Dual Stack Transition Mechanism

<draft-bound-dstm-exp-01.txt>

Abstract

The deployment of IPv6 will require a tightly coupled use of IPv4 addresses to support the interoperation of IPv6 and IPv4 within an IPv6 dominant network. Nodes will still need to communicate with IPv4 nodes that do not have a Dual IP layer supporting both IPv4 and IPv6. The Dual IP Layer Stack Transition Mechanism (DSTM) is based on the use of IPv4-over-IPv6 tunnels to carry IPv4 traffic within an IPv6 dominant 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 .......................................................... 3
2. DSTM Terminology .................................................... 4
3. DSTM Problem Statement and Assumptions .......................... 5
4. DSTM Deployment Example ........................................... 7
5. DSTM Client ........................................................... 8
5.1 DSTM Server Access Module ...................................... 8
5.2 DSTM Dynamic Tunnel Interface (DTI) ........................... 9
6. DSTM Server ........................................................... 9
6.1 DSTM Client Access Module ...................................... 9
6.2 DSTM Address Pool Access Module ............................... 9
6.3 DSTM Routing Information Access Module ....................... 9
7. DSTM Border Router .................................................... 9
8. Applicability Statement .............................................. 10
9. Security Considerations ............................................. 10
Full Copyright Statement ............................................. 11
Acknowledgments ....................................................... 11
References ............................................................ 11
Authors Addresses .................................................... 12
1. Introduction

The deployment of IPv6 will require a tightly coupled use of IPv4 addresses to support the interoperation of IPv6 and IPv4 within an IPv6 dominant network. Nodes will still need to communicate with IPv4 nodes that do not have a Dual IP layer supporting both IPv4 and IPv6. The Dual IP Layer Stack Transition Mechanism (DSTM) is based on the use of IPv4-over-IPv6 tunnels to carry IPv4 traffic within an IPv6 dominant 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.

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.

When DSTM is deployed in a network, an IPv4 address can be allocated to a Dual IP Layer IPv6/IPv4 capable node to connect with IPv4 only capable nodes. DSTM permits dual IPv6/IPv4 nodes to communicate with IPv4 only nodes and applications, without modification to any IPv4 only node or application, or the IPv4 only application on the DSTM node. This allocation mechanism is coupled with the ability to perform IPv4-over-IPv6 tunneling of IPv4 packets inside the IPv6 dominant network.

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 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 border router MUST cache the path back to the DSTM node for the IPv4 address to tunnel the packet in IPv6 to the original DSTM node.
2. DSTM 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 Border Router               A Dual IP Layer IPv4/IPv6 Capable Node that has implemented the DSTM border router software in this specification.

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

Dynamic Tunnel Interface        This is an interface on a DSTM Client that will permit the sending of IPv4 packets within IPv6 to a DSTM Border Router, and receive IPv4 packets within IPv6 from an IPv4 node or application.
3. 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 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 [1] would not be used to assign IPv4 addresses to a DSTM Dual IP Layer IPv6/IPv4 nodes, since IPv4 routing is not maintained within an IPv6 Dominant Network implementation. Using DHCPv6 [2] reduces the reliance on IPv4 infrastructure for the transition to IPv6 with DSTM. But, DHCPv6 is not the only mechanism 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.

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.
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.

Schematic Overview of DSTM

```
+-----------------------------+  IPv4
| Intranet                   |  Internet or
| DSTM Domain Intranet       |  Applications
<p>|<strong><strong><strong><strong><strong><strong><strong><strong><strong><strong><strong><strong><strong><strong>|
| Domain                     |
|</strong></strong></strong></strong></strong></strong></strong></strong></strong></strong></strong></strong></strong></strong>|
|   DSTM Server              |
|<strong><strong><strong><strong><strong><strong><strong><strong><strong><strong><strong><strong><strong><strong>|
|</strong></strong></strong></strong></strong></strong></strong></strong></strong></strong></strong></strong></strong></strong>|
| IP/IPv4 Node               |
|<strong><strong><strong><strong><strong><strong><strong><strong><strong><strong><strong><strong><strong><strong>|
| DSTM client                |
|</strong></strong></strong></strong></strong></strong></strong></strong></strong></strong></strong></strong></strong></strong>|
| DTI/Route                  |
|____________________________|
| IPv4 in IPv6               |</p>
<table>
<thead>
<tr>
<th>____________________________</th>
</tr>
</thead>
<tbody>
<tr>
<td>-----------------------------</td>
</tr>
</tbody>
</table>
```

Internet or Application layer.
4. 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.
DSTM Client

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

A DSTM Server Access Module connects to the DSTM Server to obtain an IPv4 address and TEP. DSTM recommends the use of a DHCPv6 client implementation or using the Tunnel Setup Protocol.

The DSTM client may also receive an expiration life time for that IPv4 address, which when expired the DSTM client cannot continue to use that IPv4 address.
The DSTM client must not perform any Dynamic updates to the DNS [4] for any IPv4 address returned to the DSTM Server Access Module.

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

5.2 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.

6. DSTM Server

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

6.1 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 recommends the use of a DHCPv6 server implementation or Tunnel Broker as the DSTM Client Access Module.

6.2 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.

6.3 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.

7. DSTM Border Router

The DSTM border router 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 IPv4 address can be tunneled back to the DSTM client.

8. 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.

9. 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 exauastion 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.
Full Copyright Statement

Copyright (C) The Internet Society (2002). All Rights Reserved.

This document and translations of it may be copied and furnished to
others, and derivative works that comment on or otherwise explain it
or assist in its implementation may be prepared, copied, published
and distributed, in whole or in part, without restriction of any
kind, provided that the above copyright notice and this paragraph are
included on all such copies and derivative works. However, this
document itself may not be modified in any way, such as by removing
the copyright notice or references to the Internet Society or other
Internet organizations, except as needed for the purpose of
developing Internet standards in which case the procedures for
copyrights defined in the Internet Standards process must be
followed, or as required to translate it into languages other than
English.

The limited permissions granted above are perpetual and will not be
revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an
"AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING
TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING
BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION
HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF
MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgments

The authors would like to thank the following persons for their hard
work to build the DSTM options in DHCPv6 as follows: Ted Lemon, Ralph
Droms, Myung-Ki Shin, and Bernie Volz.

References

Normative References


Authors Addresses

Jim Bound
Hewlett Packard
ZK3-3/W20
110 Spit Brook Road
Nashua, NH 03062-2698
USA
Phone: +1 603 884 0062
EMail: Jim.Bound@hp.com

Laurent Toutain
ENST Bretagne
BP 78
35512 Cesson Sevigne Cedex, FR.
Phone: +33 2 99 12 70 26
Email: Laurent.Toutain@enst-bretagne.fr

Octavio Medina
ENST Bretagne
BP 78
35512 Cesson Sevigne Cedex, FR.
Phone: +33 2 99 12 70 23
Email: Octavio.Medina@enst-bretagne.fr

Francis Dupont
ENST Bretagne
BP 78
35 512 Cesson Sevigne Cedex, FR.
Phone: +33 2 99 12 70 33
Email: Francis.Dupont@enst-bretagne.fr

Myung-Ki Shin
ETRI PEC
161 Kajong-Dong, Yusong-Gu, Taejon 305-350, Korea
Phone: +82 42 860 4847
Fax: +82 42 861 5404
Email: mkshin@pec.etri.re.kr

Jaehwoon Lee
Dongguk University
26, 3 Pil-dong, Chung-gu, Seoul, 100-715, Korea
Phone: +82-2-22603849
Email: jaehwoon@dongguk.edu

Hee-Cheol Lee
ETRI PEC
161 Gajong-Dong, Yusong-Gu, Daejon 305-350, Korea
Phone: +82 42 860 1833
Email: hclee_shep@etri.re.kr

Eva Castro
Universidad Rey Juan Carlos
Escuela Superior de Ciencias Experimentales Tecnologia
Departamento de Informatica, Estadistica y Telematica
C/ Tulipan s/n - 28933 Mostoles - Madrid SPAIN
EMail: eva@gsyc.escet.urjc.es