route request message, as the route request message displays that the client end is located in the “Restricted” NAT field, it will take destination IPv4 address as the source IPv4 address to send the router advertisement message, if the client end can receive this message, it represents that the client end is actually located in the “Restricted” NAT field.

5. In order to clarify whether it is located in the “Symmetric” NAT field, the client end will resend the route request message to another server (Server 2 in Fig. 5), Server 2 will send a router advertisement message as a response after receiving the route request message.

6. The client end compares the received router advertisement message with the originally received router advertisement message, if the information for constructing the SilkRoad address contained in the messages is the same, representing that the mapping relation of NAT address port is one-to-one correspondence. If it is different, representing that NAT has mapped the same internal addresses and ports to different external addresses and ports, the mapping relation is one-to-many, thus the client end considers that it is located in “Symmetric” NAT field.

For the router advertisement message received according to Step 2, Step 4 or Step 6, the client end constructs a SilkRoad address as per the following:

- The first 64 bits of the address are set as the “prefix information option” in the router advertisement message (e.g. 2001:***/64).
- The next 16 bits are set as the external Port contained in the router advertisement message.
- The subsequent 2 bits are set as 00 (if the client end is located after “cone” NAT) or at 10 (if the client end is located after “Restricted” NAT) or at 11 (if the client end is located after “Symmetric” NAT).
- The next 14 bits are set to 0.
- The last 32 bits are set as the external address contained in the router advertisement message.

The communication situation between the client end and other IPv6 nodes is divided into the following 3 situations:

I. The communication counterparty is the client end on the same link;

For data packets with destinations on the client end of the same link, the SilkRoad tunnel interface adopts the exchange of SilkRoad maintaining packet to substitute the address resolution process found by the neighbor, the exchange of SilkRoad maintaining packets is to obtain the IPv4 address of the communication counterparty on this link, so as to conduct direct communication;

In order to judge whether the host corresponding to the destination address is located on the same link, the client end will check its SilkRoad neighbor cache, each client end will send the SilkRoad maintaining packet to the IPv4 link connecting with it to show its existence on the link, all the client ends which have received these SilkRoad maintaining packets will put the SilkRoad address and the IPv4 address into its SilkRoad neighbor cache; therefore, if some destination SilkRoad address is located in the SilkRoad neighbor cache, the host corresponding to this address must be located on the same link, the communication between client ends on the same link is as shown in Attached Fig. 6. The communication process is as follows:

1. Client end 1, this host sends a maintaining packet, its IPv4 destination address is a reserved IPv4 multicast address 224. 0. 0. 1 (assigned by IANA). The destination IPv6 address of IPv6 header of maintaining packet is Client end 2, the SilkRoad address of the destination host.

2. After receiving the SilkRoad maintaining packet, Client end 2 judges whether the IPv4 addresses of Client end 1 belong to the same link, whether the UDP port is 5188. If all the address ports are confirmed, Client end 2 sends a maintaining packet to Client end 1 as a response, Client end 1 obtains the IPv4 address of Client end 2 after receiving this packet (this address is the private address in the NAT field).

3. Then, Client end 1 directly sends data to Client end 2 without the need to pass NAT, further without the need to pass the server.

II. Client end of another NAT field of communication counterparty;

This situation can be further subdivided into three situations:

1. This host is located in “cone” NAT field or “Restricted” NAT field, the destination host is located in “cone” NAT field

The communication between them can be conducted directly, as shown in Attached Fig. 7. As “cone” NAT won’t limit any source IPv4 address, Client end 1 will send data packets to Client end 2 directly to create the address port mapping relation in the NAT translation table of the counterparty. If Client end 1 is located in “Restricted” NAT, as NAT1 has established the destination as the mapping relation of NAT2 after sending data to Client end 2, the data packets of Client end 2 can pass NAT1;

2. The destination host is located in “Restricted” NAT field

The SilkRoad tunnel interface adopts the exchange of maintaining packets to substitute the address resolution process found by the neighbor, making the NAT where the counterparty is located to create the necessary address port mapping relation for communication, then the two client ends can directly exchange data packets, as shown in Figure 8. The detailed communication process is as follows:

- Client end 1 (i.e. the host) sends a maintaining packet to Client end 2 (i.e. destination host), the aim is to create the mapping relation with the destination of NAT2 in “Restricted” NAT1, so that the data from NAT2 can pass NAT1. If NAT1 is the “cone” type, this step can be omitted.

- Then Client end 1 sends a maintaining packet to Server 1 (i.e. the server registered by Client end 1), the destination IPv4 address is the public IPv4 address of Server 1, and the destination IPv6 address is the address of Client end 2.

- After receiving this packet, Server 1 strips the IPv4 header and UDP header, the new data packet only has one IPv6 header. The new data packet is forwarded to Server 2 (i.e. the server registered by Client end 2) through IPv6 network. The dotted line in the figure represents that this packet operates in the IPv6 network.

- After receiving this packet, Server 2 extracts the external address and external port from the destination IPv6 address, and sends to Client end 2 after encapsulating this packet in UDP. The destination port of UDP is the extracted external port, the source port is 5188, the source address of IPv4 header is the IPv4 address of Server 2, and the destination address is the extracted external address.

- After receiving the data packet from Server 2, Client end 2 extracts the external address and external port of the Client end 1 from the source IPv6 address, and learns from the address of Client end 1 that it isn’t located in “Symmetric” NAT field. Then send a maintaining packet to Client end 1, wherein the IPv4 source address is the private address of Client end 2, the IPv4 destination address is the extracted external address. The UDP source port is 5188, the destination port is the extracted external port. Even though NAT1 is the “Restricted” type, as NAT1 has established the mapping relation to NAT2 in Step 1, this packet can pass NAT1.

Next, client end 1 can directly send data packets to client end 2 without forwarding from an intermediate server. Before sending, extract the external address and external port from the destination IPv6 address which is also the SilkRoad address of Client end 2, then encapsulate the data packet in UDP, the destination IPv4 address is the extracted external address, the source IPv4 address is the private IPv4 address of this host, the

destination port is the extracted external port, and the source port is 5188. Client end 2 un-encapsulates this packet after receiving it, if it sends data packet to Client end 1, it must execute the same un-encapsulating process with Client end 1.

3. This host or the counterparty is located in “Symmetric” NAT field

The communication data packet between them must be forwarded through the server, as shown in Attached Fig. 9. The detailed process is as follows:

- The client end 1, the host encapsulates the data packet to be sent in UDP, the destination IPv4 address is the public IPv4 address of the Server 1, the source IPv4 address is the private IPv4 address of this host, both the destination port and the source port are 5188.

- Server 1 (i.e. the server registered by Client end 1) strips IPv4 and UDP header, forwards the un-encapsulated IPv6 data packets to Server 2 through IPv6 network. The dotted line in the figure represents that this packet operates in the IPv6 network.

- Server 2 (i.e. the server registered by Client end 2) extracts the external address and external port from the destination IPv6 address after receiving this packet, encapsulates this packet in UDP, and then sends to the destination host of Client end 2. The destination port of UDP is the extracted external port, the source port is 5188, the source address of IPv4 header is the IPv4 address of Server 2, and the destination address is the extracted external address.

- After client end 2 receives a data packet from server 2, if it wants to send a data packet to client end 1, it will encapsulate the packet in UDP. the destination IPv4 address is the public IPv4 address of the server 2, the source IPv4 address is the private IPv4 address of this host, both the destination port and the source port are 5188.

III. The communication counterparty is an ordinary IPv6 node

The communication data packet between the client end and ordinary IPv6 node must be forwarded through the server, the client end and the server adopt the “SilkRoad” tunnel to transfer the data flow, the data flow between the server and ordinary IPv6 node directly utilizes the IPv6 network to transfer or uses the IPv4 network to transfer through IPv6-over-IPv4 tunnel.

The communication process from the client end to the ordinary IPv6 node is as shown in Attached Fig. 10, the detailed description is as follows:

- The client end encapsulates the data packet to be sent in UDP, the destination IPv4 address is the public IPv4 address of the server, the source IPv4 address is the private IPv4 address of this host, both the destination port and the source port are 5188.

- The server strips the IPv4 and the UDP header, forwards the un-encapsulated IPv6 data packet to IPv6 node through IPv6 network. The dotted line in the figure represents that this packet operates in the IPv6 network.

- The data packet send back to the client end by the IPv6 node will be routed to the server finally. The dotted line in the figure represents that this packet operates in the IPv6 network.

- The server extracts the external address and external port from the destination IPv6 address after receiving this packet, and encapsulates this data packet in the UDP, its source IPv4 address of IPv4 header is the public IPv4 address of the server, the destination address is the extract external address, the source port is 5188, and the destination port is the extracted external port.

The communication process from ordinary IPv6 node to the client end is as sown in Attached Fig. 11, the detailed description is as follows:

- The IPv6 node sends data packets to the client end, the destination IPv6 address is the SilkRoad address of client end. The dotted line in the figure represents that this packet operates in the IPv6 network.

- This data packet will be routed to the server finally, the server extracts the external address and external port from the destination IPv6 address, and encapsulates this data packet in UDP, the source IPv4 address of

IPv4 header is the public IPv4 address of server, the destination address is the extracted external address, the source port is 5188, the destination port is the extracted external address. Then send the encapsulated data packet to the client end.

- The client end encapsulates the data packet to be sent in UDP, the destination IPv4 address is the public IPv4 address of the server, the source IPv4 address is the private IPv4 address of this host, both the destination port and the source port are 5188.

- The server strips the IPv4 and the UDP header, forwards the un-encapsulated IPv6 data packet to IPv6 node through IPv6 network. The dotted line in the figure represents that this packet operates in the IPv6 network.

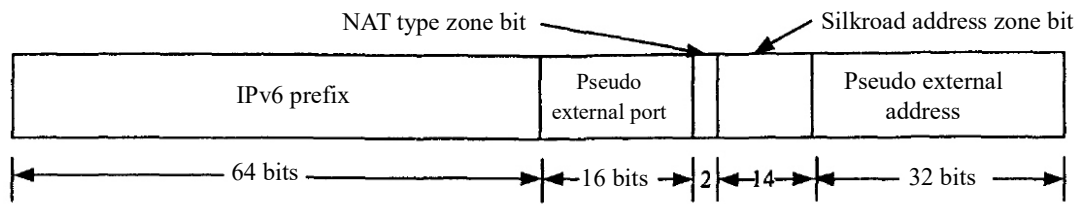


Fig. 1

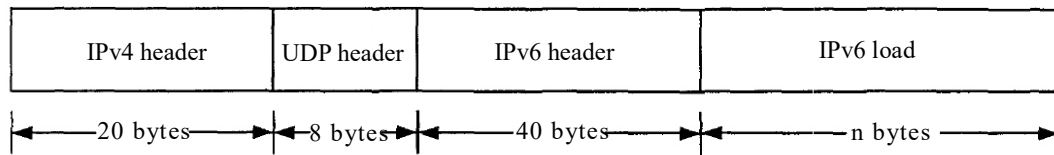


Fig. 2

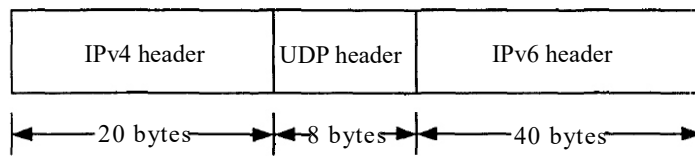


Fig. 3

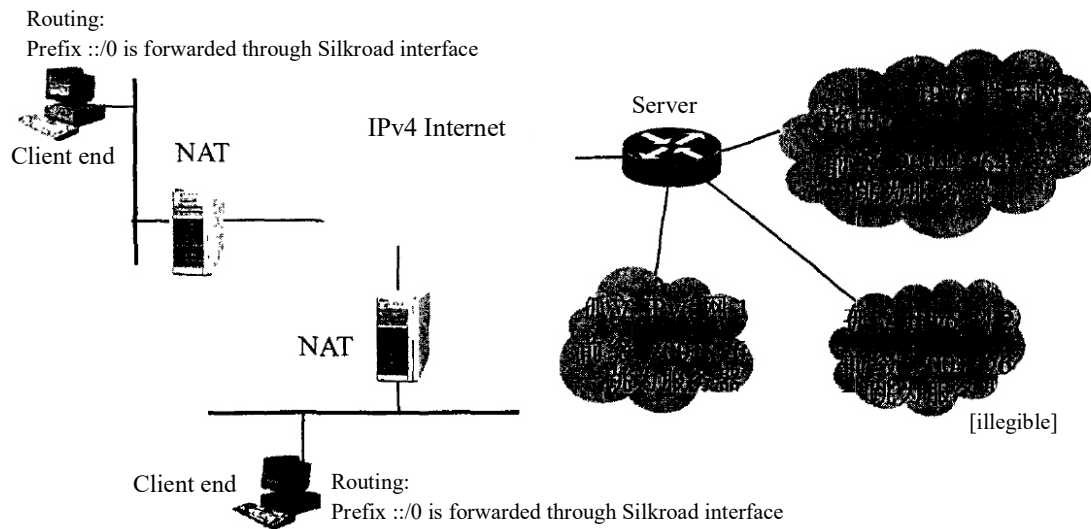


Fig. 4

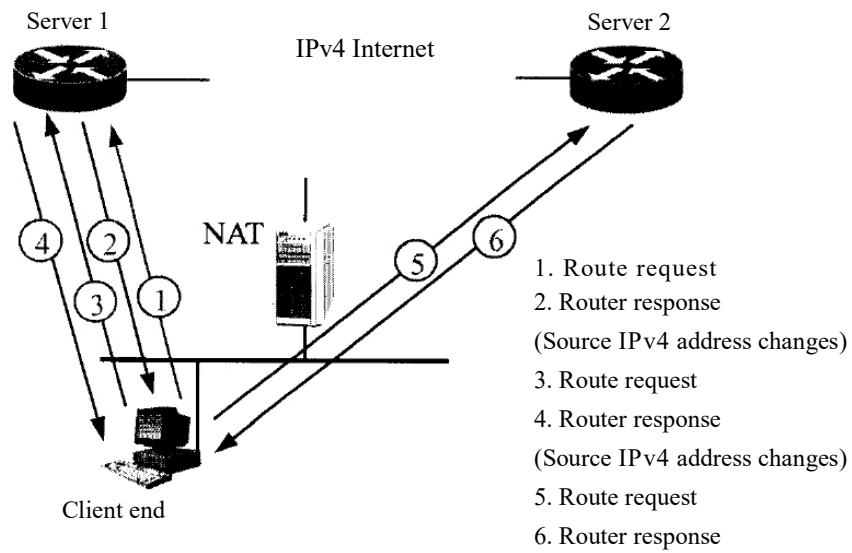


Fig. 5

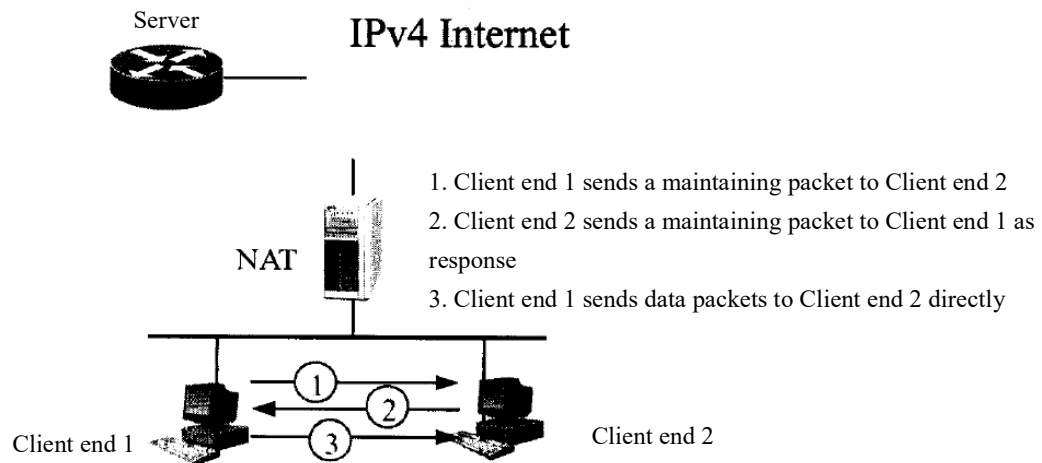


Fig. 6

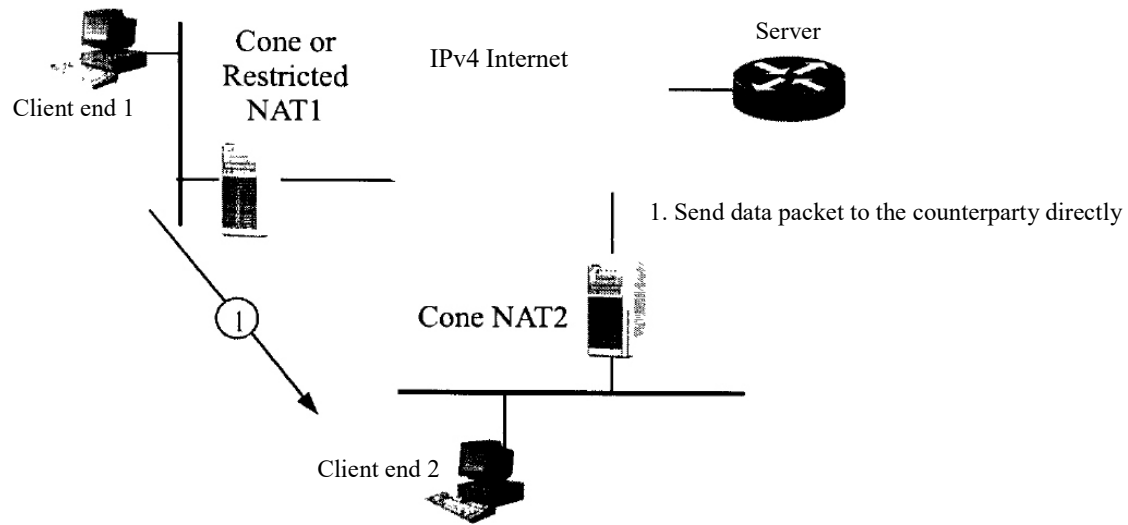


Fig. 7

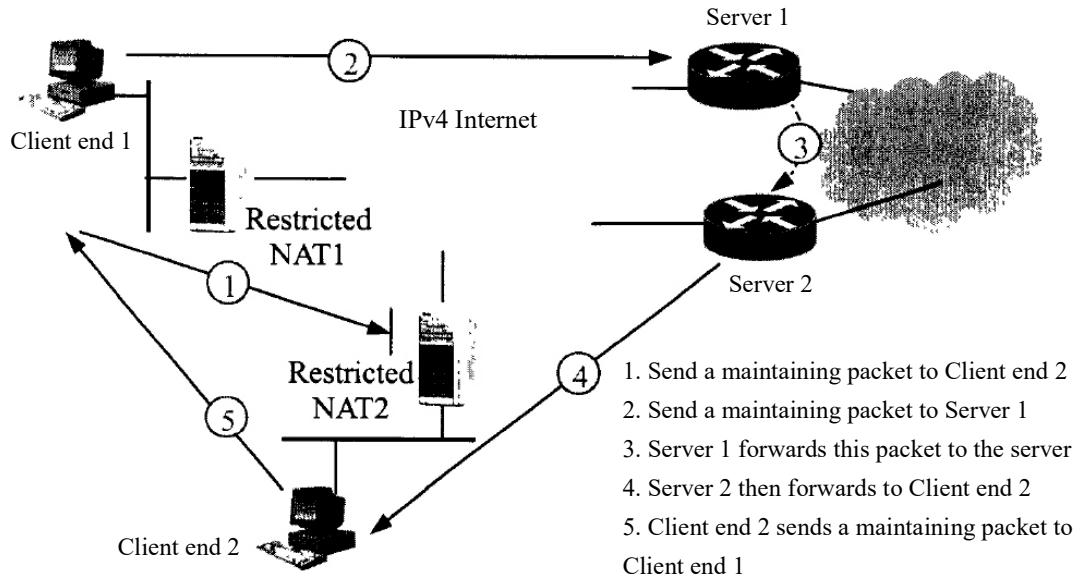


Fig. 8

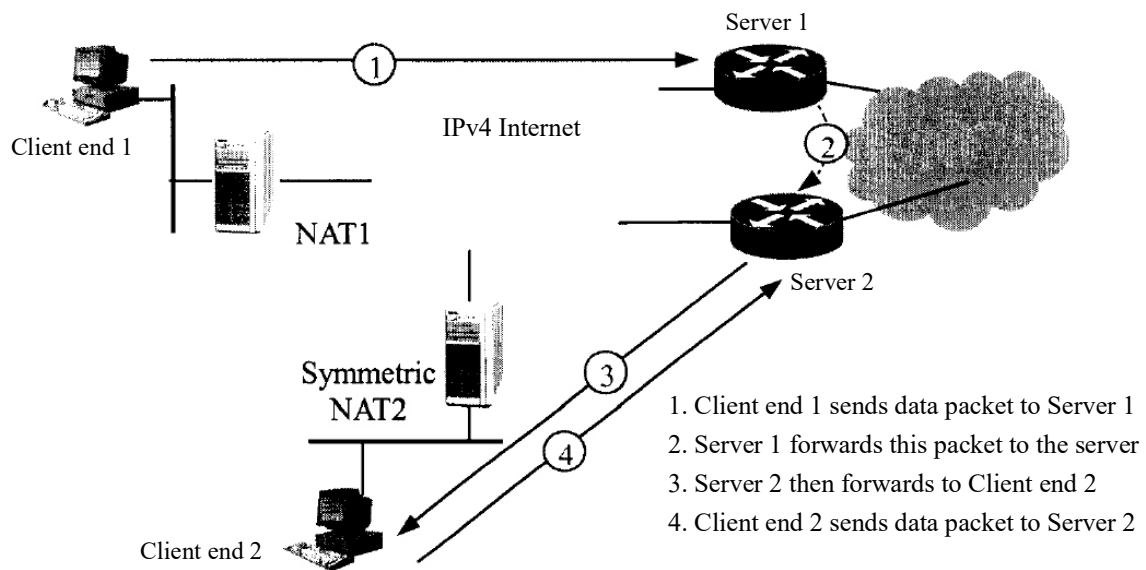


Fig. 9

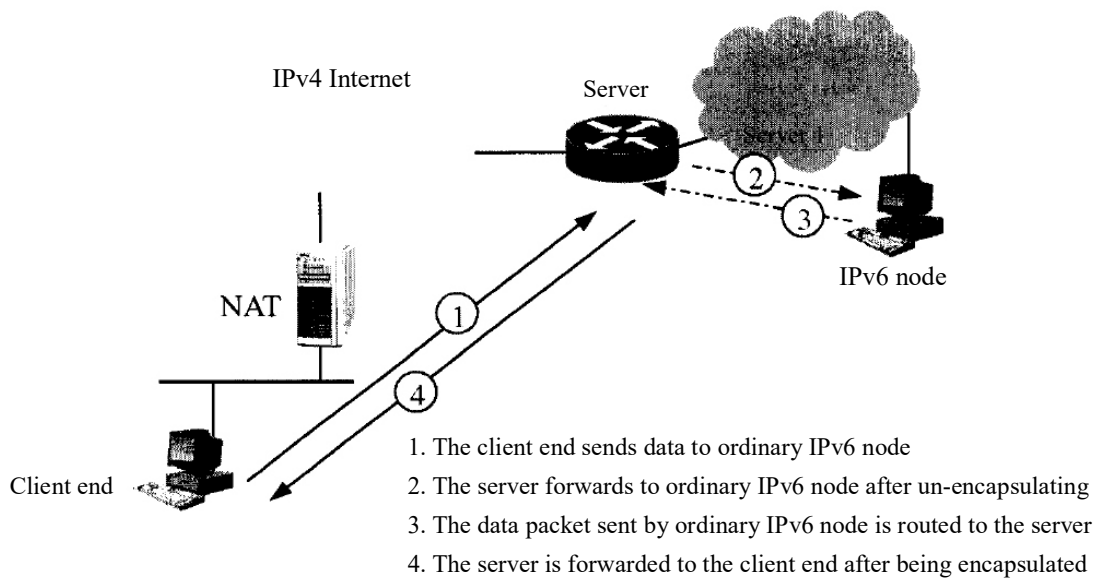


Fig. 10

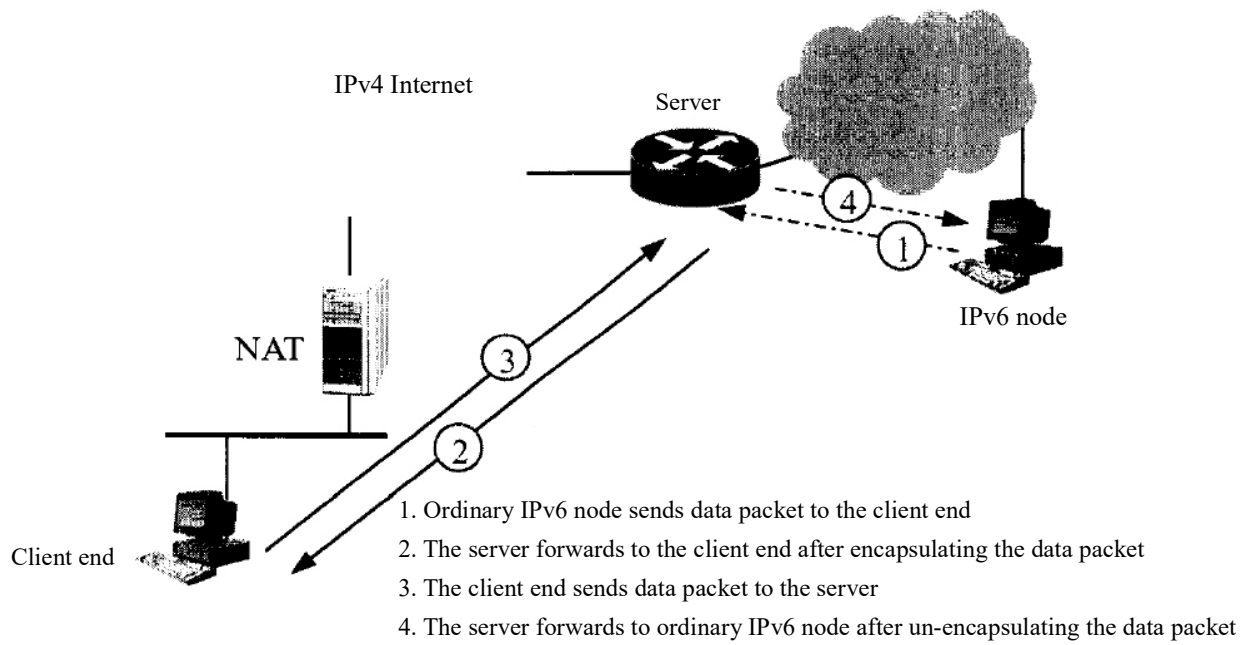


Fig. 11