DECLARATION

I, Alexa Morris, based on my personal knowledge and information, hereby declare as follows:

1. I am Managing Director of the IETF Administration LLC and have held that position since the LLC was formed in August 2018. Prior to that, starting on January 1, 2008, I was the Executive Director of the Internet Engineering Task Force, which was an activity of the Internet Society. Since the business of IETF did not change in any materially relevant manner with the formation of the LLC, I will collectively refer to both the activity and the LLC as IETF.

2. One of my responsibilities with IETF has been to act as the custodian of Internet-Drafts and records relating to Internet-Drafts. I am familiar with the record keeping practices relating to Internet-Drafts, including the creation and maintenance of such records.

3. I hereby declare that all statements made herein are of my own knowledge and information contained in the business records of IETF and are true, and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements may be punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

4. If depositions regarding the information in this declaration are required, the deposition should be taken by phone or videoconference or, if it must be in person, should be in California.

5. Since 1998, it has been the regular practice of the IETF to publish Internet-Drafts and make them available to the public on its website at www.ietf.org (the IETF website). The IETF maintains copies of Internet-Drafts in the ordinary course of its regularly conducted activities.

6. Any Internet-Draft published on the IETF website was reasonably accessible to the public and was disseminated or otherwise available to the extent that persons interested and ordinarily skilled in the subject matter or art exercising reasonable diligence could have located it. In particular, the Internet-Drafts were indexed and searchable on the IETF website.

7. Internet-Drafts are posted to an IETF online directory. When an Internet-Draft is published, an announcement of its publication that describes the Internet-Draft is disseminated. Typically, that dated announcement is made within 24 hours of the publication of the Internet-Draft. The announcement is kept in the IETF email archive and the date is affixed automatically.

8. The records of posting the Internet-Drafts in the IETF online repository are kept in the course of the IETF's regularly conducted activity and ordinary course of business. The records are made pursuant to established procedures and are relied upon by the IETF in the performance of its functions.

9. It is the regular practice of the IETF to make and keep the records in the online repository.

10. Exhibit 1 is a true and correct copy of an announcement of the publication of draft-shin-dstm-single-ipv4-00.txt, titled "Using a Single IPv4 Global Address in DSTM." I have determined that an announcement of the publication of this Internet-Draft was made on February 23, 2001. Therefore, based on the normal practice of the IETF, that Internet-Draft was reasonably available to the public within 24 hours of that announcement. At that time, the Internet-Draft would have been disseminated or otherwise available to the extent that persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, could have located it.

Pursuant to Section 1746 of Title 28 of United States Code, I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct and that the foregoing is based upon personal knowledge and information and is believed to be true.

Date: _____ By: Alexa Morr
Alexa Morris

4892-3505-2168

INTERNET DRAFT
Myung-Ki Shin
Expires: August 2001
Yong-Jin Kim

ETRI

Alain Durand

Sun

Microsystems

February 2001

Using a Single IPv4 Global Address in DSTM
<draft-shin-dstm-single-ipv4-00.txt>

Status of this Memo

progress."

The list of current Internet-Drafts can be accessed at
http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at
http://www.ietf.org/shadow.html.

Abstract

This document specifies an enhanced dual stack mechanism used in DSTM[1] by adding a new DHCPv6 option which provides a method to assign a single IPv4 global address with TCP/UDP port range to all dual stack hosts in DSTM domain instead of dynamic IPv4 global address allocation. This enhancement to DSTM will result in a more efficient mechanism to allow IPv4/IPv6 hosts to communicate with IPv4 only hosts using a single IPv4 global address only.

Table of Contents:

1. Introduction

DSTM[1] provides a mechanism for dynamic IPv4 global address allocation to dual stack hosts and a mechanism to send packets over a network that only supports IPv6 routing. To allow a dual stack host to get an IPv4 global address, DSTM uses DHCPv6. When a dual stack host wants to talk to IPv4 only hosts, an IPv4 global address is required, so that if the number of the dual stack hosts which want to get IPv4 addresses increases at a time, a lot of IPv4 global address will be needed.

Therefore, this document specifies an enhanced dual stack mechanism used in DSTM[1] by adding a new DHCPv6 option which provides a method to assign a single IPv4 global address with

TCP/UDP port
range to all requested dual stack hosts in DSTM domain instead of
dynamic IPv4 glabal address allocation. The dual stack hosts send
packets using the same IPv4 global address and one of the assigned
TCP/UDP ports. In order to identify the returning path of packets
with the same IPv4 address, a DSTM border router MUST keep the port
state as well as the association between IPv4 and IPv6 addresses.

The proposed mechanism can increases the utilization of IPv4
address when the pool of IPv4 addresses assigned in DHCPv6 for the
purposes of dynamic allocation is exhausted. That is, it will allow
for a maximum of 63K TCP and 63K UDP sessions. This enhancement to
DSTM will result in a more efficient mechanism to allow IPv4/IPv6
hosts to communicate with IPv4 only hosts using a single IPv4
global address only.

In this document, a new protocol is not defined.

2. Overview and Example

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 RFC 2119.

In addition, this document uses the following terms defined in

DSTM[1].

DSTM Domain	See [1]
DSTM Border Router	See [1] Additionally, a border router that keeps the port state as well as the association between IPv4 and IPv6 address
DSTM Host	See [1] Additionally, a host that supports to be configured using a single IPv4 address with TCP/UDP port range
DHCPv6	See [1]
DTI	See [1]
TEP	Tunnel End Point, See [1] TEP is assumed to be a border router.

In the Figure 1, the following notations, borrowed from DSTM [1] will be used:

- X will designate an IPv6 host with a dual stack, X6 will be the IPv6 address of this host and X4 the IPv4 address
- Y will designate a DSTM border router at the

```
boundary
               between an IPv6 DSTM domain and an IPv4-only
domain.
          Z    will designate an IPv4-only host and Z4 its
address.
          ==>  means an IPv6 packet
          -->  means an IPv4 packet
          ++>  means a tunneled IPv4 packet is encapsulated
in
               an IPv6 packet
               means a DNS query or response. The path
taken by this
               packet does not matter in the examples
          "a"  means the DNS name of a host


         DHCPv6
         DNS
      X6     Y6/Y4      Z4
      |         |        |
      |. . . . . .> Z    | - X6 asks the DNS for the A RR
for "Z"
      |<. . . . . . Z4   | - the answer is Z4
      |         |        | - The application sends its first
IPv4
      |         |        |   packet which arrives to the DTI
interface
      |         |        |   (If the application is compiled
for IPv6
      |         |        |   this can be done through an
IPv4-mapped
      |         |        |   address).
      |         |        | - X6 needs an IPv4 address (first
use)
      |====>    |        | - X6 queries the DHCPv6 server
for an
      |         |        |   IPv4 address and port range
      |<====    |        | - The DHCPv6 server locates the
client
      |         |        |   and provides a single IPv4
global
      |         |        |   address with port range.
      |+++++++>|        | - The X6 sends the IPv6 packet to
the Y
```

```
      |        |------->| - Y sends the packet to the
destination Z4
      |        |        | - Y keeps the association between
address
      |        |        |   and port of X between IPv4 and
IPv6
```

Figure 1

When an IPv6 host (e.g., 2001:230::1) wants to talk to an IPv4 only node (e.g., 204.71.200.75), the following will happen :

A DNS request for AAAA/A6 will return an error. This will trigger an A request, which will return the IPv4 address of the destination (e.g., 204.71.200.75). If the IPv6 host wants to establish TCP session, it will use DHCPv6 to get a single IPv4 gloabl address and TCP port range (e.g., 129.254.254.86 and TCP port 1025 ~ 1034). Thus, the IPv4 is tunneled over IPv6 from the IPv6 host to a border router (say 2001:230:ffff::1). The packet that the dual stack hosts sends to the border router looks like this :

```
Inner Source Address      = 129.254.254.86
Inner Destination Address = 204.71.200.75
Outer Source Address      = 2001:230::1
Outer Destination Address = 2001:230:ffff::1
Source TCP port           = 1025
Destination TCP port      = 23
```

When the packet reaches the TEP, the border router decapsulates the packet to the IPv4 packet. In order to identify the returning path of packets with the same IPv4 address, a DSTM border router MUST keep the port state as well as the association between IPv4 and IPv6 addresses.

The returning traffic with Destination TCP Port 1025 from 204.71.200.75 will be recognized as belonging to the same session and will be tunneled back to IPv4-in-IPv6 packet as follows:

```
Inner Source Address      = 204.71.200.75
Inner Destination Address = 129.254.254.86
Outer Source Address      = 2001:230:ffff::1
Outer Destination Address = 2001:230::1
Source TCP port           = 23
Destination TCP port      = 1025
```

3. DHCPv6 Extension Requirements

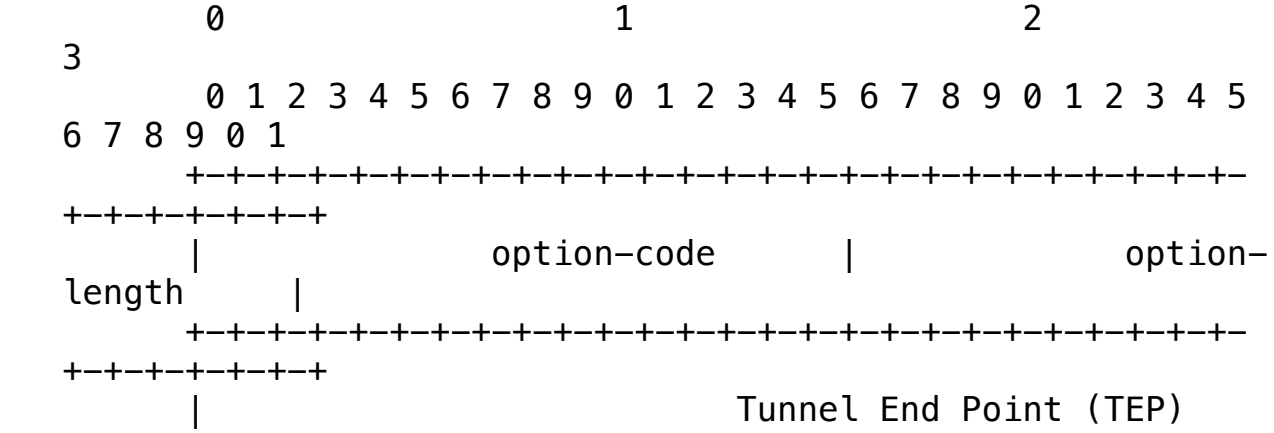
The DSTM processes will use the DHCPv6 services to communicate between the DHCPv6 Server and the DHCPv6 Client[1]. A new option is required for DHCPv6 to support a single IPv4 global address with port range in DSTM. This new DSTM option will request that the server returns an IPv4-Mapped IPv6 address and port

range to the

client.

3.1 DHCPv6 IPv4 Global Address with Port Range Option

The DHCPv6 IPv4 Address with Port Range Option informs a DHCPv6 Client or Server that the Identity Association Option (IA) [2] following this option will contain an IPv4-Mapped IPv6 Address and Port Range in the case of a DHCPv6 Client receiving the option, or is a Request for an IPv4-Mapped IPv6 Address with Port Range from a client in the case of a DHCPv6 Server receiving the option.



```
|
      |                            (If Present)
|
      |                             (16 octets)
|
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
+-+-+-+-+-+-+

      option-code:            TBD
      option-length:          Variable: 0 or 16
      Tunnel End Point:       IPv6 Address if Present
```

3.2 Client Request of IPv4 Global Address with Port Range Option

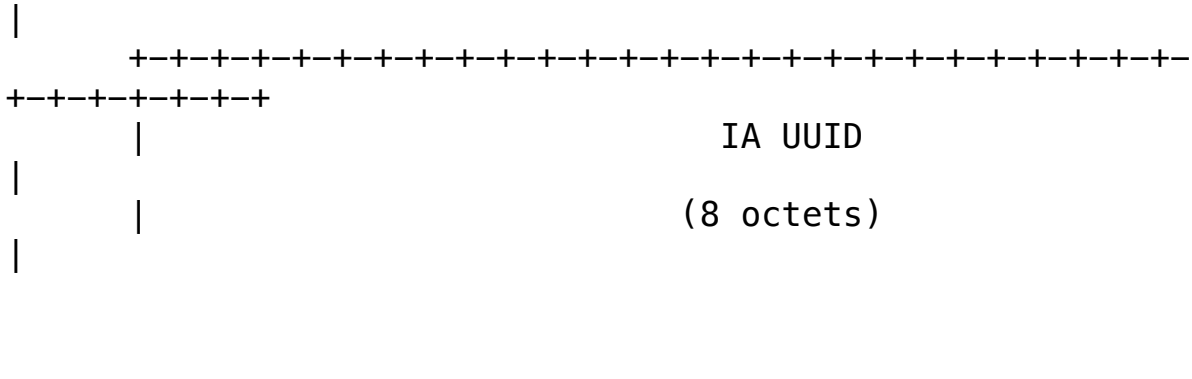
When the client requests an IPv4 address with port range from the DHCPv6 Server the TEP field MUST not be present in the IPv4 Global Address with Port Range Option.

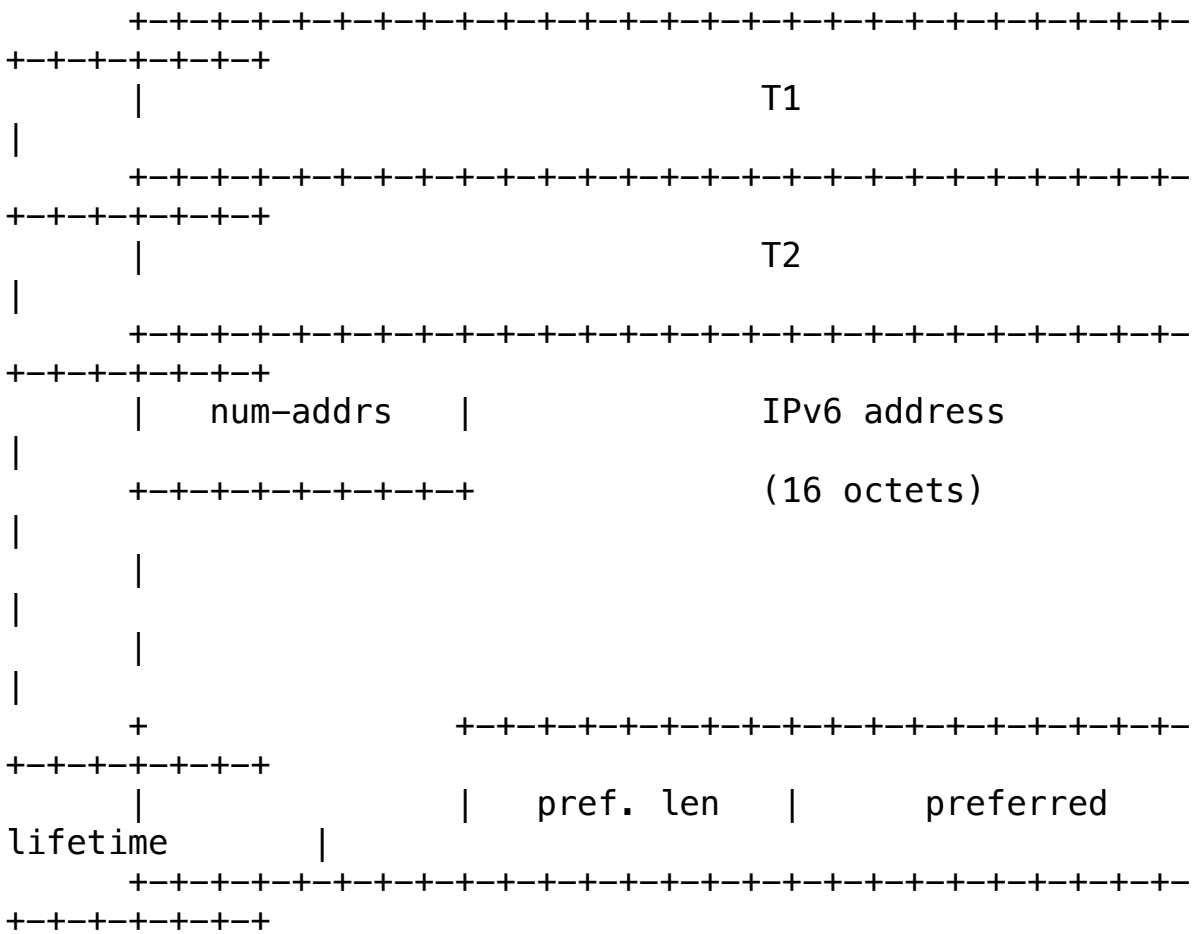
3.3 Server Reply of IPv4 Global Address with Port Range Option

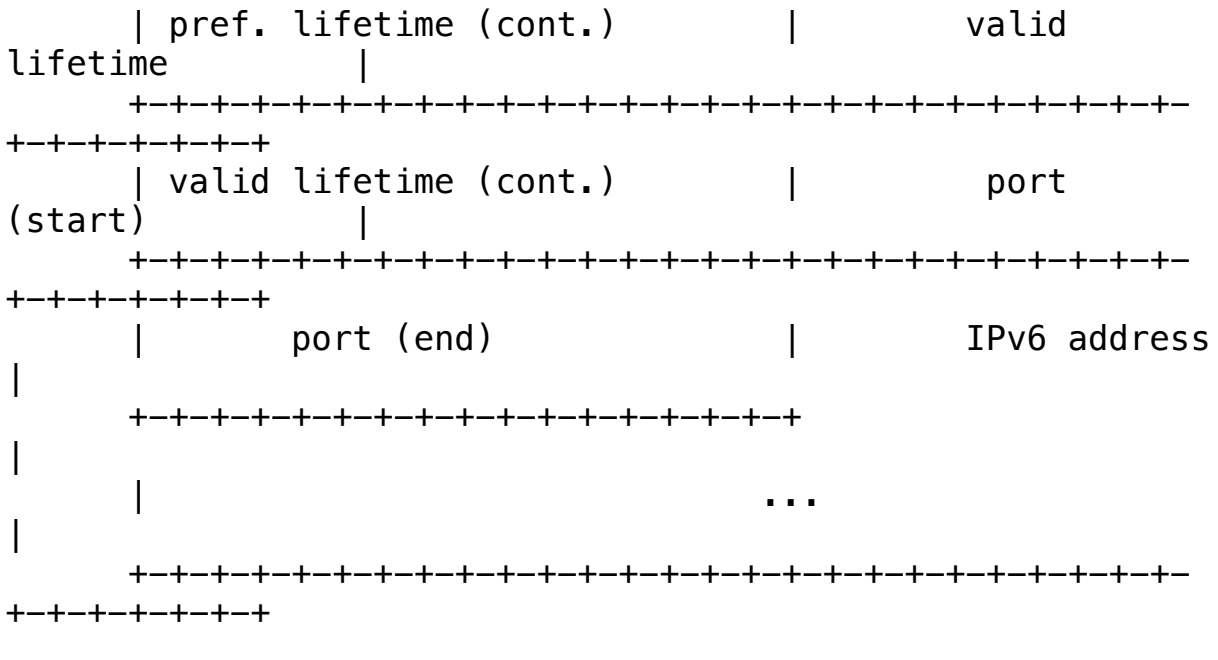
The server will reply to the client with a IPv4 Global Address with Port Range Option, that can contain an IPv6 Address Tunnel End Point, and an IA Option which MUST include an IPv4 IPv6-Mapped Address and Port Range.

The format of the IA option is:

```
       0                   1                   2
3
       0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
6 7 8 9 0 1
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
+-+-+-+-+-+-+
      |              TBD              |            variable
```







option-code
: TBD

option-len
: Variable; equal to 17 + num-addrs*25

IA UUID
: The unique identifier for this IA; chosen by the client

T1
: The time at which the client contacts the server from which the addresses in the IA were obtained to extend the lifetimes of the addresses assigned to the IA.

T2
: The time at which the client contacts any available server to extend the lifetimes of the addresses assigned to the IA.

num-addrs
: An unsigned integer giving the number of addresses carried in this IA option (MAY be zero).

IPv6 address
An IPv6 address assigned to this IA.

preferred lifetime
The preferred lifetime for the associated IPv6 address.

valid lifetime
The valid lifetime for the associated IPv6 address.

start port

The start port for the associated IPv6 address.

end port
The end port for the associated IPv6 address.

3.4 Server Processing of IPv4 Address with Port Range Option

When a DHCPv6 Server receives an IPv4 Global Address with Port Range Option in a DHCPv6 Request message, the server processing is the same as the DHCPv6 for DSTM[1] except for allocating the range of ports.

3.5 Client Processing of IPv4 Address with Port Range Option

When the Server supplies an IPv4 Global Address with Port Range in the Reply, the client processing is the same as the DHCPv6 for DSTM[1] except for acquiring the range of port.

Additional operation to configure an IPv4 IPv6-Mapped address with port range on a client is as follows:

In an implementation defined manner the Client MUST assign the port range to an interface as well as the address, instead of existing port range, supporting the Client's IPv4 stack implementation.

In an implementation defined manner the Client MUST create an entry as an IPv4-Mapped IPv6 Address with port range supporting the processing required for an IPv6 address regarding the valid and preferred lifetimes. Once the IPv4-Mapped IPv6 Address valid lifetime expires the port range MUST be deleted as well as the IPv4 address from the respective interface and a DHCPv6 Release Message MUST be sent to the DHCPv6 Server to delete the IPv4 Address and port range from the Servers bindings.

4. DSTM Border Router Requirements

In addition to the address association between IPv4 and IPv6, a border router MUST keep the port state.

5. Applicability Statement

Assuming that DSTM dose permit optionally for DSTM hosts to be configured using a single IPv4 global address and TCP/UDP port range, DSTM will result in a more efficient mechanism to allow IPv4/IPv6 hosts to communicate with IPv4 only hosts using a single IPv4 address only.

While the proposed mechanism is limited to client applications that do not insist on choosing their own source port, it can increases the utilization of IPv4 address when the pool of IPv4 addresses assigned in DHCPv6 for the purposes of dynamic allocation is exhausted. That is, it will allow for a maximum of 63K TCP and 63K UDP sessions.

With the proposed mechanism, inbound traffic (from IPv4 only hosts outside the IPv6 domain) is restricted. In this

document, we do
not consider inbound traffic. This is the same to the DSTM.

This document does not address yet the case that two hosts sharing
the same DSTM IPv4 address communicate together.

6. Security Considerations

The same as those define in DSTM [1].

References

[1] Jim Bound et al., Dual Stack Transition Mechanism (DSTM), <draft-
ietf-ngtrans-dstm-04.txt>, February 2001, Work in Progress.

[2] J. Bound, M. Carney, and C. Perkins. Dynamic Host Configuration
Protocol for IPv6, <draft-ietf-dhc-dhcpv6-16.txt>, November 2000,
Work in progress.

Authors Addresses

Myung-Ki Shin
ETRI PEC
161 Kajong-Dong, Yusong-Gu, Taejon 305-600, Korea
Tel : +82 42 860 4847
Fax : +82 42 861 5404
E-mail : mkshin@pec.etri.re.kr

Yong-Jin Kim

ETRI PEC
161 Kajong-Dong, Yusong-Gu, Taejon 305-600, Korea
Tel : +82 42 860 6564
Fax : +82 42 861 5404
E-mail : yjkim@pec.etri.re.kr

Alain Durand
Sun Microsystems
901 San Antonio Road
UMPK 17-202
Palo Alto, CA 94303-4900
Tel: +1 650 786 7503
Fax: +1 650 786 5896
Email: Alain.Durand@sun.com