INTERNET-DRAFT
NGTRANS Tools Working Group
Obsoletes draft-toutain-dstm-00.txt
Expires April 2000

Jim Bound
Compaq
Laurent Toutain
Hossam Afifi
ENST Bretagne

Dual Stack Transition Mechanism (DSTM)

<draft-ietf-ngtrans-dstm-00.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 Method (DSTM) provides a set of mechanisms 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 Method (DSTM) provides a set of mechanisms 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. In the dual stack approach defined in RFC 1933, every node needs both an IPv4 and an IPv6 address to exchange information with the IPv4 and the IPv6 world. Use of the dual stack approach can be acceptable during a short period for testing IPv6 applications and initial network deployment, but does not scale since it does not solve the lack of IPv4 addresses, once IPv6 begins production deployment.

The DSTM assigns, when needed an IPv4 address to an IPv6 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 some areas 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.

DSTM is targeted to help the interoperation of IPv6 newly deployed networks with existing IPv4 networks. The main theme of DSTM is to avoid situations where the introduction of IPv6 in a network, is delayed because IPv6 will have to interoperate with IPv4 networks and applications for some time.

DSTM is composed of a DHCPv6 server coupled with a DNS server (called AIIH server, for Assignment of IPv4 Global Addresses to IPv6 Hosts). This server will allocate temporary IPv4 addresses to IPv6 hosts using DHCPv6. This server will also be used to maintain the mapping between the allocated IPv4 address and the permanent IPv6 address of the host. Every IPv6 host will have an IPv4 interface called DTI (Dynamic Tunneling Interface) designed to encapsulate IPv4 packets into IPv6 packets and 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 discuss three scenarios depicting the use of DSTM mechanisms in different configuration settings. Section 5 describes the relation between DHCPv6 and DNS

Servers, which constitutes the AIIH Server. Section 6 discusses the DTI architecture and mechanisms. Section 7 discusses the DHCPv6 extension requirements.

2. Terminology

2.1 IPv6 AIIH Terminology

DSTM Domain	The network areas on an Intranet where an AIIH Server has access to IPv6 nodes participating in DSTM for that network.
DSTM Border Router	A borderd router within a DSTM domain and an IPv4-ONLY domain (Internet or Intranet).
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.
AIIH Server:	A Server that supports DNS [2] and DHCPv6 [4,5] and communications between DNS and DHCPv6, which is implementation defined.
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.

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

DSTM as discussed in the introduction are a set of mechanisms which use existing protocols to support the operations within DSTM. DSTM does not specify a protocol, except for defining some new DHCPv6 Extensions for transition.

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

The core assumption within this mechanism is that the user does not want to use translation as a mechanism when an IPv6 node, which has also an IPv4 stack, to communicate with an IPv4-only node or an IPv4 application. It is the authors viewpoint that the user in this case, has deployed IPv6 to support end-2-end computing, without translation.

The DSTM model is 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 DNS is used to cause access to a DNS server that will know the request is an IPv4 address for an IPv6 node above.
- Standard DHCPv6 is used to support the extensions to provide and accept from DHCPv6 clients Global IPv4 Addresses.
- The network for the IPv6 nodes would like to keep IPv4 routing tables to a minimum and use IPv6 routing whenever possible, as an initial transition mechanism for IPv6.
- Once IPv6 nodes have IPv4 addresses Dynamic Tunneling is used to move the IPv4 packet within IPv6 to an IPv6 TEP, where the packet will be forwarded using IPv4. DHCPv6 is used to provide TEPs to IPv6 nodes supporting DTI.

- Implementation defined software must exist within DSTM to support the following processes:

  o Software on a DNS implementation to inform a DHCPv6 server that a request is being made for an IPv4 address for an IPv6 node. This specifications initial assumption is that

the DNS and DHCPv6 are co-located on the same node. This eliminates the need for a network protocol for DHCPv6 and DNS to communicate over a wireless or wired medium.

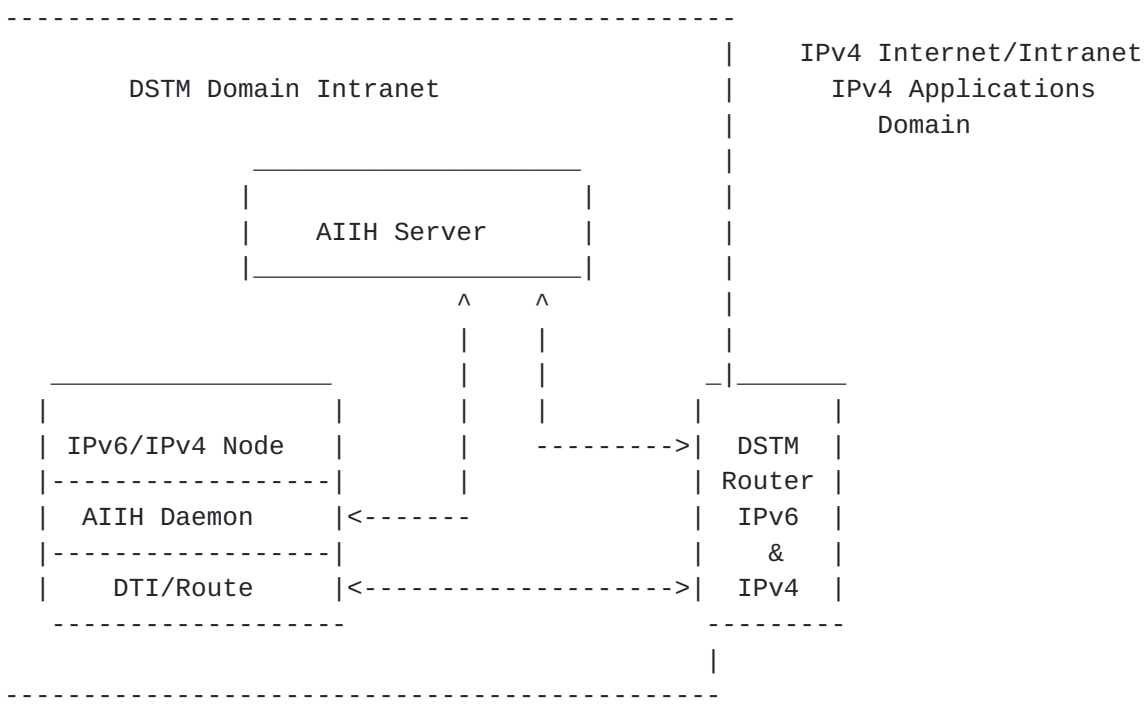
- Software on a DHCPv6 implementation to support speaking with a DNS implementation for the above purposes. In addition software within DHCPv6 to maintain configuration information about tunnel endpoints for encapsulating IPv4 packets between IPv6 nodes that can forward IPv4 packets to an IPv4 routing realm.

- The DHCPv6 and DNS processes and implementation defined parts above are collectively named the AIIH Server in this model and the specification.

- 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 an AIIH server for addresses and TEPs.

- Software in DSTM domain 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:



Both the IPv6/IPv4 node and the DSTM Router have occasion to access the

AIIH Server. For more depth please read the following sections of this specification.

For an IPv6 host to participate in the AIIH mechanism it MUST have a dual IP layer, supporting both an IPv4 and an IPv6 stack. This specification makes the assumption that for IPv6 initial deployment host nodes will not be shipped with an IPv6-only stack implementation. For embedded system type nodes that support only an IPv6 stack, AIIH cannot

be a solution.

4. Scenarios

These different scenarios illustrate interoperability problems occurring during the interoperation between IPv4 and IPv6. IPv6 end nodes have a dual stack, but only the IPv6 stack is configured through an IPv6 auto-configuration mechanisms. Intermediary routers have only an IPv6 routing table configured.

In the example below, the following notation will be used:

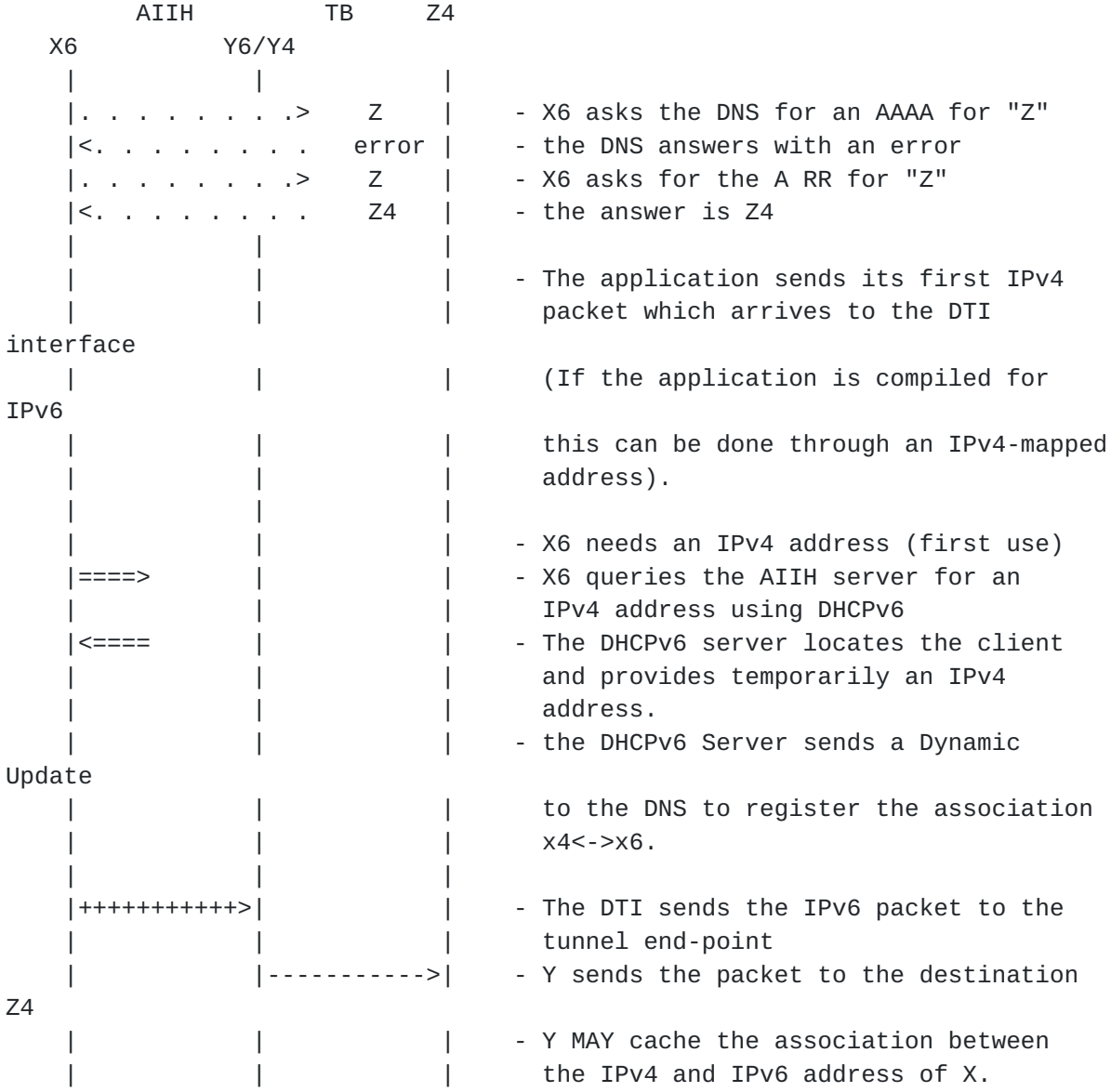
X	will designate an IPv6 host with a dual stack, X6 will be the IPv6 address of this host and X4 the IPv4 address
Y	will designate a DSTM border router at the boundary between an IPv6 DSTM domain and an IPv4-only domain.
Z	will designate an IPv4-only host and Z4 its address.
==>	means an IPv6 packet
-->	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 IPv6 node to an IPv4 node

This scenario 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 tunnel end-point, 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.



When Z answers two cases are possible either the packet comes back through Y and Y has cached the association between the IPv4 and the IPv6 address of X, or the packet arrives through another router within the

IPv6 network.

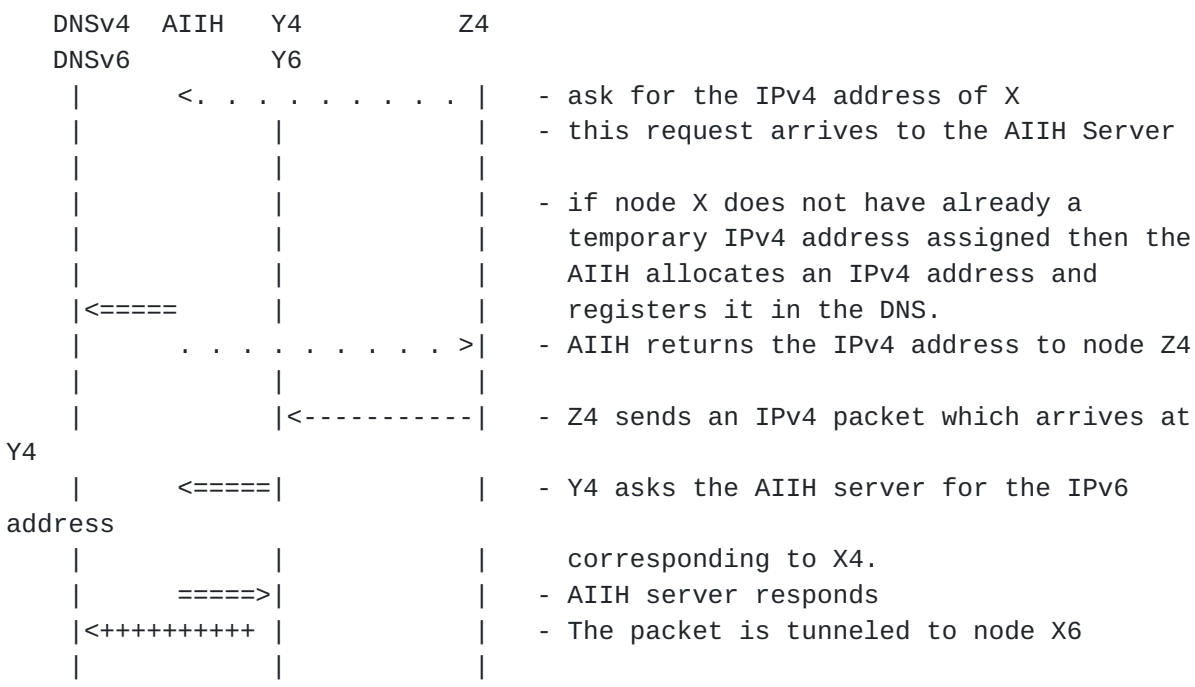
For the first case, Y simply encapsulates the IPv4 packet inside an IPv6 packet to X6. If the IPv4 packet size is greater than the MTU inside the IPv6 DSTM domain, the packet is fragmented, if the IPv4 DF bit is set to **0. Otherwise an ICMP message is sent to Z4.**

The second case corresponds to the scenario described in the next scenario, when an IPv4 packet arrives at the DSTM border router within a DSTM domain.

4.2 IPv4 node to an IPv6 node

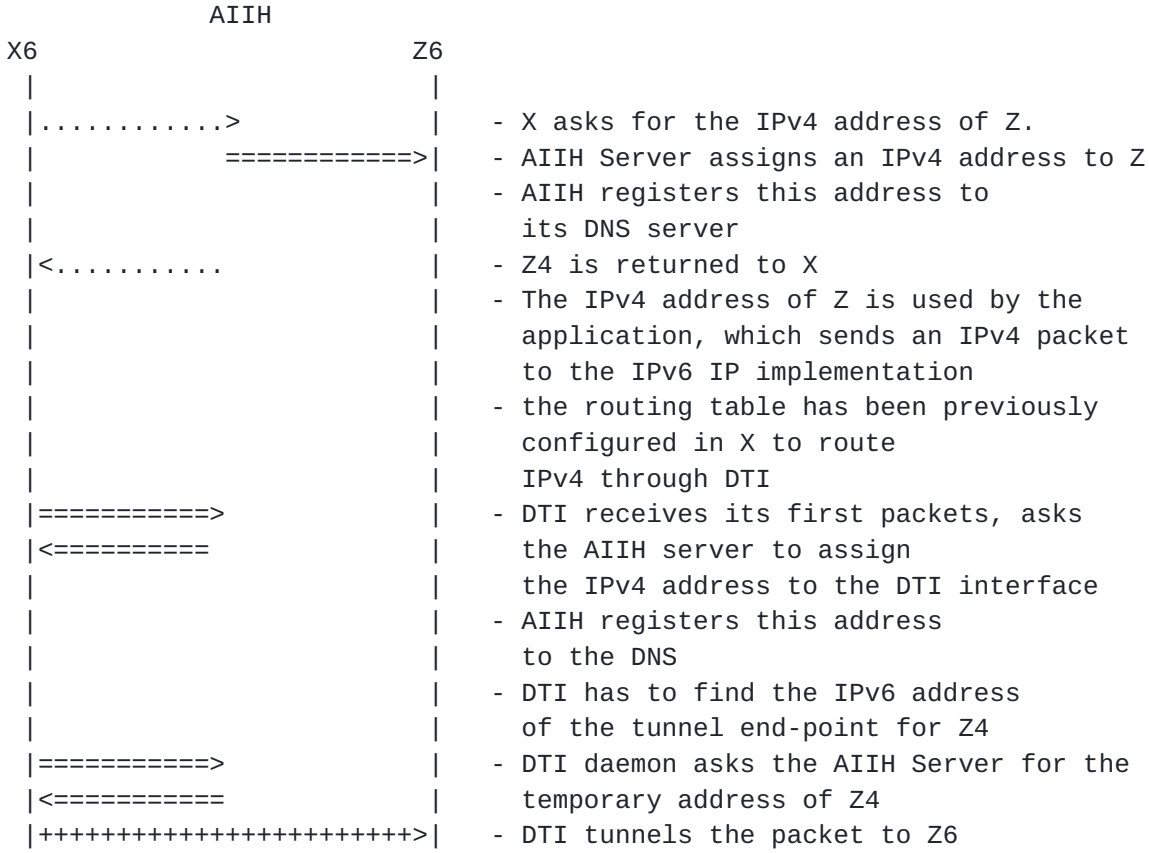
This example covers any scenario where an IPv4-only host wants to establish a session with an IPv6 host, which does not have an IPv4 address.

No modification can be made to the IPv4 host or to the application, especially the IPv4-application cannot be recompiled.



4.3 IPv4 compiled application between to IPv6 nodes

To maintain compatibility between two IPv4 applications, an IPv4 application running on an IPv6 host may wish to send IPv4 packets to another application running also on an IPv6 host, called Z6. To allow end-to-end communication without the use of a static Tunnel End Point, nodes can use the same mechanism as the DSTM border router in the previous example. This means that a DTI interface can ask the AIIH server to perform address resolution. If the resolution fails, the DTI interface can still use the static TEP.



5. AIIH Server Design Model

The design model provides two mechanisms to assign an IPv6 host an IPv4 address. The first mechanism is for the host to request an IPv4 address that is globally routable, and the second is for an AIIH Server to assign an IPv6 host a globally routable IPv4 address using the DHCPv6 Reconfigure Message. The assumption in this specification is that a site has a certain number of IPv4 Global Addresses, which can be assigned within the network on a temporary basis for use by hosts in the site.

5.1 AIIH DHCPv6/DNS Server

The AIIH Server supports a co-located DHCPv6 and DNS Server and other

implementation defined software functions. The AIIH server configuration files and database is not defined in this specification. There can be

one or many AIIH Servers on an Intranet and how they maintain consistency and Tunnel End Point configurations for IPv6 links is implementation defined.

The AIIH Server is an implementation where DNS, DHCPv6, and communications between those two applications exists. These applications MAY be co-located on the same host, but that is not a requirement of this specification. How DNS and DHCPv6 communicate is implementation defined . The AIIH Server SHOULD support the following operations:

1. Act as the Authoritative DNS Name Server for a set of IPv6 hosts that can be queried for IPv4 Global Addresses.

2. Communications between the AIIH DNS server and the AIIH DHCPv6 Server.

3. An AIIH DHCPv6 Server that can maintain a pool of IPv4 Global Addresses in an implementation defined manner.

4. An AIIH DHCPv6 Server that can maintain Tunnel End Points for IPv6 Links in an implementation defined manner.

5. An AIIH DHCPv6 Server to process DNS AIIH IPv6 host DNS queries, and Reconfiguring IPv6 hosts to assign IPv4 Global Addresses to their interfaces.

6. Support DHCPv6 Client's requesting IPv4 Global Addresses.

7. Dynamically Updating DNS with an IPv4 Global Address for an IPv6 host that supports IPv4/IPv6.

An AIIH Server MUST support a dual IPv4/IPv6 network layer and implementation of IPv4/IPv6.

The IPv4 address allocation can be triggered by two events. The first one is when an IPv6 host requests through DHCPv6 an IPv4 address to configure its IPv4 stack. The second event happens when a DNS A query is made for a node that only has an IPv6 address (see section 5.2). fails to respond to a DNS A RR query.

5.1.1. Requesting an IPv4 Global Address

An IPv4/IPv6 host can request an IPv4 Global Address by using the IPv4 Global Address Extension defined in section 7. The IPv4/IPv6 host MUST support DHCPv6 [4] and the DHCPv6 Extensions [5]. The Requests/Response Model of DHCPv6 will process this new extension as any other extension. There is no need to define a new message type for DHCPv6 for this processing or add to the DHCPv6 protocol.

Once the host has obtained an IPv4 Global Address it MUST NOT update DNS

to reflect an A type or PTR type record for this address. The reason is that the intent is to provide a host with this temporary address to use for communications with an IPv4 node. Once the reason for obtaining an IPv4 Global Address has been satisfied the host MUST Release this IPv4 Global Address from the AIIH DHCPv6 Server implementation.

On the other hand, if the address lifetime is about to expire, the AIIH client may send another request to the AIIH Server to keep this address assigned.

5.1.2 AIIH DHCPv6 Client IPv4 Global Address Requests

An AIIH DHCPv6 Server will receive DHCPv6 Requests for IPv4 Global Addresses from IPv6 hosts. The AIIH DHCPv6 Server will determine if an address is available and assign the address to the DHCPv6 Client as specified in section 7 of this specification.

5.1.3 AIIH DNS Query and DHCPv6 Processing

Once the AIIH DNS finds the IPv6 host being queried the AIIH DNS requests from its corresponding AIIH DHCPv6 Server to assign an IPv4 Global Address to the IPv6 host being queried.

The AIIH DHCPv6 Server will look within its pool of IPv4 Global Addresses for an address and if a Tunnel End Point address is required for the IPv6 host to reach the router to route packets onto the Internet. If an address is available the DHCPv6 Server will send a DHCPv6 Reconfigure Message to the IPv6 node to temporarily assign the node an IPv4 Global Address (see section 7).

Once the AIIH DHCPv6 server is certain that the IPv6 host has assigned the address to an interface, the AIIH DHCPv6 Server responds back to the corresponding AIIH DNS Server with the IPv4 Global Address assigned to the IPv6 host being queried, or that an address could not be assigned to this IPv6 host.

It is important to wait for an acknowledgment from the client to be sure that the host is up before validating an IPv4 address has been assigned. Nevertheless this could introduce a delay incompatible with the timer used during a DNS query. The dialog could be modified. Just after the DNSv6 temporary IPv4 address assignment, the AIIH DNS returns this address but with a small TTL. The real TTL will be used if the acknowledgment is received, otherwise the IPv4 address is deprecated for a some period of time.

The AIIH DNS Server will now respond to the IPv4 DNS Query as the Authoritative DNS Name Server with an address or host not found.

The AIIH DHCPv6 Server MAY send a dynamic update to DNS [6] to add an A type record to the Primary DNS Server, where the query came from to the AIIH DNS Server. The Time-To-Live (TTL) field in the update MUST NOT be set to be greater than the valid lifetime for the IPv4-Compatible address in the DHCPv6 Extension provided to the DHCPv6 Client. It is highly recommended to not update the DNS with an A record for the IPv6 host, unless that IPv6 host provides a permanent IPv4 Application service needed by IPv4 hosts.

5.1.4. Cleaning up the AIIH IPv4 Assigned Address

Once the IPv4 address expires, the DHCPv6 Server will permit the IPv4 address to be reused. But before the address can be reused the DHCPv6 Server MUST delete the IPv4 address from the Primary DNS Server, through the Dynamic Updates to DNS mechanism, if an A record was added to the relative Primary DNS Server.

If an AIIH client wants to keep the temporary IPv4 address after its expiration time, it MUST send a DHCPv6 request before the address expires.

5.2 Links with other DNS

When the Primary DNS Server for the IPv6 node receives the IPv4 hosts query, it will do a DNS search for that IPv6 host and find that there is an Authoritative DNS Server for that specific DNS A record, which represents an IPv6 host. That DNS Server will be one part of the AIIH Server software. After the AIIH DHCPv6 Server assigns the IPv6 node a temporary IPv4 Global Address, the AIIH DNS Server will respond to the original IPv4 DNS query authoritatively with an IPv4 Global Address for the IPv6 host or return host Not Found.

For Example:

IPv4 node "v4host.abc.com" queries for "v6host1.xyz.com"

Query reaches Primary DNS Server for "v6host1.xyz.com".

```
xyz.com.  IN SOA primary.xyz.com.  etc etc.
.
.
xyz.com          IN  NS  primary.xyz.com
aiih.xyz.com     IN  NS  v6trans.aiih.xyz.com
.
.
primary.xyz.com          IN   A    202.13.12.6
v6trans.aiih.xyz.com     IN   A    202.13.12.8
 .
 .
 .
v6host1.xyz.com        IN   CNAME   v6host1.aiih.xyz.com
v6host2.xyz.com        IN   CNAME   v6host2.aiih.xyz.com
v6host3.xyz.com        IN   CNAME   v6host3.aiih.xyz.com
```

DNS query will end up going to the authoritative server v6trans.aiih.xyz.com looking for v6host1.aiih.xyz.com. This permits the AIIH Server to now process a request for an IPv4 Global Address for an IPv6 host that had no IPv6 DNS AAAA Record [18].

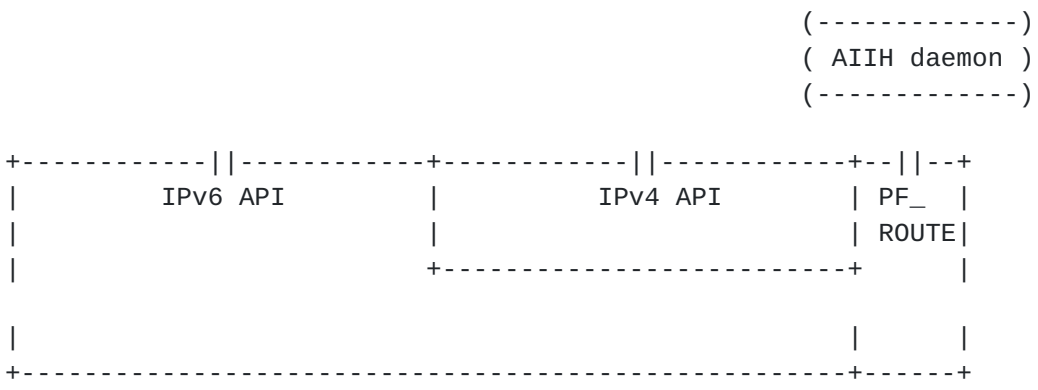
If DTI is present, the reverse DNS must be linked to the pool of addresses managed by the AIIH Server.

6. DTI

6.1. DTI Architecture

The DTI interface will be used to send IPv4 packets during the interoperation of IPv4 and IPv6. The routing table of the host forwards the information to that interface. It is possible to send all the IPv4 packets through this interface by using only the default prefix.

The DTI interface is placed between the IPv4 API and the IPv6 layer, as shown in the following figure, the architectural model assumes a BSD UNIX type platform.



On every IPv6 node an AIIH daemon is running to manage the allocation of the IPv4 addresses need and perform the address resolution when needed.

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	

6.1 Assignment of the IPv4 address to the DTI

When the DTI interface is activated, no IPv4 address is given to that interface. If the interface is active, but has no IPv4 address, when it has to send the first IPv4 packet, the interface sends a request to the daemon. The daemon will send a DHCPv6 request to the AIIH server to get the temporary IPv4 address.

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 if it has an IPv4 interface configured. This is just one example of how an implementation can determine if the AIIH daemon must be called.

6.2 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 receiver SHOULD cache the association between the IPv4 and IPv6 source address.

6.2.1 IPv6 source address

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

6.2.2 IPv6 destination address

When a DTI has to encapsulate an IPv4 packet into an IPv6 packet. The DTI as to find the IPv6 address for the destination, called in this document a Tunnel End Point (TEP). The tunnel end point can be directly the host destination or, if the destination host is IPv4-only, the IPv6 address of an IPv4/IPv6 router.

This document propose two ways for resolving the tunnel end point. The first one is dynamic and uses the AIIH Server, the second one is static and is returned in the DHCPv6 packet when a temporary IPv4 address is allocated to the interface or by static configuration of the node.

The IPv6 hosts MAY have a static TEP. DSTM border routers SHOULD use dynamic TEB, but it is possible in the case of a single homed network, and for exiting traffic only, to avoid dynamic address resolution and cache only the association of the IPv4 and IPv6 source address of incoming packets.

For a host in the case of the failure of the dynamic TEP, static TEP SHOULD be used.

For DSTM border routers, failure of the dynamic TEP SHOULD generate an ICMPv4 host unreachable message.

6.2.2.1 Dynamic TEP

Dynamic TEP determination is similar to MAC address resolution when sending a IP packet over an Ethernet link. The only difference is that no broadcast facilities can be used to find a TEP.

In the Unix operating systems, this resolution should not be done in the kernel. Some operating systems offer the possibility to do external resolution. A query is sent to a daemon in the user space. This daemon does a DHCPv6 query to find the TEP. In the rest of this document we will consider this architectural model, but this is not a limitation for implementing DTI.

When the resolver daemon receives a query from the kernel, it sends a DHCPv6 query to the AIIH Server to get the IPv4 address for this host.

Static TEP cache contains the IPv6 address of a node inside the network. The IPv6 address is stored in a cache for a duration indicated in the DHCPv6 message.

6.2.2.2 Static TEP

Static TEP may be returned by the AIIH Server with the temporary IPv4 address. This TEP is used when the dynamic TEP resolution fails or has not been activated. This will be the case when the DTI daemon asks for an address not registered in the AIIH Server (for example an IPv4 address outside of the DSTM cloud).

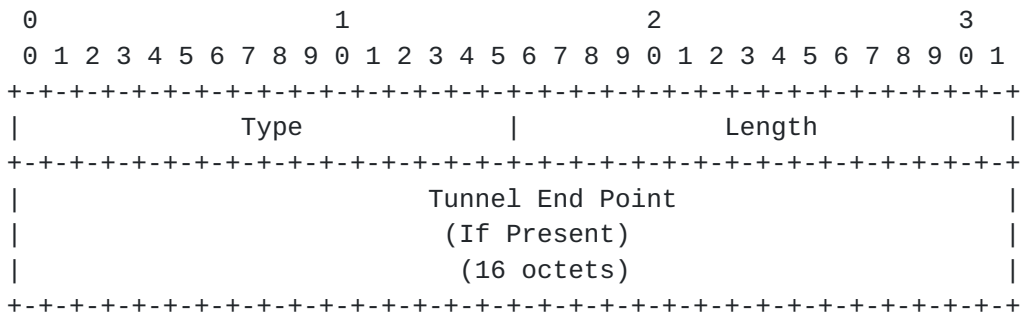
Static TEP contains the IPv6 address of a DSTM border router. Static TEP records are stored as long as the temporary IPv4 address is assigned to the interface in case of DHCP configuration, and as long as the DTI interface is active in case of manual configuration.

7. AIIH DHCPv6 Requirements

The AIIH DHCPv6 processes will use the DHCPv6 protocol and extensions to communicate between the AIIH DHCPv6 Server and the DHCPv6 Client. A new extension is required for DHCPv6 (section 4.1) to support AIIH. But there are some additional requirements placed on the AIIH processes that are not specific to the DHCPv6 protocol, but as transition and interoperation mechanisms for the IPv6 hosts.

7.1 DHCPv6 IPv4 Global Address Extension

The DHCPv6 IPv4 Global Address Extension informs a DHCPv6 Server or Client that the IPv6 Address Extension [5] following this extension will contain an IPv4- Compatible Address [20], or is a Request for an IPv4 Global Address from a Client, or a Reply assigning a Global IPv4 Address to a Client from a Server. The extension can also provide an IPv4-Compatible or IPv6 address to be used as the Tunnel End Point to encapsulate an IPv6 packet within IPv4, or an IPv4 packet within IPv6.



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.

7.2 AIIH Server Processing of an IPv4 Global Address Extension

When a DHCPv6 Server receives an IPv4 Global Address Extension it MUST assume that the next extension in 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-Compatible Address.

When a DHCPv6 Server sends a Client a Reconfigure Message to assign an IPv4 Global Address to an interface the Server MUST NOT set the "N" bit in the Reconfigure Message, so the Client performs the necessary Request/Reply DHCPv6 processing to obtain the address from the Server. The Server MUST NOT assume that the Client has assigned the address to

an interface until it has sent the corresponding Reply to the Client.

The Server will no a priori the IPv6 routable address, when sending a

Reconfiguration Message, of a Client within the Intranet, and should use that address with its own IPv6 address as the transaction binding cache until the DHCPv6 Client/Server protocol processing has completed.

The Server will look in its implementation defined IPv4 Global Address configuration to determine if a Tunnel End Point is required for a specific IPv6 Address Prefix. If that is the case the Server will put the address for the Tunnel End Point in the IPv4 Global Address Extension. If the Tunnel End Point address is an IPv4 address the Server will put that address in the extension as an IPv4-Compatible address.

7.3 AIIH Client Processing of an IPv4 Global Address Extension

When a DHCPv6 Client receives an IPv4 Global Address Extension it MUST assume that the next extension in a DHCPv6 Reconfigure or Reply Message; the Server is either assigning an IPv4 Global Address or supplying an IPv4 Global Address. The address present in either of these messages will be in the form of an IPv4-Compatible Address.

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

The Client MUST not assume it can use the IPv4 Global Address until it has received a corresponding Reply to the Client Request, which is required for a Reconfigure Message too as specified in section 7.2.

Once the Client is assured it can use the IPv4 Global 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-Compatible Address supporting the processing required for an IPv6 address regarding the valid and preferred lifetimes as specified in IPv6 Addrconf [19]. Once the IPv4-Compatible address valid lifetime expires the IPv4 address MUST be deleted from the respective interface and a DHCPv6 Release Message MUST be sent to the AIIH DHCPv6 Server to delete the IPv4 Global Address from the Servers bindings.

3. If a Tunnel End Point address is provided in the IPv4 Global Address Extension, the Client MUST create a configured tunnel to the Tunnel End Point address, in an implementation defined manner. If the Tunnel End Point address is an IPv4-Compatible address then the encapsulation is IPv4 within IPv4, if the Tunnel End Point is an IPv6 address then the encapsulation is IPv6 in IPv4. These encapsulation mechanisms are defined in other IPv6 specifications [13, 15].

8. Security Considerations

The AIIH 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 AIIH does not break secure end- to-end communications at any point in the mechanism.

9. Year 2000 Considerations

There are no Year 2000 issues in this specification.

Appendix A: DSTM Discussion and Issues

1. **DHCPv6 work needs to be proposed as DHCPv6 additional extension.**

2. **Need to review timers for DHCPv6 and DNS for performance and scalability.**

3. **Can we make the DSTM router a Transition Box with DTI using AIIH?**

4. **Some of the refernences in the spec are not needed.**

5. **Need to add acknowledgements to spec from AIIH and DTI previous work and the input.**

6. **Should DSTM also support tunneling IPv6 within IPv4 at the DTI?**

7. **Should the DSTM Overview contain more information.**

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 and C. Perkins. Dynamic host Configuration Protocol for IPv6. draft-ietf-dhc-dhcpv6-14.txt March 1999 (work in progress).

[5] C. Perkins. Extensions for the Dynamic host Configuration Protocol for IPv6. draft-ietf-dhc-dhcpv6ext-11.txt March 1999. (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/U14
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