INTERNET-DRAFT
NGTRANS Tools Working Group
Obsoletes draft-ietf-ngtrans-dstm-01.txt
Expires January 2001

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

Dual Stack Transition Mechanism (DSTM)

<draft-ietf-ngtrans-dstm-02.txt>

Status of this Memo

Abstract

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 Network. Nodes will be able to be deployed with IPv6 addresses, but 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) provides a method to assign temporary Global IPv4 Addresses to IPv6 nodes, use of dynamic tunnels within an IPv6 Network to carry IPv4 traffic, and a defined set of processes and architecture for the supporting infrastructure required for this transition mechanism.

Table of Contents:

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 Network. Nodes will be able to be deployed with IPv6 addresses, but 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) provides a method to assign temporary Global IPv4 Addresses to IPv6 nodes, use of dynamic tunnels within an IPv6 Network to carry IPv4 traffic, and a defined set of processes and architecture for the supporting infrastructure required for this transition mechanism.

The DSTM assigns, when needed an IPv4 address to a dual IP layer host. This will allow either IPv6 hosts to communicate with IPv4-only hosts, or for IPv4-only applications to run without modification on an IPv6 host. This allocation mechanism is coupled with the ability to perform dynamic tunneling of an IPv4 packet inside an IPv6 packet, to suppress the exposure of IPv4 native packets within a DSTM domain of an IPv6 network. This will simplify the network management of IPv6 deployment, since routers need only IPv6 routing tables to move IPv4 packets across an IPv6 network. This means that network managers do not need to implement a routable IPv4 address plan for DSTM.

DSTM is targeted to help the interoperation of IPv6 newly deployed networks with existing IPv4 networks. DSTM assumes that a users objective in deploying an IPv6 network is to reduce the need and reliability on IPv4 within a portion of their network. In addition the IPv4 globally routable address space available to the network is a scarce resource, and the user does not want to deploy DHCPv4[16] to assign temporary IPv4 addresses to IPv6 nodes, and would rather require those nodes to use IPv6 to obtain or be given the IPv4 temporary addresses from DHCPv6. Also, to begin to reduce the IPv4 applications a user has to support to obtain a temporary IPv6 IPv4-Mapped Address (see Section 6), the client only has to run a DHCPv6 client process with the DTI mechanisms in this specification.

The DSTM architecture is composed of a DHCPv6 server, that provides for the assignment of IPv4 Global Addresses to IPv6 Hosts. The DHCPv6 server will allocate temporary IPv4 Global Addresses to IPv6 hosts. The DHCPv6 server will also be used to maintain the mapping between the allocated IPv4 address and the permanent IPv6 address of the host. Each IPv6 DSTM host will have an IPv4 interface called the Dynamic Tunneling Interface (DTI) designed to encapsulate IPv4 packets into IPv6 packets. Also a DSTM daemon exists working with a DHCPv6 client to resolve the address space mechanics, between IPv4 and IPv6.

The specification will begin by defining the terminology (section 2), then section 3 provides a technical overview of the DSTM methodology as a transition mechanism. Then in section 4 we provide a DSTM example. Section 5 describes the DTI Architecture and Section 6 discusses discusses the DHCPv6 extension requirements. Section 7 provides the DSTM Applicability Statement.

2. Terminology

2.1 IPv6 AIIH Terminology

DSTM Domain	The network areas on an Intranet where a DHCPv6 Server has access to IPv6 nodes participating in DSTM for that network.
DSTM Border Router	A border router within a DSTM domain and an IPv4-ONLY domain.
IPv6 Protocol Terms:	See [3]
IPv6 Transition Terms:	See [15]
DHCPv6 Terms:	See [4,5]
DTI:	Dynamic Tunneling Interface. An interface encapsulating IPv4 packets into IPv6 packets.
IPv4 Global Address:	An IPv4 address that is globally routable on the Internet.
Tunnel End Point (TEP)	Destination of the IPv6 packet containing an IPv4 packet. In most cases this will be a dual stack border router.

2.2 Specification Language

In this document, several words are used to signify the requirements of the specification, in accordance with RFC 2119 [9]. 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 which uses existing protocols. DSTM does not specify a protocol. However, DSTM defines a new DHCPv6 Extension for transition.

The motivation for DSTM is to provide IPv6 nodes a means to acquire an IPv4 Global Address, for communications with IPv4-only nodes or 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 which carry only IPv6 packets. 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), which embed IPv4 addresses in the payload of a packet.

The DSTM model and assumptions are as follows:

- The DSTM domain is within an Intranet not on the Internet.

- IPv6 nodes do not maintain IPv4 addresses except on a temporary basis, to communicate with IPv4-only and IPv4 Applications.

- Standard DHCPv6 is used to support the extension to provide and accept from DHCPv6 Servers Global IPv4 Addresses.

- The DSTM domain for the IPv6 nodes will keep IPv4 routing tables to a minimum and use IPv6 routing, hence, reducing the network management required for IPv4 during transition.

- 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, where the packet will be decapulated and forwarded using IPv4. DHCPv6 is used to provide TEPs to IPv6 nodes supporting DTI, as part of the new DHCPv6 Extension.

- Existing IPv4 Applications or nodes do not have to be modified to communicate with DSTM.

- Implementation defined software will have to exist to support DSTM:

  o Ability within a DHCPv6 Server implementation to maintain configuration information about TEPs for encapsulating IPv4 packets between IPv6 nodes that can forward IPv4 packets to an IPv4 routing realm, and to maintain a pool of Global IPv4

Addresses.

- o Software within an IPv6 node to support the dynamic tunneling mechanisms in this specification to encapsulate IPv4 packets within IPv6 to send IPv4 packets on an IPv6 node. In addition a daemon must exist to access a DHCPv6 client for Global IPv4 Mapped Addresses and TEPs. How this daemon communicates with a DHCPv6 Client implementation is implementation defined, and left as an exercise for implementors of this transition mechanism.

- o Software in DSTM Border Routers to recall or be able to cache the association of IPv6 and IPv4 addresses of nodes during decapsulation and encapsulation.

A simplistic overview of DSTM is as follows:

```
-----------------------------------------------
                                              |    IPv4 Internet or Intranet
        DSTM Domain Intranet                  |      IPv4 Applications
                                              |         Domain
                ______________________        |
               |                      |       |
               | DHCPv6 Server        |       |
               |______________________|       |
                             ^                |
                             |                |
   __________________        |              _|_______
  |                  |       |             |         |
  | IPv6/IPv4 Node   |       |             |  DSTM   |
  |------------------|       |             | Border  |
  |  DSTM Daemon     |       |             | Router  |
  |  DHCPv6 client   |<-------             |  IPv6   |
  |------------------|                     |   &     |
  |    DTI/Route     |<------------------->|  IPv4   |
   -------------------                      ---------
                                             |
----------------------------------------------
```

For an IPv6 host 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 Deployment Example

In the example below, the following notation 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
```

4.1 DSTM Client/Server Example

This example describes the case where an application (either compiled for the IPv6 or IPv4 API) running on an IPv6 host (X6) wants to establish a session with an IPv4 application on an IPv4-only host (Z4).

The IPv6 host is configured with the IPv6 address of a TEP, where an IPv4 encapsulated packet will be sent.

The IPv4 routing table of node X is configured to send IPv4 packets to the DTI interface.

```
         DHCPv6
         DNS
   X6          Y6/Y4          Z4
    |            |             |
    |. . . . . . . .>    Z     |    - X6 asks the DNS for an AAAA for "Z"
    |<. . . . . . . .   error  |    - the DNS answers with an error
    |. . . . . . . .>    Z     |    - X6 asks 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 using DHCPv6
    |<====       |             |    - The DHCPv6 server locates the client
    |            |             |      and provides a temporary IPv4
    |            |             |      global address.
    |++++++++++++>|            |    - The DTI sends the IPv6 packet to the
    |            |             |      TEP.
    |            |------------>|    - Y sends the packet to the destination Z4
    |            |             |    - Y caches the association between
    |            |             |      the IPv4 and IPv6 address of X.
```

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.

5 DTI Architecture

The DTI interface is responsible for encapslating IPv4 packets within IPv6 ones. IPv4 trafic can be directed to use this interface by an entry in the host IPv4 routing table. This entry MUST be configured prior to any use of the DSTM mechanism.

A conceptual model (not required) is the DTI interface is placed between the IPv4 API and the IPv6 layer, as shown in the following figure, the architectural example assumes a BSD UNIX type platform.

```
          +------------||------------+-----------||------------+--||--+
```

```
          |         IPv6 API          |         IPv4 API          | PF_  |
          |                           |                           | ROUTE|
          |                           +---------------------------+      |

          |                                                       |      |
          +-------------------------------------------------------+------+
```

On a DSTM IPv6 node a DHCPv6 client is running to manage the allocation of the IPv4 Mapped Address.

The following example gives the configuration of an IPv4 routing table with DTI.

All IPv4 packets except those to the 192.44.77/24 prefix are sent through the dti0 interface. They will be encapsulated into IPv6 packets. Packet to the 192.44.77/24 prefix will be sent natively on the link.

Routing tables

Internet:

Destination	Gateway	Flags	Refs	Use	Mtu	Netif	Expire
default	link#1	UGSc	3	0	1460	dti0	
192.44.77.0/24	192.44.77.3	UC	0	0	1500	le0	-
192.44.77.3	**8:0:2b:1c:af:15**	UHLW	4	0	1500	le0	649
127.0.0.1	**127.0.0.1**	UHl	1	102	16384	lo0	

5.1 Assignment of the IPv4 address to the DTI

When the DTI interface is activated, an IPv4 address is not given to that interface. If the interface is active, but has no IPv4 address. When it has to send the first IPv4 packet, a request is sent to the DHCPv6 client. The DHCPv6 client will send a DHCPv6 request to the DHCPv6 server to get the temporary IPv4 Mapped Address and a TEP.

An IPv6 node can know it needs an IPv4 address if the DNS resolver on the node knows that the destination address will be an IPv4 address. Once the resolver knows this then a query to the interface index of the node will inform the IPv6 node if it has an IPv4 interface configured. This is just one example of how an implementation can determine if the DSTM daemon must be called.

5.2 DTI Encapsulation of IPv4 packets

The protocol value for IPv4 encapsulation is 4 (as for IPv4 tunneling over IPv4). When a tunneled packet arrives to the IPv6 destination, the IPv6 header is removed and the packet is processed by the IPv4 layer. The DSTM Border Router SHOULD cache the association between the IPv4 and IPv6 source address. The IPv4 packet will then be forwarded by the DSTM border router using the IPv4 infrastructure.

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

5.3 DTI IPv6 destination address

When a DTI has to encapsulate an IPv4 packet into an IPv6 packet. The DTI has to determine the TEP IPv6 address for the destination. The TEP can be the host destination or, if the destination host is IPv4-only, the IPv6 address of an IPv4/IPv6 DSTM Border Router.

The TEP can be either statically configured or dynamically acquired when the IPv6 node acquires an IPv4 Compatible Address from a DHCPv6 Server.

The TEP SHOULD be provided by the DHCPv6 server when the DSTM node receives an IPv6 Mapped Address (section 6). But, a DSTM node MAY manually configure the TEP during early deployment of IPv6, but this will not scale and is not recommended as a long term transition solution.

6. DHCPv6 Requirements

The DSTM processes will use the DHCPv6 protocol and extensions to communicate between the DHCPv6 Server and the DHCPv6 Client. A new extension is required for DHCPv6 to support DSTM. But there are some additional requirements placed on the DSTM processes that are not specific to the DHCPv6 protocol as a transition and interoperation set of mechanisms for the IPv6 hosts.

6.1 DHCPv6 IPv4 Address Extension

The DHCPv6 IPv4 Address Extension informs a DHCPv6 Server or Client that the IPv6 Address Extension [5] following this extension will contain an IPv4 Mapped Address [20], or is a Request for an IPv4 Mapped Address from a client. The extension can also provide an IPv6 address to be used as the TEP to encapsulate an IPv4 packet within IPv6.

This extension can be used with the DHCPv6 Request, Reply, Release, and Reconfigure-Init Messages for cases where a DHCPv6 wants to assign clients IPv4 Mapped Addresses.

```
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |              Type             |            Length             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                          Tunnel End Point                     |
   |                           (If Present)                        |
   |                            (16 octets)                        |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

   Type:                    TBD
   Length:                  0 or 16
   Tunnel End Point:        IPv6 Address if Present
```

An IPv4 Global Address Extension MUST only apply to the extension following and not to any additional extensions in the DHCPv6 protocol.

6.1.1 Client Request of IPv4 Global Address Extension

When the client requests an IPv4 address from the DHCPv6 Server the TEP field MUST not be present, in the IPv4 Address Extension.

The IPv6 Address Extension fields as specified in [5] and depicted below
for reference MUST be filled in as follows:

```
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |           Type = 1            |             Length            |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
   |    status     |C|I|L|Q|A|P|   reserved    |scope| prefix-len  |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                         (if present)                          |
   |                    IP address (16 octets)                     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |          (if present) preferred lifetime (4 octets)           |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |            (if present) valid lifetime (4 octets)             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |         (if present) DNS name (variable length)  ...
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type   1

Length   (unsigned integer, variable) The length of the Extension in Octets.

status   zero

bits C-P not set

scope   zero

prefix-len zero

All other fields are not present.

6.1.2 Server Reply of IPv4 Global Address Extension

The server will reply to the client with an IPv4 Address Extension, that can contain an IPv6 Address Tunnel End Point.

The server will fill in the IPv6 Address Extension depicted in 6.1.1 as follows:

Type   1

Length   (unsigned integer, variable) The length of the Extension in Octets.

status   zero unless the server could not provide the address then the status will be set as defined in [5].

bits C   set
     I   not set

```
          L     set
          Q-P   not set

     scope      zero

     prefix-len zero

     IP Address  IPv4 Mapped Address
```

Preferred Lifetime	Present
Valid Lifetime	Present
DNS Name	Not Present

6.1.3 Client Processing of IPv4 Address Extension

The processing of the IPv4 Address Extension on the client is implementation defined but here are some guidelines for developers.

When processing the IPv6 Address Extension following the IPv4 Address Extension, the IP Address provided will be an IPv4 Mapped Address. A conceptual implementation model would be to add this address to the IPv6 mechanisms that maintain timing procedures for IPv6 addresses on the IPv6 stack, and then configure the IPv4 interface for DTI, as a procedure called from the DHCPv6 client.

6.2 Server Processing of an IPv4 Address Extension

When a DHCPv6 Server receives an IPv4 Address Extension it MUST assume that the next extension is a DHCPv6 Request or Release Message; the Client is either Requesting an IPv4 Global Address or Releasing an IPv4 Global Address. If an address is present in either of these messages it will be in the form of an IPv4 Mapped Address.

A DHCPv6 Server MAY send a Client a Reconfigure-Init message using the IPv4 Address Extension to ask the Client to request an IPv4 Compatible Address. The Client will recognize this by processing the IPv4 Address Extension, as an Extension Request Extension in the Reconfigure-Init message.

The Server will know a priori the IPv6 routable address, when sending a Reconfiguration-Init message, of a Client within the Intranet, and may use that address with its own IPv6 address as the transaction binding cache until the DHCPv6 Client/Server protocol processing has completed, if the server supports this optimization.

The Server will look in its implementation defined IPv4 Address configuration to determine if a TEP is available for a specific IPv6 Address Prefix. If that is the case the Server will put the address for the TEP in the IPv4 Address Extension.

6.3 Client Processing of an IPv4 Address Extension

When the Client supplies an IPv4 Global Address as a Request or Release it MUST represent that address as an IPv4 Mapped Address.

The Client MUST not assume it can use the IPv4 Address until it has received a corresponding Reply to the Client Request.

The Client MUST not update the DNS with this new address.

Once the Client is assured it can use the IPv4 Address it can perform the following operations:

1. In an implementation defined manner the Client MUST assign the address to an interface, supporting the Client's IPv4 stack implementation.

2. In an implementation defined manner the Client MUST create an entry as an IPv4 Mapped Address supporting the processing required for an IPv6 address regarding the valid and preferred lifetimes as specified in IPv6 Addrconf [19]. Once the IPv4 Mapped address valid lifetime expires the IPv4 address MUST be deleted from the respective interface and a DHCPv6 Release Message MUST be sent to the DHCPv6 Server to delete the IPv4 Address from the Servers bindings.

3. If a TEP address is provided in the IPv4 Address Extension, the Client MUST create a configured tunnel to the TEP address, in an implementation defined manner. These encapsulation mechanisms are defined in other IPv6 specifications [13, 15].

7. Applicability Statement

DSTM is applicable for use from within the DSTM Domain to IPv4 nodes or applications on a users Intranet or to access services over the Internet.

DSTM's motivation is to support dual IP layer DSTM hosts to communicate using global IPv4 addresses across an Intranet or Internet, where global addresses are required. But, DSTM has been defined to also permit the use of Private IPv4 address space to permit the Intranet use of DSTM where users require temporary access to IPv4 services within their Intranet.

DSTM requires the use of DHCPv6 to obtain IPv4 addresses and TEPs for a DSTM host. Communications between the DSTM Daemon and the DHCPv6 client is implementation defined. The DTI mechanism is also implementation defined. DSTM does permit optionally for DSTM hosts to manually configure TEPs for DTI for early deployment of DSTM but highly recommends not doing this and configuring DHCPv6 servers with this information is really the way to execute DSTM on an IPv6 Network.

DSTM also assumes that all packets returning from an IPv4 node to a DSTM dual IP layer node return through the orginating DSTM Border Router, who has cached the association of the DSTM's IPv4+IPv6 address. At this time it is beyond the scope of DSTM to permit IPv4 packets destined for DSTM hosts to return packets through a non-orginating DSTM border router.

DSTM also through the new DHCPv6 extension permits Network Operators to inform DSTM Hosts they will need IPv4 addresses for communications using the DHCPv6 Reconfigure-Init message.

DSTM in the future can be extended to support multiple border routers for returning IPv4 packets, and for the discovery of DSTM hosts using IPv4 DNS queries as future work for DSTM.

NOTE - Authors will expand this section if required after the IETF 48 meeting at the NGTRANS meeting.

8. Security Considerations

The DSTM mechanism can use all the defined security specifications for each functional part of the operation. For DNS the DNS Security Extensions/Update can be used [10, 11], for DHCPv6 the DHCPv6 Authentication Message can be used [5], and for communications between the IPv6 node, once it has an IPv4 address, and the remote IPv4 node, IPSEC [8] can be used as DSTM does not break secure end- to-end communications at any point in the mechanism.

Changes from draft 01 to draft 02

1. Added futher 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 Dyanmic 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 their input to this specification. We would also like to thank the NGTRANS Working Group for their input.

References

[1] Mockapetris, P., "Domain Names - Concepts and Facilities", STD 13, RFC 1034, USC/Information Sciences Institute, November 1987.

[2] Mockapetris, P., "Domain Names - Implementation and Specification", STD 13, RFC 1035, USC/Information Sciences Institute, November 1987.

[3] S. Deering and R. Hinden. Internet Protocol, Version 6 (IPv6) Architecture", RFC 2460, December 1998.

[4] J. Bound, M. Carney, and C. Perkins. Dynamic host Configuration Protocol for IPv6. draft-ietf-dhc-dhcpv6-15.txt May 2000 (work in progress).

[5] J. Bound, M. Carney, and C Perkins. Extensions for the Dynamic host Configuration Protocol for IPv6. draft-ietf-dhc-dhcpv6ext-12.txt May 2000. (work in progress).

[6] P. Vixie, S. Thomson, Y. Rekhter, and J. Bound. Dynamic Updates to the Domain Name System (DNS). RFC 2136, April 1997.

[7] William R. Cheswick and Steven Bellovin. Firewalls and Internet Security. Addison-Wesley, Reading, MA 1994 (ISBN: 0-201-63357-4).

[8] IPSEC - This needs to include the Arch, Auth, and ESP specs.

[9] S. Bradner. Key words for use in RFCs to indicate Requirement Levels. RFC 2119, March 1997.

[10] D. Eastlake and C. Kaufman. Domain Name System Security Extensions. RFC 2065, January 1997.

[11] D. Eastlake. Secure Domain Name System Dynamic Update.
RFC 2137, April 1997.

[12] R. Callon and D. Haskins. Routing Aspects Of IPv6 Transition
RFC 2185, September 1997.

[13] A. Conta and S. Deering. Generic Packet Tunneling in IPv6.
RFC 2473, December 1998.

[14] E. Nordmark. Stateless IP/ICMP Translator (SIIT)
draft-ietf-ngtrans-siit-03.txts, November 1998
(work in progress)

[15] R. Gilligan and E. Nordmark. Transition Mechanisms for IPv6
hosts and Routers. draft-ietf-ngtrans-trans-mech-01.txt,
August 1998 (work in progress).

[16] R. Droms. Dynamic host Configuration Protocol.
RFC 2131, March 1997.

[17] Rekhter, Moskowitz, Karrenburg, Groot. Address Allocation
for Private Networks. RFC 1918. February 1996.

[18] This needs to reflect the new DNS work for IPv6.

[19] Thomson, Narten. IPv6 Stateless Address Configuration.
RFC 2462, December 1998.

[20] Hinden, Deering. IP Version 6 Addressing Architecture.
RFC 2373, July 1998.

Authors' Address

Jim Bound
Compaq Computer Corporation
110 Spitbrook Road, ZKO3-3/W20
Nashua, NH 03062
Phone: (603) 884-0400
Email: bound@zk3.dec.com

Laurent Toutain
ENST Bretagne
BP 78
35 512 Cesson Sëvignë Cedex
Phone : +33 2 99 12 70 26
Email : Laurent.Toutain@enst-bretagne.fr

Hossam Afifi

ENST Bretagne
BP 78
35 512 Cesson Sëvignë Cedex
Phone : +33 2 99 12 70 36
Email : Hossam.Afifi@enst-bretagne.fr

Francis Dupont
ENST Bretagne
BP 78

35 512 Cesson Sëvignë Cedex
Phone : +33 2 99 12 70 36
Email : Francis.Duponti@enst-bretagne.fr

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