

INTERNET-DRAFT
NGTRANS Working Group
Obsoletes [draft-ietf-ngtrans-dstm-06.txt](#)
Expires August 2002

Jim Bound
Compaq
Laurent Toutain
Octavio Medina
Francis Dupont
ENST Bretagne
Hossam Afifi
INT
Alain Durand
Sun Microsystems

Dual Stack Transition Mechanism (DSTM)

<[draft-ietf-ngtrans-dstm-07.txt](#)>

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in 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>.

To view the entire list of current Internet-Drafts, please check the "1id-abstracts.txt" listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), ftp.nordu.net (Europe), munnari.oz.au (Pacific Rim), ftp.ietf.org (US East Coast), or ftp.isi.edu (US West Coast).

Distribution of this memo is unlimited.

Abstract

During the initial deployment of IPv6, hosts in native IPv6 networks will need to maintain connectivity with hosts and/or applications who can only be reached through IPv4. The Dual Stack Transition Mechanism (DSTM) provides a method to assure this connectivity based on the use of IPv4-over-IPv6 tunnels and the temporal allocation of a global IPv4 address to hosts requiring such communication. This document defines the processes and architecture required for this transition mechanism.

Table of Contents:

1. Introduction	3
2. Terminology	4
2.1 IPv6 DSTM Terminology	4
2.2 Specification Language	5
3. DSTM Overview and Assumptions	5
4. DSTM Node Requirements	7
4.1 Configuration of the IPv4 stack	7
4.2 IPv4 packet forwarding	8
4.3 DSTM processing of IPv4 packets	8
4.4 IPv6 packet construction	8
5. DSTM Server Requirements	9
6. Applicability Statement	10
7. Security Considerations	10
Acknowledgments	11
Normative References	12
Informative References	12
Authors' Address	12

1. Introduction

The initial deployment of IPv6 will require a tightly coupled use of IPv4 addresses to support the interoperation of IPv6 and IPv4 within an IPv6-only 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 Stack Transition Mechanism (DSTM) is based on the use of IPv4-over-IPv6 tunnels to carry IPv4 traffic within an IPv6-only network and provides a method to allocate a temporary IPv4 Address to IPv6/IPv4 nodes.

DSTM is targeted to help the interoperation of IPv6 newly deployed networks with existing IPv4 networks. 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. Under this premise, supporting native IPv4 and native IPv6 simultaneously largely increases the complexity of network administration (address plan, routing infrastructure). It is proposed, in this case, to configure the network only for IPv6. In this specific scenario, DHCPv4[7] can not be directly used to assign IPv4 addresses to IPv6 nodes, since no IPv4 connectivity is maintained in the network.

When DSTM is deployed in a network, an IPv4 address is allocated to a dual stack node if the connexion can not be established using IPv6. This allows either IPv6 nodes to communicate with IPv4-only nodes, or IPv4-only applications to run on an IPv6 node without modification. This allocation mechanism is coupled with the ability to perform IPv4-over-IPv6 (4over6) tunnelling, hiding IPv4 packets inside the native IPv6 domain. This simplifies network management: only the IPv6 routing plan is managed inside the network.

The DSTM architecture is composed of an address server (DSTM server), a gateway and a number of nodes (DSTM nodes). The address server is in charge of IPv4 address allocation to client nodes. This allocation is very simple since there is no localization purpose in this address. The DSTM server has just to guarantee the uniqueness of the IPv4 address for a period of time. The gateway, or Tunnel End Point (TEP), can be seen as a border router between the IPv6-only domain and an IPv4 internet or intranet. This node performs encapsulation/decapsulation of packets to assure bi-directional forwarding between both networks. Finally, in order to assure IPv4 connectivity, nodes in the IPv6-only domain should be able to dynamically configure their IPv4 stack (by asking the server for a temporary address) and must be capable to establish 4over6 tunnels towards a Tunnel End Point. The exact details on how DSTM nodes communicate with the DSTM Server is out of the scope of this proposal and will be described in other documents.

This specification begins by the definition of the terminology ([section 2](#)). [Section 3](#) provides a technical overview of the DSTM methodology as a transition mechanism. In [section 4](#), the requirements for DSTM nodes is presented. [Section 5](#) describes the DSTM server requirements. Finally, [section 6](#) provides the DSTM Applicability Statement.

[2. Terminology](#)

[2.1 IPv6 DSTM Terminology](#)

DSTM Domain	The network areas on an Intranet where IPv6 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 Server	A process in charge of managing the IPv4 address space that will be allocated to DSTM Nodes.
Tunnel End Point (TEP)	Destination of IPv6 flows containing IPv4 packets.
DSTM	It assures the forwarding function between the domain and a given IPv4 network.
4over6 Tunnelling	Encapsulation of IPv4 packets over IPv6. Used for carrying IPv4 flows from one node to another in a DSTM Domain.
DSTM Client	A process on a DSTM Node who manages the temporary IPv4 address allocated by the DSTM Server.
DSTM Node	A node that implements both IPv4 and IPv6 stacks, 4over6 tunnelling and is a DSTM client. A DSTM node generates only IPv6 packets on the network.
IPv6 Protocol Terms:	See [1]

IPv6 Transition Terms: See [[6](#)]

DHCPv6 Terms: See [[2](#)]

2.2 Specification Language

In this document, several words are used to signify the requirements of the specification, in accordance with [RFC 2119](#) [4]. These words are often capitalized.

MUST	This word, or the adjective "required", means that the definition is an absolute requirement of the specification.
MUST NOT	This phrase means that the definition is an absolute prohibition of the specification.
SHOULD	This word, or the adjective "recommended", means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications must be understood and carefully weighed before choosing a different course. Unexpected results may result otherwise.
MAY	This word, or the adjective "optional", means that this item is one of an allowed set of alternatives. An implementation which does not include this option MUST be prepared to interoperate with another implementation which does include the option.

silently discard

The implementation discards the packet without further processing, and without indicating an error to the sender. The implementation SHOULD provide the capability of logging the error, including the contents of the discarded packet, and SHOULD record the event in a statistics counter.

3. DSTM Overview and Assumptions

DSTM, as discussed in the introduction, is a method that uses existing protocols. This document does not specify a new protocol. However, DSTM defines node, server and TEP behaviours as well as the properties of the temporary addresses allocation mechanism.

The motivation for DSTM is to provide IPv6 hosts a means to acquire an IPv4 address, for communications with IPv4-only hosts or through IPv4 applications.

The core assumption within this mechanism is that it is totally transparent to applications, which can continue to work with IPv4

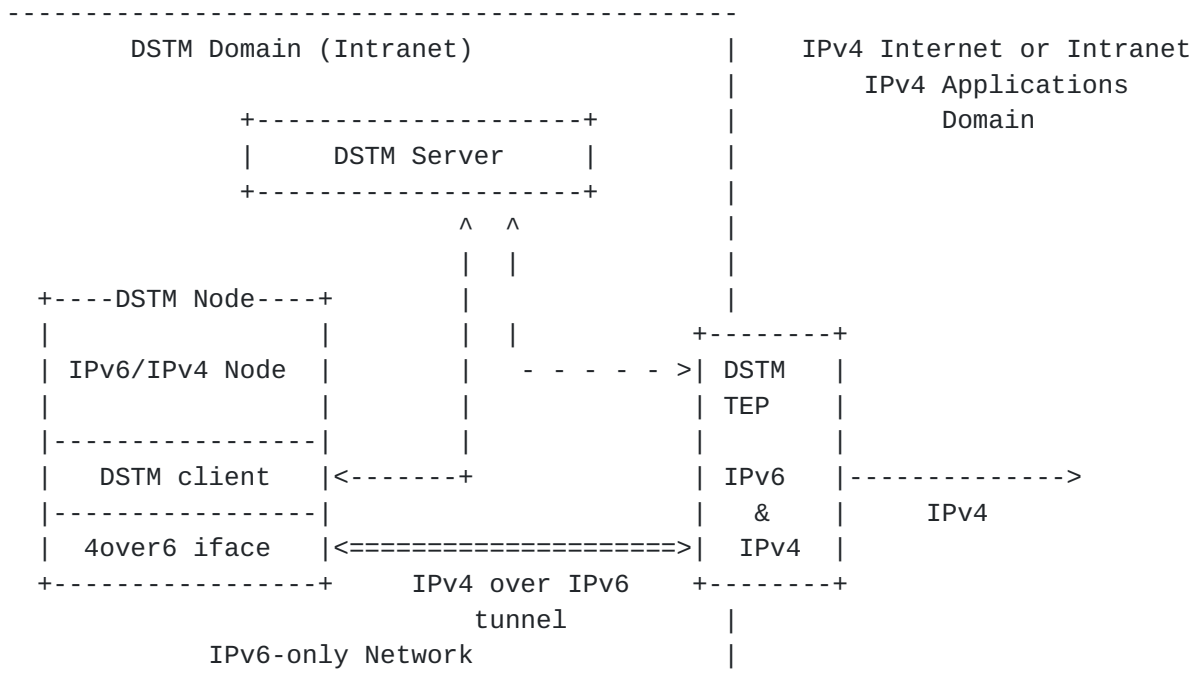
addresses. It is also transparent to the network, where only IPv6

packets are carried. It is the authors' viewpoint that the user, in this case, has deployed IPv6 to support end to end computing without translation. This aspect is fundamental during a transition process to guarantee that every existing application will continue to work (e.g. IPsec, H.323), despite the presence of IPv4 addresses in the payload of a packet.

The following assumptions describe the model used by DSTM:

- A DSTM domain is within an Intranet not on the Internet.
- IPv6 nodes do not maintain an IPv4 address except on a temporary basis, to communicate with IPv4-only nodes and/or IPv4 applications.
- The temporary IPv4 address allocation is performed by the DSTM server. Different protocols (DHCPv6 being the logical choice) can be used for the allocation process. Native IPv6 communication between server and client is one restriction in this matter.
- As an extension to the address allocation process, the DSTM server may also allow provide a range of port numbers to be used by the client. This would allow the use of the same IPv4 address by several DSTM nodes at the same time, reducing the size of the required IPv4 address pool.
- Inside a DSTM domain, IPv4 routing tables are kept to a minimum on behalf of IPv6 routing, hence, reducing the network management required for IPv4 during transition.
- Once an IPv6 node has obtained an IPv4 address (and maybe a port range), 4over6 tunnelling is used to forward packets from the node to a DSTM TEP, where the packet is decapsulated and forwarded using IPv4. As part of the address allocation process, the DSTM server SHOULD provide the client with the IPv6 address of the TEP to be used.
- Existing IPv4 applications do not need to be modified to run on DSTM nodes.
- A DSTM Node can communicate with any IPv4-only host, as long as the destination address is reachable from the TEP used by the node.

A schematic overview of DSTM is as follows:



For an IPv6 node to participate in DSTM it MUST have a dual IP layer, supporting both an IPv4 and an IPv6 stack. DSTM is not a solution for IPv6 ONLY nodes.

4. DSTM Node Requirements.

4.1 Configuration of the IPv4 stack

As long as communications can take place in native IPv6, no IPv4 address is given to the DSTM node. The host can detect the need of an IPv4 address by different methods: when a query to the DNS resolver results in an IPv4 destination address, when an application opens an IPv4 socket, or when an IPv4 packet is sent to the kernel and no interface is ready to forward that packet.

When the first IPv4 packet needs to be sent, the DSTM client MUST contact the DSTM server. This document does not specify any particular mechanism for DSTM client/server communication. Following this message exchange, the client obtains from the server a temporary IPv4 address as well as the IPv6 address of a TEP. If allowed by the implementation, the server MAY also provide the port range to be used. This information is used to configure the 4over6 interface. It is at this point that the IPv4 stack is configured.

[4.2](#) IPv4 packet forwarding

In the absence of an IPv4 routing infrastructure, a DSTM node can not directly send IPv4 packets on the network. It has to encapsulate them into IPv6 packets and send them to a Tunnel End Point (which can be seen as a particular DSTM node) that will decapsulate the packet and forward them into the IPv4 network.

On a DSTM node, this encapsulation is done by a 4over6 interface. All IPv4 traffic can be directed to that interface by an IPv4 routing table entry. The exact details of the 4over6 interface and the associated routing table entries are implementation dependant.

[4.3](#) DSTM processing of IPv4 packets

When a DSTM Node needs to send an IPv4 packet, it is sent to the 4over6 interface. If the 4over6 interface is not configured (it does not have an IPv4 address), the process SHOULD be blocked and the DSTM Server SHOULD be contacted to get a temporary address. Once an address is allocated, it is used as the IPv4 source address for all the packets leaving the interface. The other fields of the IPv4 packet are normally filled.

[4.4](#) IPv6 packet construction

When the 4over6 interface encapsulates an IPv4 packet into an IPv6 packet, it has to determine the IPv6 destination address. Usually, this will be the address of a TEP. At the node, the address of the TEP can be either statically configured or dynamically acquired when the DSTM node obtains an IPv4 address from the DSTM Server.

The IPv6 address of the TEP SHOULD be provided by the DSTM server when the DSTM node receives a temporary IPv4 address ([section 5](#)). However, a DSTM node MAY manually configure the TEP during early deployment of DSTM. This will not scale and is not recommended as a long term transition solution.

The next header type for encapsulation of IPv4 is 4 (as for IPv4 tunnelling over IPv4). When a tunnelled packet arrives to the IPv6 destination, the IPv6 header is removed and the packet is processed by the IPv4 layer. The IPv4 packet will then be forwarded by the TEP using the IPv4 infrastructure. The TEP SHOULD cache the association between the IPv4 and IPv6 source addresses.

The IPv6 source address of an encapsulated packet SHOULD be the IPv6 address of the physical interface on which the IPv6 packet will be sent.

5. DSTM Server Requirements

The DSTM server is in charge of the temporary IPv4 address allocation. This allocation is very simple since there is no localization purpose in this address. The DSTM server has just to guarantee the uniqueness of the IPv4 address for a period of time. To reduce the need of IPv4 addresses, some implementations MAY include a port range as part of the allocation process. This would allow the use of the same IPv4 address by several nodes simultaneously.

The DSTM server MUST memorize the mapping between the IPv6 address of the node requesting an address and the allocated IPv4 address. The IPv4 address is allocated by the server for a fixed amount of time. This duration MUST be included in the response. If the client needs the IPv4 address for a longer period of time, the client MUST renew the lease.

Routing in the IPv4 realm MUST ensure that the pool of IPv4 global addresses managed by a DSTM server is routed to one or more TEPs in the DSTM domain. When allocating an address to a DSTM Node, the server message SHOULD include the IPv6 address of the TEP in charge of the allocated address. Additionally, the DSTM Server MAY be in charge of configuring the IPv4/IPv6 mapping table at the TEP, if it can not be constructed dynamically or dynamic construction is disabled for security reasons.

The communication between the DSTM client and the server MUST be in IPv6. Describing the different methods that can be used to assure such communication is out of scope and will be described in other documents.

The DSTM server MAY allocate a temporary IPv4 address without a request from the client.

The DSTM server SHOULD be able to authenticate the DSTM client.

6. 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.

Bound,Toutain,Medina and al. Expires August 2002

[Page 9]

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 choice of the method to be used is out of scope and will be described in other documents.

The exact capacities of the 4over6 tunnelling interface 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 4over6 interfaces 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 node'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.

A line for future work on DSTM may include the support of multiple TEPs for returning IPv4 packets and the discovery of DSTM nodes using IPv4 DNS queries.

7. 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 [9, 10]. Concerning address allocation, when connections are initiated by the DSTM nodes, the risk of Denial of Service attacks (DOS) based on address pool exhaustion is limited since DSTM is used in an intranet environment. In this scenario, If DHCPv6 is deployed, the DHCPv6 Authentication Message can be used [2]. Also, since the TEPs are inside an intranet, they can not be used as an open relays. Finally, for IPv4 communications on DSTM nodes, once the node has an IPv4 address, IPsec [3] can be used since DSTM does not break secure end-to-end communications at any point.

Changes from draft 03 to draft 04

1. Changed DHCPv6 options and processing to comply with [draft-ietf-dhc-dhcpv6-16.txt](#)

Changes from draft 02 to draft 03

1. Working Group Edits

Changes from draft 01 to draft 02

Bound,Toutain,Medina and al. Expires August 2002

[Page 10]

1. Added further clarifications to DSTM components.
2. Added client/server details for DHCPv6 ngtrans extension.
3. Removed optional scenarios to simplify this mechanism.
4. Removed AIIH concepts and changed to be DSTM components.
5. Add Applicability Statement
6. Added acknowledgment section and new coauthors Francis Dupont and Alain Durand.

Changes from draft 00 to draft 01

1. Added text explaining why the draft does not use DHCPv4 to assign IPv4 compatible addresses to the "Introduction".
2. Defined what is mandatory and what is optional and added relative text in various places to clarify this change. And added [RFC 2119](#) adjectives to the spec where appropriate.
3. Scenario 1 where IPv6 node wants to communicate with IPv4 node is mandatory.
4. Scenarios 2 and 3 are now optional where an IPv6 node is assigned an IPv4 compatible address because an external IPv4 node is attempting communications with the IPv6 node.
5. For scenario 1 DHCPv6 is only needed for DSTM and not the tightly coupled paradigm of a co-existent DHCPv6 and DNS server. Also added mandatory and optional to the DSTM AIIH/NODE/ROUTER Diagram.
6. Made Static Tunnel Endpoints mandatory and Dynamic Tunnel End Points optional.
7. Fixed DHCPv6 Reconfigure statements to take into account changes to the Reconfigure message in the DHCPv6 working group, to support AIIH processing.

Acknowledgments

The authors would like to acknowledge the implementation contributions by Stephane Atheo at ENST Bretagne who has implemented a DSTM prototype on FreeBSD and input to this specification. We would also like to thank the NGTRANS Working Group for their input.

Normative References

- [1] S. Deering and R. Hinden. Internet Protocol, Version 6 (IPv6) Architecture", [RFC 2460](#), December 1998.
- [3] IPSEC -
S. Kent, R. Atkinson. Security Architecture for the Internet Protocol. [RFC 2401](#), November 1998.
S. Kent, R. Atkinson. IP Authentication Header.
[RFC 2402](#), November 1998.
S. Kent, R. Atkinson. IP Encapsulating Security Payload
[RFC 2406](#), November 1998.
- [4] S. Bradner. Key words for use in RFCs to indicate Requirement Levels. [RFC 2119](#), March 1997.
- [5] A. Conta and S. Deering. Generic Packet Tunneling in IPv6.
[RFC 2473](#), December 1998.
- [6] R. Gilligan and E. Nordmark. Transition Mechanisms for IPv6 Hosts and Routers. [RFC 2893](#), August 2000.
- [7] R. Droms. Dynamic Host Configuration Protocol.
[RFC 2131](#), March 1997.
- [8] Thomson, Narten. IPv6 Stateless Address Configuration.
[RFC 2462](#), December 1998.
- [9] Hinden, Deering. IP Version 6 Addressing Architecture.
[RFC 2373](#), July 1998.

Informative References

- [2] J. Bound, M. Carney, C. Perkins, and R. Droms. Dynamic Host Configuration Protocol for IPv6. [draft-ietf-dhc-dhcpv6-16.txt](#)
October 2001 (work in progress).

Authors' Address

Jim Bound
Compaq Computer Corporation
110 Spitbrook Road
Nashua, NH 003062, USA.
Email: Jim.Bound@compaq.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

Hossam Afifi
INT
91011 Evry, FR.
Phone : +33 1 60 76 40 40
Email : Hossam.Afifi@int-evry.fr

Alain Durand
Sun Microsystems
901 San Antonio Road
UMPK 17-202
Palo Alto, CA 94303-4900, USA.
Email: Alain.Durand@sun.com

