IETF v6ops Working Group
Internet-Draft
Expires: January 17, 2006

Min Liu
Xianguo Wu
ICT
Mingye Jin
China Unicom
Defeng Li
HUAWEI

July, 2005

Tunneling IPv6 with private IPv4 addresses through NAT devices
draft-liumin-v6ops-silkroad-03.txt

Status of this memo

Copyright Notice

Abstract

The growth of IPv6 networks started mainly using the transport facilities offered by the current Internet. This led to the development of several techniques to manage IPv6 over IPv4 tunnels.

However, classic tunneling methods do not work when the IPv6

candidate node is isolated behind a Network Address Translator (NAT) device. We propose here a service, called Silkroad, to enable nodes located behind one or several IPv4 NATs to obtain IPv6 connectivity. It can provide IPv6 connectivity through all existing NAT types and does not require any update of them. In addition, Silkroad could provide managed IPv6 prefixes with path optimized routing directly between clients.

Table of Contents:

1. Introduction

The growth of IPv6 networks started mainly using the transport facilities offered by the current Internet. Complete upgrades of current Internet from IPv4 to IPv6 will take a long time. Thus the key to a successful IPv6 transition is compatibility with the large installed base of IPv4 hosts and routers. This led to the development of several techniques to manage IPv6 over IPv4 tunnels. Classic tunneling methods designed for IPv6 transition operate by sending IPv6 packets as payload of IPv4 packets. However, these methods do not work when the IPv6 candidate node is isolated behind a Network Address Translator (NAT) device. The reason is that usually NATs will perform ingress filtering and refuse to allow the transmission of many payload types.

In this memo, we propose a service, called Silkroad, to enable nodes located behind one or several IPv4 NATs to obtain IPv6 connectivity. It provides connectivity for clients located behind all existing NAT types, including symmetric NAT. Silkroad does not need special IPv6 addressing prefix and can provide the users with stable/dynamic IPv6 address. In addition, Silkroad could provide route optimization between clients. Unlike Teredo, which is primarily a way to make 6to4 style automation work through NATs, Silkroad is one way to make a managed tunnel work through NATs. It is a efficient method for ISPs that are willing to provide IPv6 connectivity to their customers behind NATs, but may not be able to do it natively due to a number of reasons. Silkroad approach is expect to be useful to stimulate the growth of IPv6 and to allow early IPv6 network providers to provide easy access to their IPv6 network.

This document is intended to present a framework describing the guidelines for the provision of a Silkroad service within the Internet. It details the general architecture of the proposed approach and also outlines a set of viable implementation. The memo

is organized as follows. Section 2 contains the definition of the terms used in the memo. Section 3 introduces the background information. Section 4 provides an overall description of the Silkroad model. Section 5 presents the route optimization of Silkroad in certain scenarios. Section 6 contains the format of the messages. Section 7 is a discussion of some other issues of this solution. Section 8 and Section 9 contain a security discussion and IANA consideration.

In appendix A, we compare the mechanism to some other proposed mechanisms: Teredo[6] and an instance of Tunnel Broker concept--TSP[12].

2. Silkroad Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

This section defined other terminology used with Silkroad:

2.1 Silkroad Client (SC)

A dual stack node that has some access to the IPv4 Internet and that wants to gain access to the IPv6 Internet.

2.2 Silkroad Access Router (SAR)

A dual stack router that has access to the IPv4 Internet through a globally registered address. It will be used to help Silkroad clients to gain IPv6 connectivity.

2.3 Silkroad Navigator (SN)

A node that is used to help SARs to route between each other. The only requirement for SN is reachable for its SARs. It may be IPv4 or IPv6 addressable, which is up to the specific ISP. It is recommended for ISP whose SARs are relatively few. However, it is mandatory for ISP who has many SARs and SCs.

2.4 Silkroad UDP port

The UDP port number at which Silkroad Access Routers are waiting for packets. The value of this port is TBD. In this memo, we use port 5188 temporarily.

3. Background

3.1 What is NAT?

The need for IP address translation arises when a network's internal IP addresses can not be used outside the network either because they are invalid for use outside, or because the internal addressing must be kept private from the external network.

Network Address Translation(NAT)is a method by which IP addresses are mapped from one realm to another. It is often used to connect an isolated address realm with private unregistered addresses to an external realm with globally unique registered addresses. [1] describes the operation of NAT devices and the associated considerations in general.

Typically, NATs are not programmed to allow the transmission of arbitrary payload types. As a result, many existing tunnel techniques for IPv6 transition operation, which send IPv6 packets as payload of IPv4 packets, can not work if the user is using private IPv4 address behind a NAT box.

3.2 Types of NAT

It is assumed that the reader is familiar with NATs. It has been observed that NAT devices can adopt widely different strategies among implementations. Four treatments observed in implementations are described in [5], which are Full Cone NAT, Restricted Cone NAT, Port Restricted Cone NAT and Symmetric NAT.

Silkroad can provide IPv6 connectivity for clients located behind all these four NAT types. However, determining the type of NAT will be important when we want to optimize the transmission performance of Silkroad.

3.3 Traversal of User Datagram Protocol (UDP) Through NATs

Experience shows that TCP and UDP are the only protocols guaranteed to cross the majority of NAT devices. Although transporting IPv6 packets as the payload of TCP packets would be possible, it often result in a very poor QoS (Quality-of-Service). What's more, it is hard for applications to enforcing their own control on the transmission rate in TCP. As a result, current traversal techniques through NATs are generally based on UDP. Silkroad also transports IPv6 packets as the payload of UDP packets.

4 Silkroad Description

Silkroad communication procedures are based on assumptions on NAT treatment of UDP; such assumptions may prove invalid when new NAT devices are deployed.

Silkroad is designed to robustly enable IPv6 traffic through NATs, and the price is a reasonable amount of overhead, due to UDP encapsulation. Thus Silkroad SHOULD NOT be used except when the direct IPv6 connectivity is not locally available and the node can not use a global IPv4 address.

4.1 Silkroad Model

The typical model of Silkroad is shown in Figure 1.

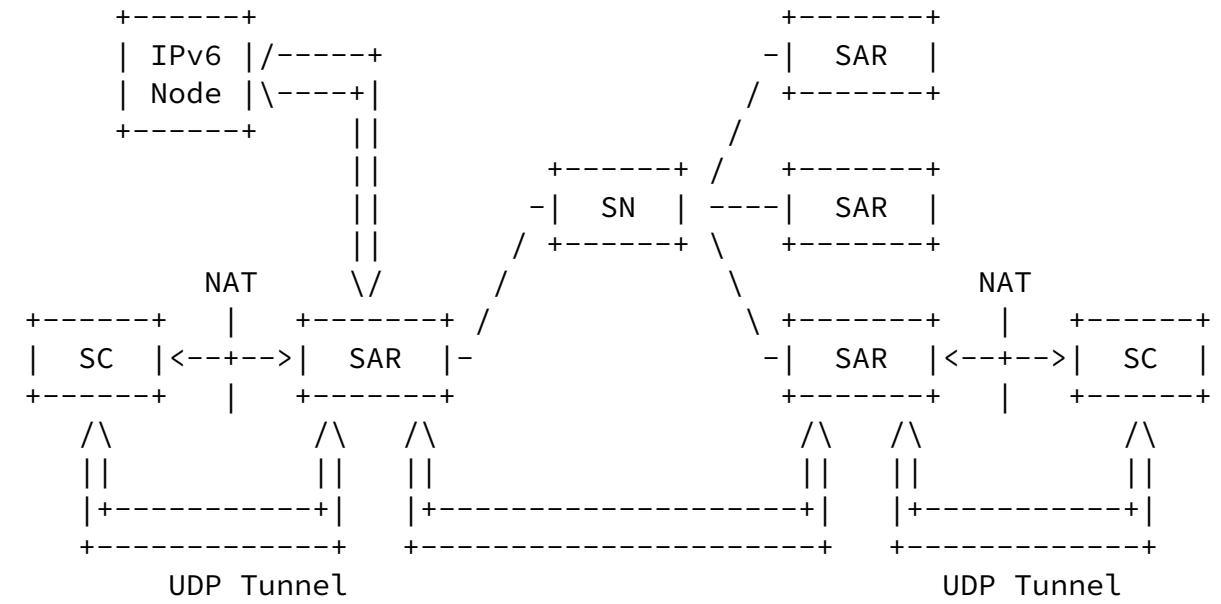


Figure 1: The Silkroad model

As can be seen from Figure 1, the Silkroad service requires the cooperation of three kinds of entities: Silkroad clients(SCs), who want to use IPv6 despite being located behind a NAT; Silkroad access routers(SARs), who provide for the interconnection between the Silkroad clients and the existing IPv6 Internet; Silkroad navigators(SNs), who will help the SAR to forward packets.

The Silkroad service is realized by having clients interact with SARs to send and receive IPv6 packets through the Silkroad service

protocol. There will be no direct interaction between SCs and SNs. For ISP whose SCs and SARs are relatively few, its SARs could configure static tunnels between each other. Under this case, SN is recommended but not mandatory. For large ISP that havs many SARs and SCs, and it is diffult or imposssible to implement N^2 trust model, it will be necessary to deploy SN to help SARs to route between each other during the packet transmission process. In this process, the role of SN is like a DNS(Domain Name System). There may be hierarchical SNs for one ISP. Each of them takes charge of a different SAR domain. The authentication and coherence for SARs and

SNs in one ISP will follow the specific ISP's security and route consideration and existing machenisms. There will be no automatic synchronization and interaction between SARs and SNs belonging to different ISPs, unless there are prior agreement. Generally, the packet forwarding between SARs belonging to different ISPs will follow IPv6 rules and no route optimization could be made.

The deployment model of Silkroad makes two assumptions:

- That all Silkroad clients and Silkroad access routers will be cognizant of the Silkroad port;

- That all Silkroad access routers will know the address of its Silkroad navigator.

4.1.1 Silkroad Client (SC)

A SC is a node that has some access to the IPv4 Internet and that wants to gain access to the IPv6 Internet despite being located behind a NAT. It mainly has the following functions:

- Manage UDP tunnel with SAR

  Create, modify or delete tunnel;
  Determining the type of NAT;
  Optimize routes;
  Send keep-alive packets;

- Security control with SAR

- Ingress filtering

- Provide transparent Silkroad support for applications

4.1.2 Silkroad Access Router (SAR)

A SAR is a dual-stack (IPv4 & IPv6) router that has access to the

IPv4 Internet through a globally routable address. It mainly has the following functions:

- Manage UDP tunnel:

Create, modify or delete tunnel;

Determining the type of NAT;
Maintain usage statistics for every active tunnel;

- IPv6 address assignment and management

- Maintain the list of recent communication peers

- Update routing cache with the help of SN

- Connect to SN to search whether one IPv6 destination is a SC serviced by another SAR; if yes, get the IPv4 address of the SAR

- Secure qualification for SC

- Forward packets in IPv6/IPv4 networks

- Access control and security control

The ISP must ensure that the SAR is capable to handle the amount of users and the traffic that goes through it.

4.1.3 Silkroad Navigator (SN)

The only requirement for SN is reachable for its SARs. It may be IPv4 or IPv6 addressable, which is up to the specific ISP. A SN mainly has the following functions:

- Manage and control SARs in its domain

- Help SARs to update their routing cache

- Help SARs to search one specific SC's SAR, and provide its address

- If having lower level SNs, manage them and help them to do address resolution

As we have mentioned above, for large ISP that has many SARs and SCs, it will be necessary to deploy SN to help SARs to route between each

other during the packet transmission process. In this process, the role of SN is like a DNS. There may be hierarchical SNs for one ISP. Each of them take charge of a different SAR domain. But at this time, it is recommended to offer native IPv6 instead of deploying too many SNs.

4.2 Silkroad Operation

4.2.1 Determining the SAR

The first phase of Silkroad operation is determining an appropriate SAR to provide Silkroad service to the SC. In other words, the SC has to learn the IPv4 address of its SAR. There are many possible ways to do this. For example, the SC could get the SAR's information from its administrator, or using DNS to look up a service name. What's more, a pre-configured or pre-determined IPv4 anycast address could also be used to find the SAR. Of course, ISP could use other unspecific methods to advertise its SARs' address or domain name. Anyway, once determined, the corresponding SAR's information will be automatically saved in the SC's configuration file. This SAR will become the SC's default SAR, unless the SC explicitly changes its configuration.

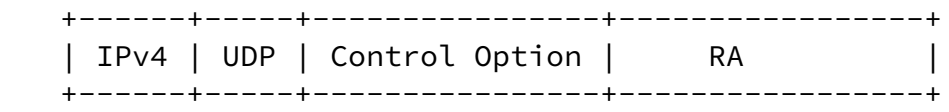
4.2.2 Obtaining IPv6 Address/prefix

In order to obtain an IPv6 address/prefix, SC sends the SAR a normal Neighbor Discovery [2] (ND) Route Solicitation (RS) or a DHCPv6 [3] SOLICIT or prefix delegation request [4] message over UDP.

The SAR replies with a normal ND Route Advertisement (RA) or a further DHCPv6 message over UDP tunnel to the SC. The default prefix length will be a /64. Whether of not providing an arbitrary length prefix is up to the specific ISP's policy and business process. The ISP may require prior agreement for special requirements.

The message replied by SAR also contains a "Control Option" domain that specifies the IPv4 address and port number from which the SAR received the prefix request. At the same time, the SAR creates a mapping between the SC's IPv6 address, and its IPv4 address and port number. In fact, when a prefix request arrives at the SAR, it may have passed through one or more NATs between the SC and the SAR. As a result, the source address of the request received by the SAR will be the mapped address created by the NAT closest to the SAR. The SAR copies that source IP address and port into the "Control Option" domain and sends it back to the source IP address and port of the request.

When the SAR replies RA, the packet will have the following format:



The IPv6 address/prefix assigned to SCs is belonging to the IPv6 addressing space managed by the SAR. SC could preserve a stable IPv6 address even though its IPv4 address is dynamic.

Similarly, SCs can also request for temporary addresses. These addresses will be assigned a lifetime and removed after its expiration unless an explicit lifetime extension request is submitted by the SC.

As mentioned above, once a SAR has assigned an IPv6 address/prefix to a SC, this SAR will make an address binding in its mapping table, in which the assigned IPv6 address/prefix is associated with the mapped IPv4 address and mapped port of the SC. Address binding MAY be dynamic with dynamic IPv4 address of SCs. In addition, the SAR will maintain the management information about this UDP tunnel.

4.2.3 Determining the Type of NAT

The previous section presented a simple address assignment procedure. When the SC receives the prefix response, it compares the IP address and port in Control Option with the local IP address and port it bound to when the request was sent. If these do not match,the SC is behind one or more NATs; otherwise, the SC need not use the Silkroad service.

For better transmission efficiency, the SC could choose to determine the type of NAT behind which it is located with the help of SAR. To determine that, the SC sends Test Requests and SAR replies with Test Response. The procedure May generally work as in [5] (Of course, the exact implementation will be flexible).

The SC would send a Test Request packet to a different SAR IPv4 address from the same source IP address and port. If the address and port in the Control Option in the response are different from those in the first response, the client knows it is behind a symmetric NAT.

To determine if it's behind a full-cone NAT, the SC can send a Test Request with flags that tell the SAR to send a response from a

different IP address and port than the request was received on. If the SC receives this response, it knows it is behind a full cone NAT.

Of course, the SC can also send a Test Request with flags that tell the SAR to send the Test Response from the same IP address the

request was received on, but with a different port. This can be used to detect whether the SC is behind a port restricted cone NAT or just a restricted cone NAT.

Once determined, the NAT type will be saved by the SC.

4.2.4 Packet Transmission from a SC to a Regular IPv6 Node

The exchange of packets between a SC and a regular IPv6 node is presented in the following figure, in which "A" is a SC located behind the NAT , "SAR1" is the SAR chosen by "A", and "B" is a regular IPv6 node.

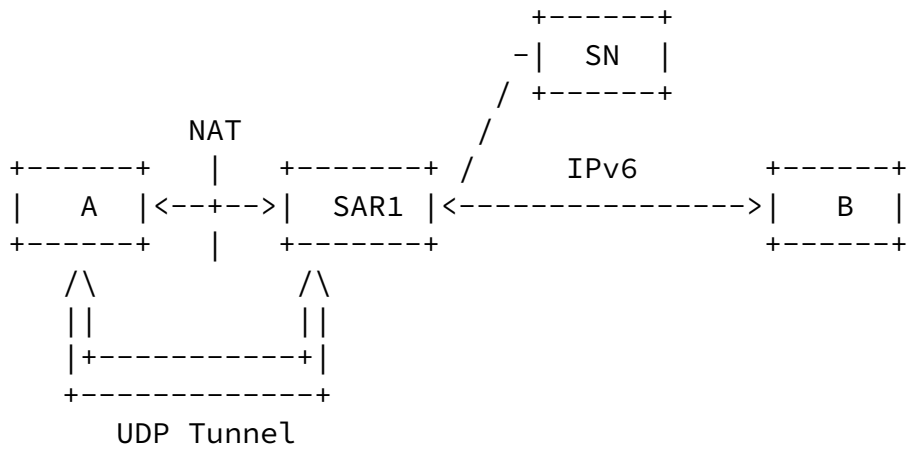
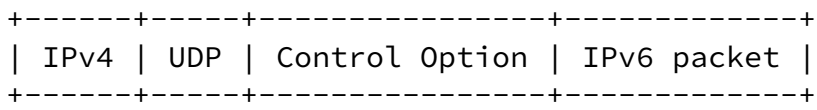


Figure 2: Packet transmission from a SC to a regular IPv6 node

We assume that A has already gotten its IPv6 address from SAR1. We also assume that the address of each entity is the following:

- A's private IPv4 address and port are: 1.0.0.1:1234
- A's mapped IPv4 address and port are: 2.0.0.2:5678
- A's IPv6 address is: 3ffe:8330:1::1234
- SAR1's IPv4 address and port are: 3.0.0.3:5188
- B's IPv6 address is: 2001:250:f006:1::5678

A wants to transmit an IPv6 packet to B. A's first action is to encapsulate this IPv6 packet in a UDP Datagram within IPv4, and send it from source address and port 1.0.0.1:1234, to the address of SAR1: 3.0.0.3:5188. We call it Silkroad packet. (The prefix response packet from SAR described in 4.2.2 and the Test Request and Test Response packets described in 4.2.3 are also Silkroad packets.) This packet will have the following format:



The packet is received by the NAT. NAT uses the existing mapping for 1.0.0.1:1234, and replaces the UDP source address and port by the mapped values 2.0.0.2:5678, before forwarding the packet.

The packet is received over IPv4 UDP tunnel by SAR1. SAR1 examines the IPv6 destination and checks if there is an entry for this IPv6 address in the list of recent communication peers, and if the entry is still valid. If there is no entry for this IPv6 destination or the entry is invalid, SAR1 will connect to its SN to search whether B is one SC serviced by another SAR. The search process is like the disposal process of DNS. The SN will search SARs' information in its own management domain. If there is no entry, it will ask its upper SN for help. The address resolution process will be restricted in one ISP's network, that means SNs belonging to different ISPs will not cooperate with each other unless there are prior agreements. In the case shown in Figure 2, the search process will be ended with the conclusion that B is not one SC in the ISP's network. Thus the SAR1 will discard the IPv4 and UDP header and Control Option domain, and forward other content of the packet over IPv6 to the address of B: 2001:250:f006:1::5678. In this way, no route optimization could be made.

If SAR1 gets the route information for B from the address resolution process with the help of SN, it will update the list of recent communication peers: if there is no entry for B in the list, add one entry for B and indicate B is a regular IPv6 node; Otherwise, set the status to valid.

4.2.5 Packet Transmission from a Regular IPv6 Node to a SC

Consider the same scenario in Figure 2. When B wants to transmit an IPv6 packet to A, B simply follows IPv6 rules. Because the IPv6 address of A is belonging to the address space of SAR1, and SAR1 is IPv6 reachable, the packet will be forwarded to SAR1 over IPv6. In this process, no route optimization could be made. SAR1 will check the address binding in its mapping table, in which it will find that the destination IPv6 address is associated with A's mapped IPv4 address and port. Thus SAR1 will forward the packet to A in UDP tunnel. At the same time, SAR1 will check the list of recent communication peers. If there is one entry for B, SAR1 will update the period of validity; otherwise, SAR1 will add one entry for B. The default period of validity will be 30 seconds. After 30 seconds, tne entry will be set invalid. Every time SAR receives packet from the peer, the period of validity for the peer will be reset to 30 seconds.

4.2.6 Exchanges Between Two Silkroad Clients

The following figure shows two SCs,"A" and "B", connected through the NATs "NAT1" and "NAT2". "SAR1" is the SAR chosen by "A" and "SAR2" is the SAR chosen by "B".

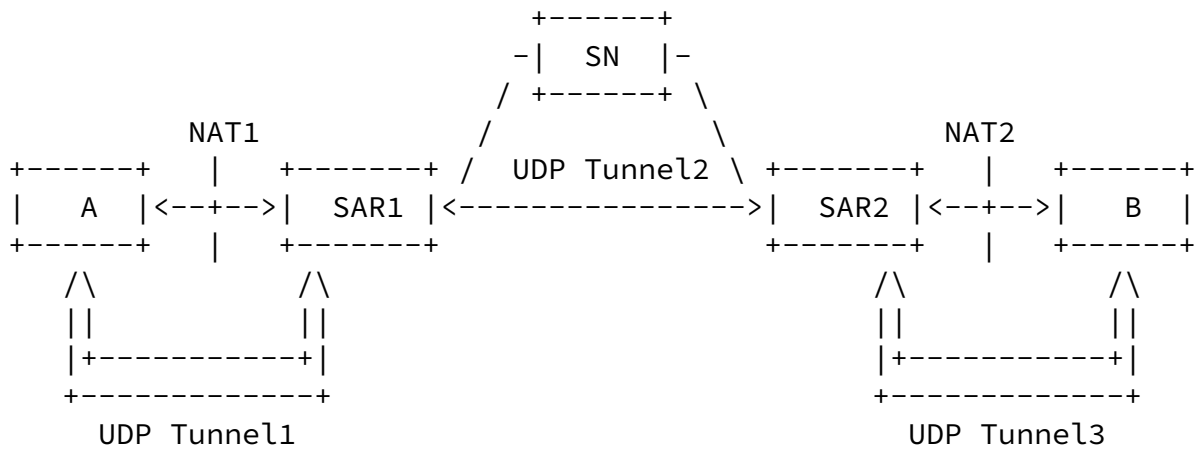


Figure 3: Packet transmission between two SCs

We assume that A and B have already gotten their IPv6 addresses from SAR1 and SAR2 respectively. In this example, we do not consider any

route optimization based on different NAT types. Route optimization will be introduced in section 5. We also assume that the address of each entity is the following:

- A's private IPv4 address and port are: 1.0.0.1:1234
- A's mapped IPv4 address and port are: 2.0.0.2:5678
- A's IPv6 address is: 3ffe:8330:1::1234
- SAR1's IPv4 address and port are: 3.0.0.3:5188
- SAR2's IPv4 address and port are: 4.0.0.4:5188
- B's private IPv4 address and port are: 5.0.0.5:1234
- B's mapped IPv4 address and port are: 6.0.0.6:5678
- B's IPv6 address is: 2001:250:f006:1::5678

A has learnt B's address, for example from the DNS, and starts communication with B. The data packets will be sent from A's IPv6 address (3ffe:8330:1::1234) to B's IPv6 address (2001:250:f006:1::5678). The transmission process from A to SAR1 is the same as explained in section 4.2.4.

SAR1 examines the IPv6 destination and will find that B is one SC serviced by SAR2. SAR1 may get the route information from the list of recent communication peers or from the address resolution process with the help of SN.

If SAR1 gets the route information for B from the address resolution process with the help of SN, it will update the list of recent communication peers: if there is no entry for B in the list, add one entry for B; Otherwise, update the entry content and set the status to valid.

After determining the address of SAR2, SAR1 will tunnel the IPv6 packet together with the Control Option to the address of SAR2: 4.0.0.4:5188. The transmission between SAR1 and SAR2 may follow different ways. It can manage IPv6 packet over another UDP tunnel, like UDP tunnel2 in Figure 3. The advantage of this method is that the disposal of SAR1 before forwarding will be simple, just replacing the UDP source address and port by the values 3.0.0.3:5188 and replacing the UDP destination address and port by the values 4.0.0.4:5188. However, the price is a reasonable amount of overhead, due to UDP encapsulation. Silkroad can also send IPv6 packets between SARs as payload of IPv4 packets just like traditional tunnels. But this method does not support Control Option and SAR1 must

unencapsulate the packet and reencapsulate it before forwarding. Anyway, the ISP can specify the transmission method between its SARs. The default disposal is that when there is Control Option in the packet, SAR will take UDP tunnel to forward it; otherwise, traditional tunnel will be used. In fact, Control Option generally only appears in the foremost several packets in one session. As a result, SARs may need to "listen" to both, UDP and IP encapsulation. But no matter what transmission method is token between SARs, SCs only need to support UDP encapsulation.

For simplification, in the following description, we assume SARs always take UDP tunnel to forward packets between each other.

When SAR2 receives the packet over IPv4 UDP tunnel2, it will find that B is a SC serviced by itself, and the address binding in its mapping table shows that the IPv6 destination address 2001:250:f006:1::5678 is associated with B's mapped IPv4 address and port: 6.0.0.6:5678. Thus SAR2 will replace the UDP source address and port by the values 4.0.0.4:5188 and replace the UDP destination address and port by the values 6.0.0.6:5678, then forward the packet in UDP tunnel3. At the same time, SAR2 will check the list of recent communication peers. If there is one entry for A, SAR2 will update the entry content; otherwise, SAR2 will add one entry for A.

NAT2 will receive this message. It will use the existing mapping to rewrite 6.0.0.6:5678 to 5.0.0.5:1234, and forward the packet to B. Then the packet will be received over IPv4 UDP tunnel3 by B.

Note that SAR1 and SAR2 may be the same SAR. In this way, UDP tunnel2 will be elided.

5 Route Optimization

For better transmission efficiency, we can do some route optimization in certain scenarios. Route optimization is optional. ISPs could decide whether to support route optimization for their Silkroad clients. Generally, route optimization will only be done between SCs belonging to the same ISP, unless there are prior agreements between different ISPs.

5.1 Exchanges Between Two Silkroad Clients

As described in 4.2.6, Figure 4 shows two SCs,"A" and "B", connected through the NATs "NAT1" and "NAT2". "SAR1" is the SAR chosen by "A" and "SAR2" is the SAR chosen by "B". As we have mentioned above, SAR1 and SAR2 may be the same SAR . In this way, UDP tunnel2 will be elided.

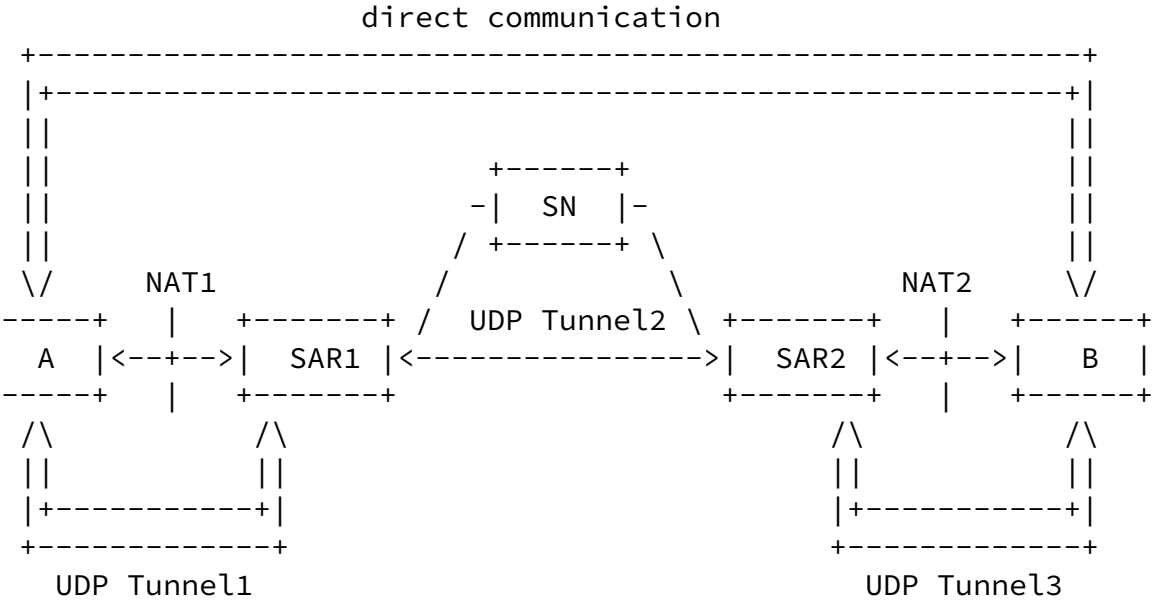


Figure 4: Exchanges between two SCs

In fact, A and B can communicate with each other directly, unless NAT1 and NAT2 are both Symmetric NAT. Of course, they need the help of SAR1 and SAR2 to exchange some parameters at first.

Assume that A wants to communicate with B. If A wants to do route optimization, A could determine the type of NAT behind which it is located with the help of SAR1 as described in 4.2.3. Then A will include its mapped address and mapped port together with its type of

NAT in the Control Option in the encapsulated packet to B. If both NAT1 and NAT2 are Full Cone NAT, B will reply IPv6 packets encapsulated in UDP directly to A, with Control Option indicating its mapped address and mapped port. Then A and B will communicate with each other directly through UDP tunnel. If both NAT1 and NAT2 are Symmetric NAT, A and B can not transmit packets to each other without

the help of SAR. In other case, A and B must generate some Test packets to establish corresponding mapping at the Restricted Cone NAT/Port Restricted Cone NAT/Symmetric NAT before they can transmit packets directly to each other. In this case, it is recommended that A and B choose to do route optimization only if they want to transmit large bulk traffic. If they only want to transmit a few of messages, there is no need to send test packets to make route optimization.

5.2 Exchanges Between Two Silkroad Clients on the Same Link

The following figure shows two Silkroad Clients, A and B, connected to the same link, which is connected to the Internet through the NAT1. The exchanges between A and B will use the SAR1. We are not making any assumption about the type of NAT1. This scenario explains how the exchanges between clients on the same link can be optimized to avoid routing all packets through SAR1 and NAT1.

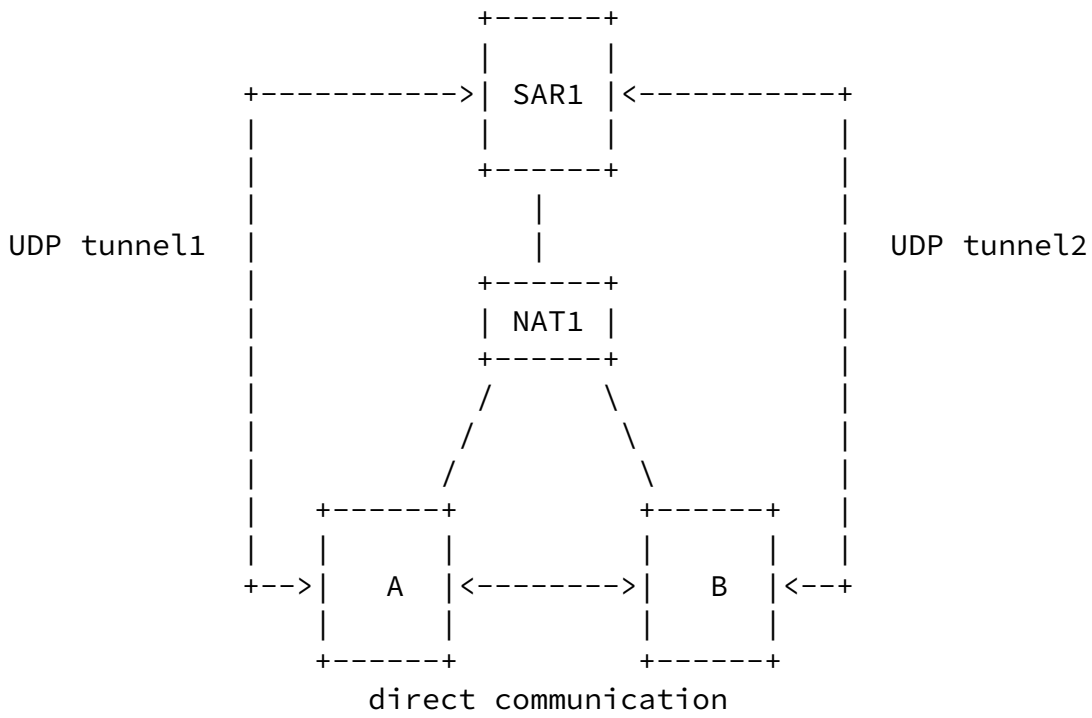


Figure 5: Packet transmission between two SCs on the same link

We assume that A and B have already gotten their IPv6 addresses from

SAR1 respectively.

Of course, A and B are possibly located behind the same NAT, if they are both using the same mapped IPv4 address. However, even if the mapped IPv4 addresses are different, they are also possibly located behind the same NAT. On the other hand, even if they are behind the same NAT, it is possible that they can not communicate with each other directly. Thus they have to take some actions to confirm that they are directly reachable.

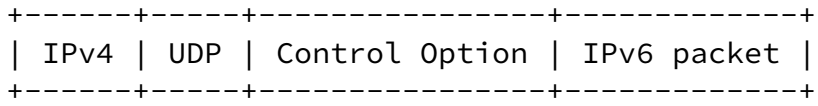
There are several ways to gain this end. Here we only give a viable alternative to implement it.

If A wants to discover whether it and B are on the same link, it can include its private address in the Control Option in the packet sent to B through NAT1 and SAR1. When B receives this packet, it will reply encapsulated packets including its private address to SAR1's address and A's private address simultaneously. If A receives both packets, it will confirm that it and B are on the same link and they are directly reachable. Then the packets will be sent directly on the local link, avoiding the loop through SAR1 and NAT1.

6 Message Formats

In this section, we will introduce Silkroad packet in details.

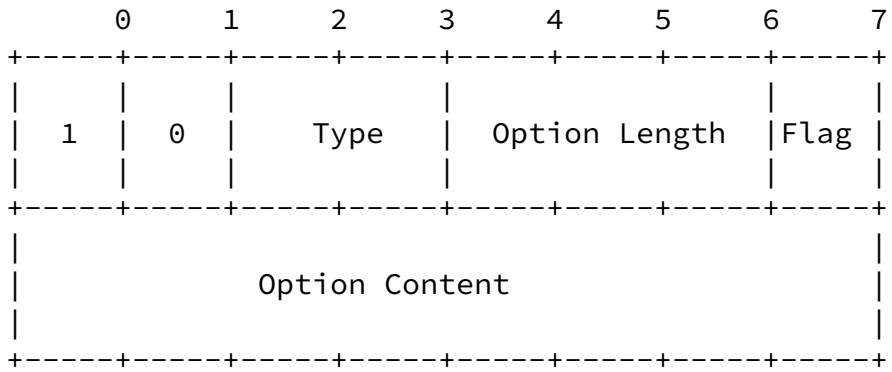
Silkroad packets are transmitted as the payload of UDP packets within IPv4. In order to control and optimize the transmission, Control Option will be inserted in the first bytes of the UDP payload:



The first bit of the Control Option is set to 1; this is used to discriminate between the Control Option and the simple IPv6 in UDP encapsulation, in which the first 4 bits of the packet contain the indication of the IPv6 protocol "0110".

The Control Option has two different formats: one for control use and one for test use.

Format 1 (control use):



Type in this format is 2 bits, which indicates the content type of this option. We have already defined 3 types as follows:

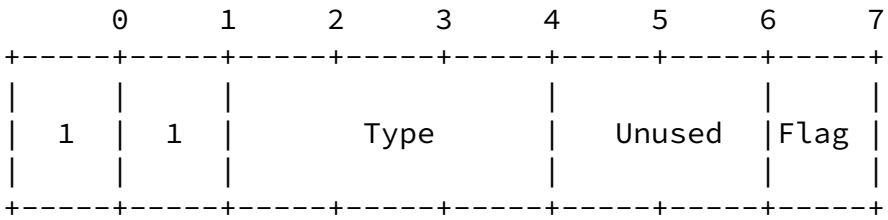
11 - Mapped address and port
10 - Private address and port
01 - Type of NAT
00 - unused

Option Length is 3 bits, which indicates the length of this option content in unit of byte.

The 1 bit Flag is used to indicate whether there are other options

following this option in this packet. It means the Control Option domain in one packet could carry more than one type of option.

Format 2 (test use):



Type in this format is 3 bits, which indicates the content type of this option. We have already defined 5 types as follows:

111 - Test request, need not reply
110 - Test request, need reply
101 - Test request, need reply from a different IP address and port than the request was received on
100 - Test request, need reply from the same IP address the request was received on, but with a different port
011 - Test response
010 - unused
001 - unused
000 - unused

(111 type packet can be used as keep-alive packet)

The 1 bit Flag is used to indicate whether there are other options following this option in this packet.

7 Other Issues of the Solution

7.1 Lifetime of NAT Mappings

Regardless of their types, NAT mappings are not kept forever.

Generally, if no traffic is observed on the specified port for a "lifetime" period, the corresponding mapping will be removed. The Silkroad client that wants to maintain a mapping open in the NAT will have to send some "keep-alive" traffic before the lifetime expires.

7.2 Lifetime of Silkroad Tunnel

As mentioned in 4.2.2, IPv6 addresses can be assigned to the SC permanently. In this way, SC could preserve a stable IPv6 address even though its IPv4 address is dynamic. Similarly, SC can also request for temporary addresses. The lifetime of these temporary IPv6 addresses should be relatively longer than the lifetime of the IPv4 connection of the SC.

In addition, there should be keep-alive mechanism on SARs. In this case, if no "refresh" traffic is observed on the assigned address for a duration that exceeds a refresh interval, the Silkroad tunnel will be canceled and the address binding will be removed or be set as unactive.

7.3 Mobility Support in Silkroad

Silkroad could support mobility in one ISP' network. Assume A is a SC, SAR1 is the home SAR chosen by A, and A has gotten its home address from SAR1. When A move to SAR2's access domain, A will register on SAR2 and get a care-of address from SAR2. If A wants to keep its IPv6 address the same. It could register its new care-of address with SAR1 and ask SAR1 to serve as home agent to deliver all the packets destined for A to A's current point of attachment. Of course, A and SAR1 must share a security association and be able to use Message Digest 5 (RFC 1321) with 128-bit keys to create unforgeable digital signatures for registration requests. The signature is computed by performing MD5's one-way hash algorithm over all the data within the registration message header and the extensions that precede the signature. To secure the registration request, each request must contain unique data so that two different registrations will in practical terms never have the same MD5 hash.

Silkroad will not consider support mobility between different ISPs, unless there are prior agreements.

8 Security Consideration

Generally, Silkroad service is limited in one ISP's scrope. The ISP should perform IPv4 ingress filtering at its borders. In particular, the ISP should block the SAR's address from being used as a source address from the outside. The ISP should perform IPv4 ingress filtering towards its customes, especially SCs, so that they will not be able to forge the IPv4 source address of the packets.

For the interaction between SN and SAR, secure SNMP could be adopted [7,8,9]. In addition, if a simpler approach based on RSH commands is used, standard IPsec mechanisms can be applied [10].

For the interaction between SC and SAR, a loss of confidentiality may occur whenever a SC disconnects from the Internet without tearing down the tunnel previously established through the SAR. As a result, the SAR will keep tunneling the IPv6 traffic addressed to that user to its old IPv4 address. However, the fact may be that this IPv4 address has already been dynamically assigned to another user. This problem could be solved by implementing on every tunnel the keep-alive mechanism as mentioned in section 7.2. In this way, the SAR will immediately stop IPv6 traffic forwarding towards disconnected users.

On the other hand, the SC must ensure that the Silkroad tunnels that it uses remain valid. It does so by checking that packets are regularly received from the SAR.

NATs make SC lose end-to-end connectivity but have more security, because a NAT can also be regarded as one type of firewall. With the help of Silkroad a SC become reachable in the IPv6 internet and be a potential goal of attackers. To ensure the security of communications, a SC can use IP security services such as AH or ESP with a global IPv6 connectivity.

As the same with Teredo, it is hard for Silkroad to find out a man-in-the-middle attacker, because the deed of a NAT is similar with that of man-in-the-middle attacker. An implementation of identification process between SC and SAR will effectly prevent man-in-the-middle attack. A way to defeat the protection is off-line dictionary attack. If the identification process is encrypted with a symmetry or asymmetry encryption system, it is quite difficult to put man-in-the-middle attack in practice.

9 IANA Considerations

This memo requests an allocation of a "privileged" UDP port (TBD).

10 Acknowledgments

The authors would like to thank Li Zhongcheng, Cai Yibing, Shi Jinglin, Tony Hain and Ma Jian for their comments, and Zhang Tianle for initial implementations.

Normative References

[1] P. Srisuresh and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC2663, Aug 1999.

[2] Narten, T., Nordmark, E. and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

[3] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C. and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[4] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633, December 2003.

Informative References

[5] J. Rosenberg, J. Weinberger, C. Huitema and R. Mahy, "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)", RFC 3489, March 2003.

[6] C. Huitema, "Teredo: Tunneling IPv6 over UDP through NATs", draft-huitema-v6ops-teredo-01.txt (Work in Progress), February 2004.

[7] B. Wijnen, D. Harrington and R. Presuhn, "An Architecture for Describing SNMP Management Frameworks", RFC 2571, April 1999.

[8] U. Blumenthal and B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", RFC 2574, April 1999.

[9] B. Wijnen, R. Presuhn and K. McCloghrie, "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)", RFC 2575, April 1999.

[10] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[11] A. Durand, P. Fasano, I. Guardini and D. Lento, "IPv6 Tunnel

---

Broker", RFC 3053, January 2001.

[12] M. Blanchet, F. Parent, "IPv6 Tunnel Broker with the Tunnel Setup Protocol (TSP)", draft-blanchet-v6ops-tunnelbroker-tsp-01(Work in Progress), June 2004.

Authors' Addresses

Min Liu
Institute of Computing Technology
Chinese Academy of Sciences
Box 2704, Beijing, 100080 PRC
Email: liumin@ict.ac.cn

Xianguo Wu
Institute of Computing Technology

Chinese Academy of Sciences
Box 2704, Beijing, 100080 PRC
Email: xgwu@ict.ac.cn

Mingye Jin
China Unicom
No.133A, Xidan North Street, Xicheng
Beijing,100032 PRC
Emailú¦jinmy@chinaunicom.com.cn

Defeng Li
HUAWEI Technologies Co., LTD.
Hua Wei Bld., No.3 Xinxi Rd.,
Shang-Di Information Industry Base,
Hai-Dian District, Beijing, 100085 PRC
Email: 77cronux.leed0621@huawei.com

Appendix A. Comparison to Other Mechanisms

A.1 Teredo

Teredo is primarily a way to make 6to4 style automation work through NATs. However, Silkroad is one way to make a managed tunnel work through NATs. They are two complementary technologies.

Teredo provides an automated IPv6 prefix as a derivative of the IPv4 address. This creates an implicit limit on the stability of the Teredo addresses, which can only remain valid as long as the underlying IPv4 address and UDP port remains valid. In addition, Teredo does not provide connectivity for clients located behind a symmetric NAT, which is common in large enterprises.

Silkroad is also a tunnel service to enable nodes located behind IPv4 NAT devices to obtain IPv6 connectivity over IPv4 UDP. However,it can provide connectivity for clients located behind all existing NAT types, including symmetric NAT. Moreover, Silkroad does not need special IPv6 addressing prefix and can provide the users with

stable IPv6 address. Of course, the route optimization May be more complicated in Silkroad than in Teredo, because there is no information about the IPv4 address and UDP port through which a Silkroad client can be reached in its IPv6 address.

A.2 Tunnel Broker Solutions

There are several proposed tunnel broker mechanisms. We'll take TSP[12] as an instance of this model. TSP is one "Tunnel Setup Protocol", which is not presented to specify any protocol for trafficing data/IPv6 payload but to provide one easy way to configure and maintain many different tunnels. From this point, TSP has relation to all existing tunnel technologies. But it is a "pure procedure" management technology for tunnels. It is different from specific tunnel technologies. The goal of Silkroad is to define a specific tunneling techique to provide IPv6 connetivity for users behind NATs. It could provide stable and managed IPv6 prefixs and route optimizations. TSP works also for tunnel configuration across ISPs. However, Silkroad service will be in one ISP's scope and communications across ISPs will follow IPv6 rules, unless there are prior agreements between ISPs. In addition, in the new version of Silkroad, SN will only help SARs to update routing cache and find the destination SAR. SN will not receive the tunnel request from SCs and will not assign SARs to provide Silkroad service. So the basic model of Silkroad is quite different from traditional tunnel broker.

Intellectual Property Statement

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

Copyright Statement