Network Working Group
Internet-Draft
Expires: April 20, 2006

J. Bound
Hewlett Packard
L. Toutain
GET/ENST Bretagne
JL. Richier
IMAG

October 17, 2005

Dual Stack IPv6 Dominant Transition Mechanism (DSTM)
draft-bound-dstm-exp-04.txt

Status of this Memo

Copyright Notice

Abstract

In an IPv6 dominant environment, some applications will still require IPv4 addresses to interoperate. Dual stack may be configured on these hosts, but this will imply the configuration of network equipments (such as routers) to proceed IPv4 packets. The Dual Stack IPv6 Dominant Transition Mechanism (DSTM) is based on the use of

IPv4-over-IPv6 tunnels to carry IPv4 traffic within an IPv6 network and provides a method to allocate a temporary IPv4 address to Dual IP Layer IPv6/IPv4 capable nodes. DSTM is also a way to avoid the use of Network Address Translation for early adopter IPv6 deployment to communicate with IPv4 legacy nodes and applications.

Table of Contents

1. Introduction

In an IPv6 dominant environment, some applications will still require IPv4 addresses to interoperate. Dual stack may be configured, with a permanent IPv4 address, on these hosts, but this will imply the configuration of network equipments (such as routers) to proceed IPv4 packets. The Dual Stack IPv6 Dominant Transition Mechanism (DSTM) is used to transition dual stack network to an overlay network where IPv4 packets are sent over IPv6. DSTM is based on the use of IPv4-over-IPv6 tunnels to carry IPv4 traffic within an IPv6 network and provides a method to allocate a temporary IPv4 address to Dual IP Layer IPv6/IPv4 capable nodes. DSTM is also a way to avoid the use of Network Address Translation for early adopter IPv6 deployment to communicate with IPv4 legacy nodes and applications.

The DSTM architecture is composed of a DSTM address server, and DSTM capable nodes. The DSTM server is responsible for IPv4 address allocation to client nodes and MAY >LT : MUST ? < also provide tunnel end points (TEP) to the DSTM nodes. The DSTM server MUST guarantee the uniqueness of the IPv4 address for a period of time. The DSTM nodes will use TEPs to tunnel IPv4 packets within IPv6 to a DSTM Border router. The DSTM border router then decapsulates the IPv6 packets and transmits the IPv4 packets to the destination IPv4 node. The DSTM server controls also the creation/suppression of tunnel on the TEP.

This document describes DSTM basic behavior. DSTM is targeted to help the interoperation of IPv6 newly deployed networks with existing IPv4 networks, where the user wants to begin IPv6 adoption with an IPv6 dominant network plan, or later in the transition of IPv6, when IPv6 dominant networks will be more prevalent. In that case DSTM is used to avoid blocking situation where transition is delayed due to a lack of IPv6 porting for some applications. DSTM can also be used as an access mechanism in case an host is located on a IPv6 network. In that case the DSTM client may contact a remote DSTM server to get a temporary IPv4 address to access to remote resources.

2. Specification of Requirements

In this document, several words are used to signify the requirements of the specification. These words are often capitalized. 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].

3. Terminology

DSTM Domain:
The network areas on an Intranet where dual IPv6/IPv4 nodes use DSTM to assure IPv4 communication. An IPv4 address allocation server may be deployed inside the domain to manage an IPv4 address pool. IPv4 routing access may not be maintained within a DSTM domain.

DSTM Client:
A Dual IP Layer IPv4/IPv6 Capable Node that has implemented the DSTM client software in this specification.

DSTM Server:
A Dual IP Layer IPv4/IPv6 Capable Node that has implemented the DSTM server software in this specification.

DSTM TEP:
A Dual IP Layer IPv4/IPv6 Capable Node ensuring encapsulation/ decapsulation of tunneled packets. TEP tunnel creation/deletion is controlled by the DSTM server.

IPv6 Dominant Network:
A network that is using IPv6 as the dominant network transport for network operations.

4. DSTM Problem Statement and Assumptions

Since the IPv4 globally routable address space available is becoming a scarce resource, it is assumed that users will deploy IPv6 to reduce the need and reliability on IPv4 within a portion of their networks. Some users will require an aggressive transition to IPv6 and will begin the deployment of IPv6 reducing immediately the reliance on IPv4 wherever possible. Under this premise, supporting native IPv4 and native IPv6 simultaneously largely increases the complexity and cost of network administration (e.g. address plan, routing infrastructure). It is proposed, in this case, to define the network strategy plan to support IPv6 only use as soon as possible. Reliance on IPv4 infrastructure points like name service and address allocation for Dual IPv6/IPv4 capable nodes will move to an IPv6 strategy.

Using DSTM, DHCPv4 [RFC2131] may be used to assign IPv4 addresses to a DSTM nodes, since IPv4 routing is not maintained within an IPv6 dominant network implementation, to support DHCPv4 some IPv4 network connecvity would be required. Using DHCPv6 [RFC3315] reduces the reliance on IPv4 infrastructure for the transition to IPv6 with DSTM. But, DHCPv6 and DHCPv4 are not the only mechanisms that can be supported to allocate IPv4 addresses to a DSTM client.

DSTM is a transition mechanism that uses existing protocols. DSTM does not specify a protocol. However, DSTM defines client, server, and border router behavior and the properties of the temporary addresses allocation mechanisms.

The core assumption within DSTM is that it is completely transparent to applications, which can continue to work with IPv4 addresses. It is also transparent to the network, which carries only IPv6 packets. DSTM assumes the user, has deployed IPv6 to support end-2-end applications and security, without translation.

DSTM implementation would also support the use of IPv6 dominant networks as specified in IPv6 Enterprise Scecnarios and Analysis [RFC4057] [ENTANA]

The DSTM architecture base assumptions are as follows:

1. The DSTM domain is within an Intranet not on the Internet.
2. Dual IPv6/IPv4 nodes do not maintain IPv4 addresses except on a temporary basis, to communicate with IPv4 Applications.
3. The temporary IPv4 address allocation is done by the DSTM server, different protocols such as DHCPv6 or other mechanism can be used to assign the IPv4 address. DHCPv6 is the recommended default mechanism.
4. DSTM will keep IPv4 routing tables to a minimum and use IPv6 routing, which will reduce the network management required for IPv4 during transition within a DSTM Dominant IPv6 Network.
5. Once IPv6 nodes have obtained IPv4 addresses Dynamic Tunneling is used to encapsulate the IPv4 packet within IPv6 and then forward that packet to an IPv6 TEP DSTM border router, where the packet will be decapsulated and forwarded using IPv4. The IPv4 allocation mechanism, from the DSTM server, can provide the TEP IPv6 address to the DSTM client, in addition to manual configuration.
6. Existing IPv4 applications or nodes do not have to be modified.

Implementation defined software will have to exist to support DSTM:

1. DSTM server implementation is required to maintain configuration information about TEPs for encapsulating IPv4 packets between IPv6 nodes that can forward IPv4 packets to an IPv4 routing destination, and to maintain a pool of IPv4 addresses.
2. DSTM client implementation is required to support the dynamic tunneling mechanisms in this specification to encapsulate IPv4 packets within IPv6, and be able to communicate with the DSTM server to obtain IPv4 addresses and TEPs.
3. DSTM border router implementation is required to support the decapsulation of IPv6 packets from DSTM clients and forward them to the IPv4 destination, and cache the IPv6 address and the source IPv4 address used by the DSTM client.

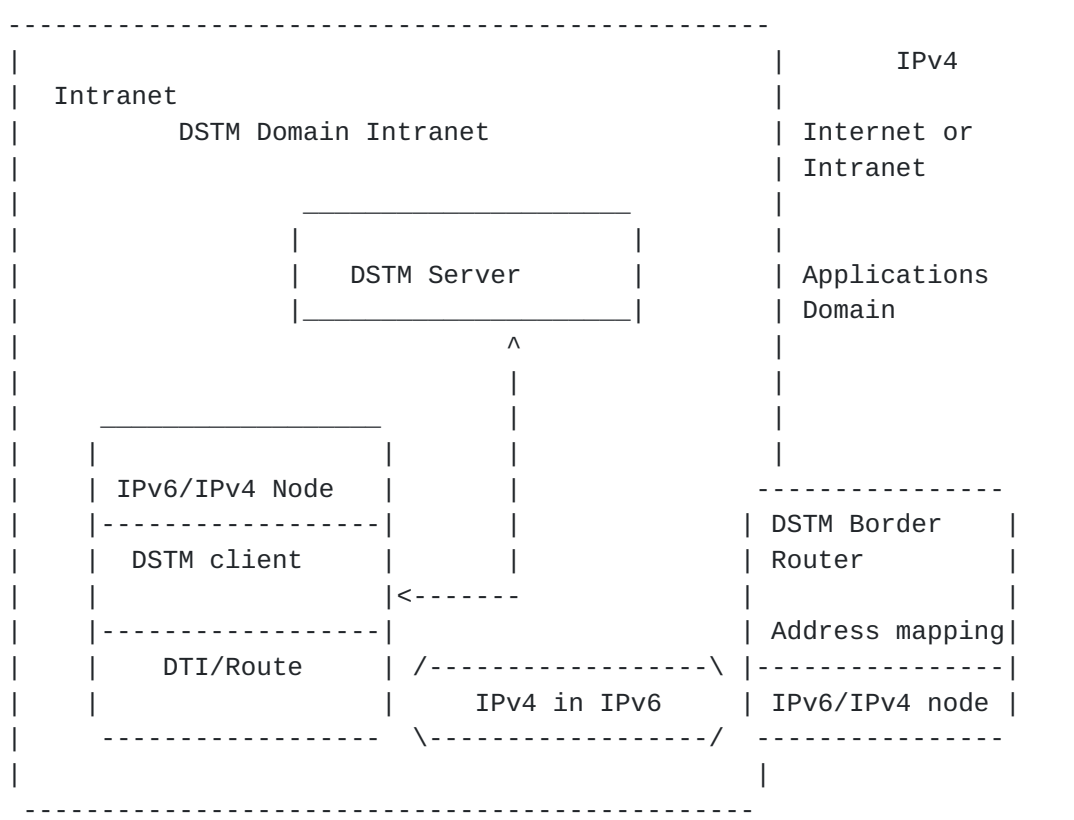

Figure 1: DSTM Architecture

5. DSTM Deployment Example

In the example below, the following notation will be used:
X will designate a dual IPv6/IPv4 node, X6 will be the IPv6 address of this node 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 node 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 node
This example describes the case where an application running on a dual IPv6/IPv4 node (X6) wants to establish a session with an IPv4 application (Z4).

The IPv4 routing table of node X is configured to send IPv4 packets

to the nodes Dynamic Tunnel Interface (DTI) interface.

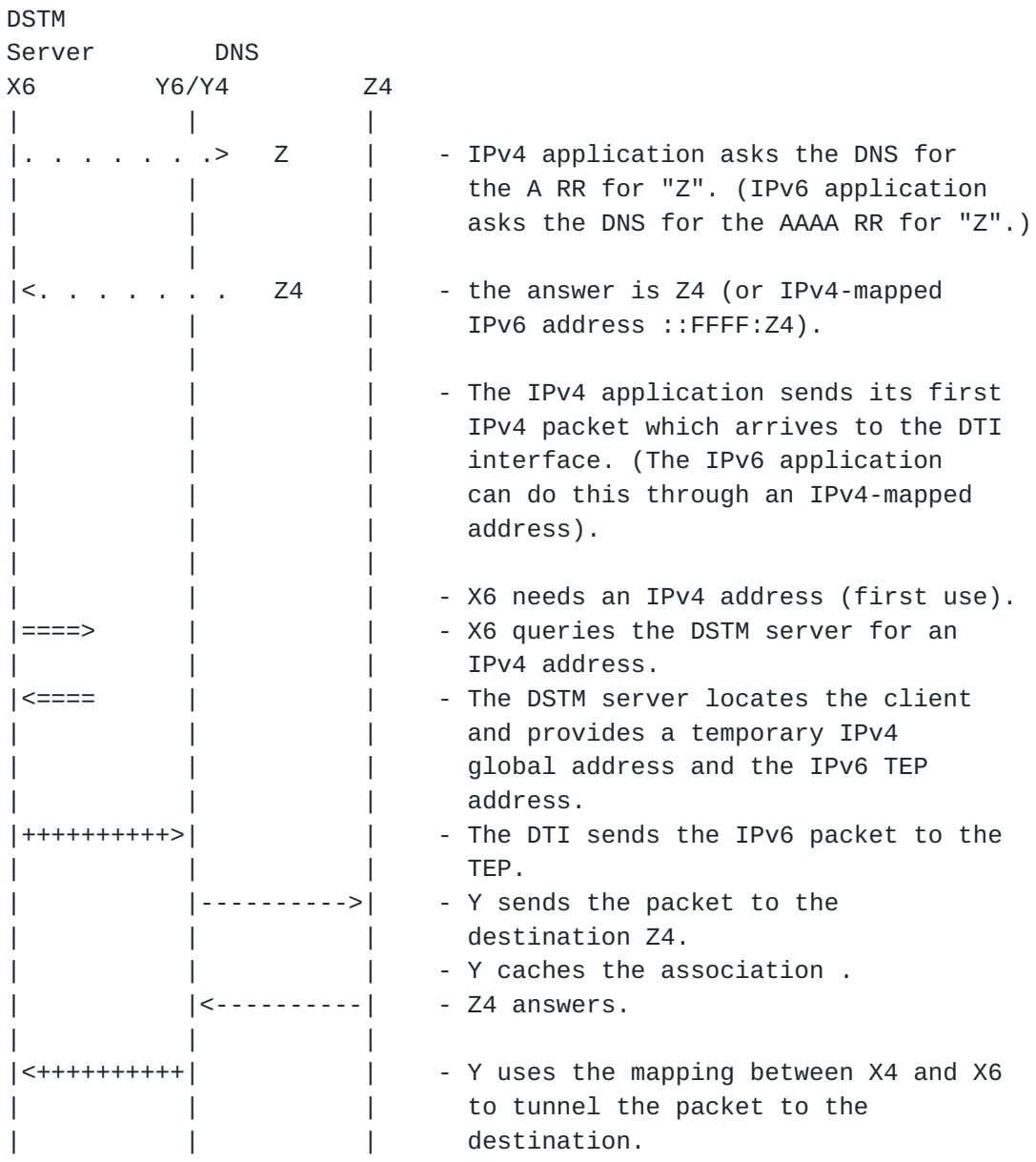

Figure 2: DSTM exchanges

When Z responds the packet returns back through Y. Y having cached the association between the IPv4 and the IPv6 address of X, is able to send the packet encapsulating the IPv4 packet within IPv6 back to X.

6. DSTM Client

A DSTM client requires the implementation of a DSTM Server Access Module and a Dynamic Tunnel Interface.

6.1 DSTM Server Access Module

A DSTM Server Access Module connects to the DSTM Server to obtain an IPv4 address and TEP. TSB/TSP [TSP] is mandatory. The client may implement other addresses allocation protocols such as DHCPv6 [RFC3315] but in case of failure MUST use TSP.

The DSTM client may also receive an expiration life time for that IPv4 address, which when expired the DSTM client cannot continue to used that IPv4 address.

The DSTM client must not perform any Dynamic updates to the DNS [RFC2136] for any IPv4 address returned to the DSTM Server Access Module.

The TEP can also be manually configured on the DSTM client.

6.2 DSTM Dynamic Tunnel Interface (DTI)

The DSTM client implementation after obtaining an IPv4 address and TEP configures its DTI to send an IPv4 packet to the IPv6 TEP of a DSTM border router, and receive IPv4 packets from an IPv6 TEP for an IPv4 application on a DSTM client.

7. DSTM Server

A DSTM server implementation requires the implementation of a DSTM Client Access Module, Address Pool Access Module, and Routing Information Access Module.

7.1 DSTM Client Access Module

The DSTM Client Access Module is required to accept requests from DSTM clients for an IPv4 address and TEPs, and then return an IPv4 address and TEPs to the DSTM client. DSTM mandates the use of a TSP as the default behavior.

7.2 DSTM Address Pool Access Module

The DSTM Address Pool Module is required to maintain a pool of IPv4 addresses for DSTM clients and maintain the lifetimes for those addresses. The lifetime for those IPv4 addresses can be provided to the DSTM client with the IPv4 address and TEPs.

7.3 DSTM Routing Information Access Module

The DSTM Routing Information Access Module is required to learn or manually configure the TEPs within the DSTM domain to provide TEPs to the DSTM clients.

8. Tunnel End Point (TEP)

The DSTM border router or TEP is required to be able to receive IPv6 packets from DSTM clients and then decapsulate the inner IPv4 packets and send to the IPv4 destination address in the IPv4 packets. The DSTM border router is required to maintain the IPv6 address of the DSTM clients that send IPv6 packets with IPv4 encapsulated, so IPv4 packets sent to the DSTM clients can be tunneled back to the DSTM client. DSTM Border router is configured by the DSTM Server.

TEP role can be played by any router without any modification. For instance CLI commands can be sent by the DSTM Server to setup and destroy dynamically tunnels.

9. Using TSP protocol between a DSTM client and Server

When using TSB/TSP, the DSTM Client contacts the server using the TCP mode of TSP, addressing the known IPv6 server address. The TCP server port should be the TSP assigned service port.

The message are formatted as described in [TSP]. The connection should be secured using SASL as described in [RFC2222].

The client sends a tunnel request of type v4v6 (cf. Figure 3). The message contains the DSTM Client IPv6 global address (the one which will be the tunnel extremity).

```
<tunnel action="create" type="v4v6">
 <client>
      <address type="ipv6"> GLOBAL_IPV6_ADDR </address>
 </client>
</tunnel>
```

Figure 3: Request sent by the client to the server

When the DTSM client wants to extend the lease, it sends the same message.

When the DTSM address is not needed anymore, the client should release the address by sending a similar message, but with action set

to "delete".

If the DSTM server accepts the client create request, it sends a response (cf. Figure 4).

```
<tunnel action="info" type="v4v6" lifetime="LIFE">
 <server>
   <address type="ipv4" length="32"> TEPV4ADDR </address>
   <address type="ipv6"> TEPV6ADDR </address>
 </server>
 <client>
  <address type="ipv4" length="32"> ASSIGNEDV4ADDR </address>
 </client>
</tunnel>
```

Figure 4: Response of the DSTM the server

- ASSIGNEDV4ADDR is the IPv4 address for the DSTM client.
- LIFE is the duration of the lease (or of the extension of the lease), in minutes.
- TEPV6ADDR is the IPv6 address of the TEP. The DSTM client and the TEP should create a point to point IPv4 on IPv6 tunnel between GLOBAL_IPV6_ADDR and TEPV6ADDR.
- TEPV4ADDR is an IPv4 address of the TEP. If the client uses a pseudo IPv4 interface for the IPv4 on IPv6 tunnel, TEPV4ADDR may be used as the remote IPv4 address for the point to point interface (in the case unnumbered interface are not possible). Also TEPV4ADDR can be used by the DSTM client as the default IPv4 address.
Both TEPV4ADDR and ASSIGNEDV4ADDR are host addresses, with a prefix length of 32.

When receiving this response, the client should accept it by sending the message (cf. Figure 5):

```
<tunnel action="accept"></tunnel>
```

Figure 5: acknowledgement from DSTM client

10. Applicability Statement

DSTM is applicable for use from within a DSTM Domain in which hosts need to communicate with IPv4-only hosts or through IPv4-only applications on a user Intranet or over the Internet.

The motivation of DSTM is to allow dual IP layer nodes to communicate

using global IPv4 addresses across an Intranet or Internet, where global addresses are required. However, the mechanisms used in DSTM can also be deployed using private IPv4 addresses to permit the Intranet use of DSTM where users require temporary access to IPv4 services within their Intranet.

In DSTM, a mechanism is needed to perform the address allocation process. This can be decoupled in two functions: the management of the IPv4 address pool and the communication protocol between server and clients. A number of mechanisms, like DHCPv6, can perform these functions.

The exact capacities of the DTI required by DSTM is implementation defined. Optionally, it is allowed that DSTM nodes configure manually (in a static manner) the tunnel to the TEP; but the recommendation is not to do this. The dynamic configuration of DTI as a result of the address allocation process is the right way to execute DSTM on an IPv6 Network.

DSTM also assumes that all packets returning from an IPv4 node to a DSTM node are routed through the originating DSTM TEP who maintains the association of the DSTM client's IPv4/IPv6 addresses. At this time it is beyond the scope of this proposal to permit IPv4 packets destined to a DSTM node to be forwarded through a non-originating DSTM TEP.

11. Security Considerations

The DSTM mechanism can use all of the defined security specifications for each functional part of its operation. For DNS, the DNS Security Extensions/Update can be used. Concerning address allocation, when connections are initiated by the DSTM nodes, the risk of Denial of Service attacks (DOS) based on address pool exaustion is limited since DSTM is configured in an Intranet environement. In this scenario, If DHCPv6 is deployed, the DHCPv6 Authentication Message can be used too. Also, since the TEPs are inside an Intranet, they can not be used as an open relay. Finally, for IPv4 communications on DSTM nodes, once the node has an IPv4 address, IPsec can be used since DSTM does not break secure end-to-end communications at any point. Also TSP can be used with the Transport Layer Security protocol over a VPN.

12. Acknowledgement

The authors want to thank the members of the DSTM IPv6 forun design team. A special thank to David Binet, Tim Chown, Francis Dupont, Florent Parent, Jaehwoon Lee and Myung-Ki Shin for their help and c ontributions.

13. References

13.1 Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[RFC2136] Vixie, P., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, April 1997.

[RFC2222] Myers, J., "Simple Authentication and Security Layer (SASL)", RFC 2222, October 1997.

[RFC3053] Durand, A., Fasano, P., Guardini, I., and D. Lento, "IPv6 Tunnel Broker", RFC 3053, January 2001.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

13.2 Informative References

[ENTANA] Bound, J., Pouffary, Y., Klynsma, S., Chown, T., and D. Green, "IPv6 Enterprise Network Analysis", draft-ietf-v6ops-ent-analysis-03.txt (work in progress), July 2005.

[RFC4057] Bound, J., "IPv6 Enterprise Network Scenarios", RFC 4057, June 2005.

[TSP] Blanchet, M. and F. Parent, "Tunnel Setup Protocol", draft-blanchet-v6ops-tunnelbroker-tsp-03.txt (work in progress), Mars 2006.

Authors' Addresses

Jim Bound
Hewlett Packard
ZK3-3/W20
110 Spit Brook Road
CS 17607
Nashua, NH 03062-2698
USA

Email: Jim.Bound@hp.com

Laurent Toutain
GET/ENST Bretagne
2 rue de la Chataigneraie
CS 17607
35576 Cesson-Sevigne Cedex
France

Fax: +33 2 99 12 70 30
Email: Laurent.Toutain@enst-bretagne.fr

Jean-Luc Richier
IMAG
BP 72
38 402 Saint Martin d'Heres cedex
France

Fax: +33 4 76 82 72 87
Email: Jean-Luc.Richier@imag.fr

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.