INTERNET-DRAFT
NGTRANS Tools Working Group
Expired December 1999

Laurent Toutain
Hossam Afifi
ENST Bretagne

Jim Bound
Compaq

Dual Stack Transition Mechanism (DSTM)

<draft-toutain-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. 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. This specification defines a mechanism called "Assignment of IPv4 Global Addresses to IPv6 hosts" (AIIH), which will assign an IPv6 host a temporary IPv4 Global Address, which can be used to communicate with a host that supports IPv4 or IPv4/IPv6. This document includes also the definition of a Dynamic Tunneling Interface (DTI) to ease the automatic IPv4 address assignment and to remove the IPv4 routing table from routers. Another objective is to demonstrate that IPv6 Addresses can be deployed now instead of non-Global IPv4 Addresses within an Intranet.

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. 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.

This specification defines a mechanism called "Assignment of IPv4 Global Addresses to IPv6 hosts" (AIIH), which will assign an IPv6 host a temporary IPv4 Global Address, which can be used to communicate with a host that supports IPv4 or IPv4/IPv6. A AIIH Server combines the functionality of a extended DHCPv6 server and a DNS server. An AIIH DHCPv6 server assigns dynamically temporary IPv4 addresses to Dual Stack Equipments. The AIIH DNS server is used to keep a mapping between the name, the IPv4 address and the IPv6 address of a Dual Stack Equipment.

Another objective of this document is to define the functionality of a dynamic tunneling interface (DTI) encapsulating IPv4 packets into IPv6 packets. This will ease the assignment of dynamic IPv4 address since the network topology is hidden. This allows, most of the time, a flat addressing plan. The second advantage is that IPv4 packets will not be directly forwarded anymore. The IPv4 routing table can be suppressed.

This document also proposes some steps to migrate from the dual environment described in RFC 1933 to an IPv6 only domain. It exhibits some scenarios to validate the introduction of AIIH servers and DTI interfaces.

The methods described in this document may not be used for the general case. The best way is to migrate as quickly as possible hosts and applications to IPv6 or to use Application Level gateways (ALG). This document proposes a way to remove a possible blocking situation during the migration period, which would postpone the introduction of IPv6.

1.1. Scenarios

To study the behavior of the AIIH Server and the DTI interface, we focus on the following scenarios:

- The first scenario is the case of an IPv6 application running on a IPv6 host initiating a dialog with an IPv4 equipment.

- The second scenario is an IPv4 application, running on an IPv6 host initiating a dialog with an IPv4-only host.

- The third scenario is an IPv4-only application running on an IPv4-only host initiating a dialog with a IPv6 host.

1.3. Architecture model

The design model supports the following network configuration abstraction:

```
<------- domain -------------------------><-provider-v4-only---->
|                                         |                      |
host X ----------------------- Router Y ------------------- host Z
(Intranet)                (Intranet & Internet)        (Intranet)
```

Host X represents an IPv4/IPv6 implementation, that has an IPv6 address. The IPv6 address is denoted as X6 and, if available, the IPv4 address will be denoted as X4.

Router Y represents an IPv4/IPv6 implementation that has both an IPv4 Global addresse and an IPv6 Address. The IPv4 address is denoted as Y4 and the IPv6 address is denoted as Y6. Router Y implements two routing tables, one for IPv4 and one for IPv6. Router Y belongs to the same domain as host X.

Host Z represents an IPv4 or IPv4/IPv6 implementation that has an IPv4 Global Address, and MAY have an IPv6 Address. The IPv4 address is denoted as Z4 and if an IPv6 address exists it is denoted as Z6.

1.2. Migration steps

RFC 1933 describes the Dual Stack approach and defines a way to introduce compatibility between IPv4 and IPv6 applications. If the operating system and the applications have been "v6fied", dialogs between IPv6 hosts will use the IPv6 protocol. Otherwise dialogs with at least one IPv4 host or application will use IPv4 protocol. IPv6 applications can use both stacks with IPv4-mapped addresses.

Nevertheless, this requires a dual configuration either for the hosts or for the intermediary equipments. This does not solve the problem for the lack of IPv4 addresses since each equipment still needs a IPv4 address.

This is the first step of the transition. It is more or less the state of IPv6 platforms now deployed in the 6bone.

The second step is to remove the static configuration of IPv4 addresses when possible. When it will be necessary, an AIIH server will assign a temporary IPv4 address to a host that needs to communicate with an IPv4-only equipment or with a IPv4-only application. The rest of the time, the IPv6 stack will be used.

The configuration during this step will be difficult since an addressing plan will still be necessary for the IPv4 protocol and routers will have to manage the IPv6 and the IPv4 routing plan.

The third step is to remove the IPv4 routing functions inside routers and keep only the IPv6 routing plan. The IPv4 packets produced by IPv4 applications or hosts will be encapsulated inside IPv6 packets. DTI interfaces will establish the mapping between the IPv4 address and the IPv6 address of the destination by using the AIIH server of the destination (if available). The IPv4 source address will be, as in step 2, assigned temporary by the AIIH server.

Note that DTI interface can be deployed without any dynamic address allocation, without a AIIH Server. In this case manual configuration is needed to assign address to the DTI interface and to configure the DNS. So it is more logic in a migration process to start with dynamic IPv4 address allocation and then use DTI to remove IPv4 routing.

In the fourth step, the mechanisms described in step 3 are the same, but they are managed by the IPv6-only provider which carries IPv4 packets using tunnels. This allows a company to get a unique provider, which manages the inter-connectivity with the IPv4 world. Some security measures must be taken to avoid attacks like deny of service by requesting the entire IPv4 address pool of the provider. These measures are not in the scope of this document.

1.3. Document architecture

The specification will begin by defining the terminology (section 2), then discuss the AIIH design model (section 3), then the DTI architecture model is described with its interaction with the AIIH Server (section 4). Section 5 completes the mechanism by defining the DHCPv6 Extension needed to assign a temporary IPv4 address to an IPv6 node. The specification then discusses Security (section 5) and Year 2000 considerations (section 6). Appendix A will enumerates Open Issues that need to be discussed in the ngtrans Tools Working Group, and maintain the state of Open Issues as STILL OPEN, RESOLVED, or PARTIALLY RESOLVED during the draft updates to AIIH. Appendix B will keep a historical account of changes to the draft and rationale for those changes as they occur, and maintain consistence with the Open Issues in Appendix A.

2. Terminology

2.1 IPv6 AIIH Terminology

AIIH Domain	An area where AIIH Server can access to IPv6 equipments.
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.
DTI encapsulation box:	A intermediary equipment doing the IPv6 tunneling when the end-system is unable to do it.
DTI resolver:	An application that finds the IPv6 destination address using the IPv4 address of the packet being encapsulated. As ARP or Neighbor discovery the DTI resolver is only called for the first packet.
DTI daemon	synomyn to DTI resolver
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.
Transition Box	An equipment managing the encapsulation of IPv4 packets either when one of the links is IPv4-only or when the destination has only an IPv4 stack.
Tunnel End Point	Destination of the IPv6 packet containing a 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. AIIH 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 enterprise on a temporary basis for use by hosts in the site. The design model also assumes that the site has an IPv4/IPv6 router in the site that is used to send and receive packets over the Internet.

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 IPv6-only stack implementation. For embedded system type nodes that support only an IPv6 stack, AIIH cannot be a solution.

3.1 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 a IPv6 host requests through DHCPv6 an IPv4 address to configure its IPv4 stack. The second event is when the AIIH DNS Server fails to response to a A RR query. The temporary IPv4 address is sent by the AIIH DNS Server which keeps the mapping with the IPv6 address and the name of the equipment in the AIIH domain. The temporary IPv4 address is stored in the AIIH DNS Server as a A record.

3.1.1. 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 5. 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.

3.1.2 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 5 of this specification.

In case of an IPv4 addressing plan (i.e. step 2 of the migration process), the AIIH Server MUST be configured to allocate IPv4 address in regard with the network topology.

The AIIH DHCPv6 Server sends a Dynamic Update to the AIIH DNS server. The TTL must be shorter than the duration of the allocation to the client.

3.1.3 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 5).

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 a acknowledgment from the client to be sure that the host is up before validate an IPv4 address assignation. 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 while.

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.

The Dynamic Update will be done for the direct queries, this will allows other queries for the IPv4 address to get the same answer. If DTI is present, another Dynamic Update will be done for the reverse queries. The type recorded should be TEP (Tunnel End Point). See discussion paragraph 4.1.1.

3.1.4. 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, thru the Dynamic Updates to DNS mechanism, if an A record was added to the relative Primary DNS Server.

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

3.2 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.

3.3 Scenarios

These scenarios take place during the step 2 of the migration process. IPv6 equipments have a dual stack, but only the IPv6 stack is configured. Routers have both of their stacks configured.

Notation of the equipment is defined in paragraph 1.2.

```
==>  means a IPv6 packet
-->  means a IPv4 packet
..>  means a DNS query or response. The path taken by this
     packet is unknown
"Z"  means the DNS name of "Z"
```

3.3.1 X6 (with a v6 application) to Z4

```
      AIIH   Y4          Z4
X6           Y6
 |            |            |
 |            |            |    - X6 asks the DNS for a AAAA for "Z"
 |            |            |    - the DNS answers a error
 |            |            |    - X6 asks for the A RR for "Z"
```

```
    |            |            |    - the answer is Z4
    |            |            |    - X6 needs a IPv4 address
    |====>       |            |    - X6 queries the AIIH server for an
    |            |            |      IPv4 address using DHCPv6
    |<====       |            |    - The DHCP server locates the client
    |            |            |      and attributes temporally a v4
    |            |            |      address. (the tunnel end-point is
    |            |            |      not set in the response)
    |            |            |    - The AIIH Server may register IPv4
    |            |            |      address to the DNS through
    |            |            |      a Dynamic Update
    |------------+----------->|    - X4 can send the IPv4 packet to Z4
    |<-----------+----------->|    - and vice versa.
```

3.3.2 X6 (with a v4 application) to Z4

Same behavior as 3.3.1, except that X will request directly a A RR to the DNS instead of going first through a AAAA query.

3.3.3 Z4 to X6

```
         AIIH   Y4     DNS   Z4
   X6           Y6
    |            |            |
    |            |      <-----|   - Z asks for ôXö
    |       <-...|            |   - The request reaches to the AIIH
    |            |            |     Server
    |<=====      |            |   - The AIIH Server assigns a v4
    |            |            |     address to X
    |=====>      |            |   - X acknowledges
    |      ..................>|   - The AIIH server answers with the
    |            |            |     newly assigned v4 address
    |            |            |   - The AIIH Server may register the
    |            |            |     IPv4 address through a Dynamic Update
    |<-----------+------------|   - Z4 can send the packet to X4
    |<-----------+----------->|   - and vice versa
    |            |            |
```

4. DTI

4.1. DTI Architecture

The DTI interface will be used to send IPv4 packets during the migration process. The routing table of the host forwards the information to that interface. It is possible to send all the IPv4 packets through this interface. Some other prefixes can be used to send directly native IPv4 packets.

The DTI interface is placed between the IPv4 API and the IPv6 layer, as shown in the following figure.

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

```
|         IPv6 API         |         IPv4 API        |
|                          |                         |
|                          +-------------------------+
|                                                    |
+----------------------------------------------------+
```

The following example gives the configuration of a routing table using DTI. The addresses in this example are private, but the use of global IPv4 addresses gives a similar result. With this routing table, if the destination address contains the prefix 10.35.3/24 IPv4 packet are send directly on the link. If the destination prefix is 10.34.3.0/24, packets are sent to the DTI interface. Otherwise the packet is sent to the default router.

```
Routing tables

Internet:
Destination    Gateway            Flags    Refs      Use   Mtu  Netif Expire
default        10.35.3.3          UGSc        3        0  1500    le0
10.34.3/24     10.34.3.2          UXc         0       10  1460   dti0
10.35.3/24     link#3             UC          0        0  1500    le0   -
10.35.3.3      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
```

In this example, the DTI already has an IPv4 address. But this address can be dynamically acquired using the AIIH Server as explained in chapter 3.

When a DTI has to encapsulate a IPv4 packet into 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 or, if the destination host is IPv4-only, a IPv6 address of a transition box.

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 proceed by the IPv4 layer. The receiver should memorize the association between IPv4 destination address and TEP.

This document propose two ways for resolving tunnel end point. The first one is dynamic and use the AIIH DNS Server, the second one is static and is returned in the DHCPv6 packet when a temporary IPv4 address is allocated to the interface. The dynamic resolution is mandatory. The tunnel end point in the DHCPv6 message is optional. This TEP is used when dynamic TEP fails (for example, the destination does not have a AIIH server).

Dynamic TEP should be used when IPv4 host or application are spread inside a domain. Static TEP should be used when the boundary between IPv4 and IPv6 domain is clear (for example an IPv6 domain, connected to an IPv4-only provider).

4.1.1 Dynamic TEP

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

In 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 DNS 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.

The AIIH DNS Server MUST be reachable in the reverse query DNS tree for the range of IPv4 addresses managed by this server.

When the resolver daemon receives a query from the kernel, it sends a reverse query to the DNS to get the record for this host. Three kinds of records can be proceeded by the daemon:

- PTR record: the daemon sends another query to the DNS to get the AAAA record of this host and returns the value to the kernel.

- AAAA record: the value is returned to the kernel

- TEP record: this record must be introduced for the DTI interface to avoid confusion between the destination and the tunnel end point (see paragraph 4.2.1). It contains the address of the tunnel end point. Its value is returned to the kernel. We recommend the use of this record. Only the AIIH server will have to manage such records. They are, most of the time, created by the AIIH DHCP Dynamic Update when a temporary address is allocated to an IPv6 host.

The IPv6 address is stored in a cache for a duration indicated in the TTL field of the DNS answer. The following example shows a entry for destination 10.34.3.1

```
/homes/toutain>netstat2 -rnf inet
Routing tables

Internet:
Destination    Gateway            Flags  Refs   Use   Mtu  Netif Expire
default        10.35.3.3          UGSc     3     21  1500    le0
10.34.3/24     10.34.3.2          UXc      0    109  1460   dti0
10.34.3.1      3ffe:305:1002:4:a00:2bff:fe1b:8942 UHLS  0  0 1460 dti0 27
10.35.3/24     link#3             UC       0      0  1500    le0   -
10.35.3.2      8:0:2b:1c:11:1f    UHLWl    0     29  1500    lo0
10.35.3.3      8:0:2b:1c:af:15    UHLW     4      0  1500    le0    304
10.35.3.255    ff:ff:ff:ff:ff:ff  UHLWb    0      2  1500    le0
127.0.0.1      127.0.0.1          UHl      1    298 16384    lo0
```

4.1.2 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. This will be the case when the DTI daemon asks for a TEP RR on a non AIIH DNS Server.

Static TEP is used to tunnel packets to a transition box linked to a IPv4 network. In some domains where the delimitation between the IPv6 and the IPv4 is strict it is sub-optimal to wait for the failure of the DNS query before using the static TEP. DHCPv6 configuration message should contain a flag to force the use of static TEP.

4.1.3 IPv4-only hosts

It is not possible to modify IPv4-only hosts or the applications running on such hosts. These hosts are configured to send IPv4 packet on the network to a transition box that will encapsulate IPv4 packet into IPv6 packets. For an IPv4-only host, this equipment is viewed has a default router.

This means that an addressing plan is required for these hosts. At least two IPv4 addresses are needed. This will depend on the number of IPv4 addresses available. One extreme possibility is to keep the addressing plan that existed before DTI, but this could lead to a waste of IPv4 addresses. The other possibility is, if the capability of the IPv4-only allows it, to assign a prefix length of 30 to that link.

The IPv4 address is configured manually in the reverse DNS tree in association with a TEP record that gives the IPv6 address of the tunnel end point.

Depending on the DF bit of the IPv4 packet, the translation box will do the fragmentation (i.e. use the IPv6 fragmentation extension) or will send a ICMP message to the IPv4-only host.

4.2 Examples

The notation +++> means a IPv4 packet encapsulated in a IPv6 packet.

4.2.1 X6 (with v6 application) to Z4 with TEP dynamic resolution

Z4 is in the same domain as X6. The DNS for "Z" is configured in the reverse query DNS database as follow:

```
128.3.4.6  PTR   Z.aiih...  ;the database is statically configured for Z
           TEP   3ffe:..... ;address of the Tunnel End Point
```

The DNS has been configured with the address of Z

```
Z  A  128.3.4.6



      AIIH         TB     Z4
X6          Y6/Y4
 |            |            |
 |            |            |    - X6 asks the DNS for a AAAA for "Z"
 |            |            |    - the DNS answers a error
 |            |            |    - X6 asks for the A RR for "Z"
 |            |            |    - the answer is Z4
 |            |            |    - routing protocol has been previously
 |            |            |      configured in X to route v4 through
 |            |            |      dti (compatible with IPv4-mapped
 |            |            |      addresses).
 |            |            |    - X6 needs a IPv4 address (first use)
 |====>       |            |    - X6 queries the AIIH server for an
 |            |            |      IPv4 address using DHCPv6
 |<====       |            |    - The DHCP server locates the client
 |            |            |      and attributes temporally a v4
 |            |            |      address. (the tunnel end-point is
 |            |            |      not set in the response).
 |            |            |    - the DHCP Server sends a Dynamic Update
 |            |            |      to the DNS to memorize the association
 |            |            |      x4<->x6 (x4 TEP X6).
 |            |            |    - dti has to find the IPv6 address of
 |            |            |      the tunnel end-point for Z4
 |......................>  |    - dti daemon asks the dns for the IPv6
 |            |            |      TEP for Z4 (transition box)
 |<......................  |    - AIIH DNS answers the TEP
 |++++++++++++++++++>      |    - The dti sends the v6 packet to the
 |            |            |      tunnel end-point
 |            |     ------>|    - The TB sends the packet to
 |            |            |      the destination
```

If the tunnel end point for Z4 had been recorded in the DNS with a AAAA record, then the source would have been confused and would have sent the packet directly in IPv6 to the transition box.

4.2.2 X6 (with v4 application) to Z4 with TEP dynamic resolution

The dialog is the same as shown in paragraph 4.2.1 when an IPv4 application wants to talk with a IPv4 application on Z4.

To maintain compatibility between two v4 application, a v4 application running on a IPv6 host may wish to send IPv4 packets to another application running also on an IPv6 host, called Z6. Y6 is not used in this model. It was kept to show that X and Z can belong to two separate AIIH domains.

```
      AIIH         AIIH
X6           Y6            Z6
 |            |             |
 |............|.....>       |    - X asks for the v4 address of ôZö.
 |            |      =====>|    - AIIH Server assigns a v4 address to Z
 |            |             |    - AIIH registers this address to
 |            |             |      its DNS server
 |<...........|.....        |    - Z4 is returned to X
 |            |             |    - The v4 address of Z is used by the
 |            |             |      application, which sends v4 packet
 |            |             |      to the kernel
 |            |             |    - routing table has been previously
 |            |             |      configured in X to route
 |            |             |      v4 through dti
 |=====>      |             |    - dti receives its first packets, asks
 |<=====      |             |      the AIIH server to assign
 |            |             |      the v4 address to the DTI interface
 |            |             |    - AIIH registers this address
 |            |             |      to the dns server
 |            |             |    - dti has to find the IPv6 address
 |            |             |      of the tunnel end-point for Z4
 |.................>        |    - dti daemon asks the dns for the
 |<..................       |      TEP RR for Z4
 |++++++++++++++++++++++++>|    - dti tunnels the packet to Z6
```

4.2.3 Z4 to X6 with TEP dynamic resolution

This example covers any scenario where a IPv4-only host wants to reach an IPv6 host. This could be any application, but in this example, we will focus on a DNS query for a IPv4-only host to the DNS server of the domain.

The IPv4-only host is configured with an IPv4 address and a default router. The DNS is also configured with the IPv4 address of the DNS server. Therefore, the DNS server must have a statically assigned IPv4 address. This configuration could be stored in the AIIH Server or directly on the host running the name server. We will suppose in this example that the configuration is stored in the AIIH Server.

```
DNSv4  AIIH   Y4          Z4
DNSv6         Y6
 |            |             |
 |            |             |    - Z4 wants to know the IPv4 address
 |            |             |      of some equipment in the Internet
 |            |             |    - Z4 has been configured with Y4 as
 |            |             |      default router and DNSv4 as resolver
 |            |<-----------|    - Z4 sends a query to the default route
 |            |             |    - Y receive the packet, Y routing table
 |            |             |      lead packets (except for the link where
 |            |             |      Z4 is connected) to the DTI interface.
 |      <=====|             |    - DTI has to find the TEP. It sends a
```

```
 |      =====>|            |     query to the AIIH server for the TEP
 |            |            |     for DNSv4.
 |<=====      |            |   - AIIH assigns the IPv4 address to DNSv6
 |<+++++++++++ |           |   - The query is tunneled to DNSv6
 |            |            |
```

4.2.3 X6 to Z4 with static TEP resolution

This example covers the case where X6 wants to reach a host outside the AIIH domain. Y is the last router for the IPv6 domain and is connected to the Internet v4. In this example, Y belongs to the domain.

This scenario is used when a web browser in the IPv6 domain contact a IPv4 HTTP server.

```
      AIIH         DNS    Z4
X6          Y6/Y4
 |            |            |
 |=====>      |            |   - X6 after the first DNS query to get
 |            |            |     Z4 address, sends a request to the
 |            |            |     AIIH server to obtain a temporary
 |            |            |     IPv4 address.
 |<=====      |            |   - AIIH returns the IPv4 address and
 |            |            |     the tunnel end-point
 |....................>    |   - dti daemon asks the dns for the IPv6
 |            |            |     TEP for Z4 (transition box)
 |            |            |
 |            |            |
 |            |            |   - no answer, the DTI use the static TEP
 |+++++++++++>|            |   - Packet is tunneled to the static TEP
 |            |----------->|   - and sent with IPv4 to Z4
```

When Z4 replies, the packet will not necessary reach the router Y. Routing in the internet is not symmetrical and can change. The AIIH Server does not participate to the routing protocol, so the given TEP can be sub-optimal. The IPv4 packet sent by Z4 will reach a router YÆ (by definition YÆ is at the boundary between a IPv4-only domain and an IPv6 domain). YÆ can find out the TEP to reach X6 by using the dynamic TEP resolution.

To avoid the time-out when the dynamic TEP resolution fails, the DTI can be configured to send directly packets to the static TEP.

5. 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 5.1) 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.

5.1 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.

```
 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.

<< NOTE >>
flags are missing in this specification
<<END of NOTE>>

5.2 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.

5.3 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 5.2.

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].

6. 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.

7. Year 2000 Considerations

There are no Year 2000 issues in this specification.

Appendix A - Open Issues

- Need to add Examples for the new A6 Record types and how AAAA records can be used initially and references.

  OPEN 1/99

- Should use new Basic API terms for APIs.

  OPEN 1/99

- Need to add references for IPsec.

  OPEN 1/99

- Need to change references for DNS SEC esp solutions for Dynamic Updates to DNS.

  OPEN 1/99

- Need to look at issues for TCP TIME_WAIT state and other issues of addresses timing out.

  OPEN 1/99

- Need to add words to the design objective of preserving the end-to-end model for IPv6.

  OPEN 1/99

- The draft does not speak of PTR records for the IPv6 node A record once its created. But its only useful during the lifetime of the assigned IPv4 address.

  STILL OPEN 3/98 Draft. Closed - New A6 Records

- RFC 1183 RT Record is Experimental and there is some concern its obsolete. Though some implementations still support some code for the RT record. Also the Route Through semantics specified may need to strongly state the query is passed thru to the AIIH server. This needs to be discussed.

  RESOLVED 3/98 Draft RT record deprecated.

- The Primary Server must look for the IPv6 node A record first before finding the RT record. This needs to be verified as an implementation issue.

  RESOLVED 3/98 Draft - Use CNAME Records.

- When the AIIH Server responds to the query it may not be authoritative. This needs to be verified and checked. RESOLVED 3/98 Draft - Use CNAME Records and AIIH Server will be authoritative for the AIIH ZONE.

- Use of TTL for DNS Caches can cause problems for existing IPv4 applications that cache IPv4 addresses.

  PARTIALLY RESOLVED - 3/98 Draft do not update DNS unless application will be permanent as opposed to transient. But TTL's that are updated still need some thought for legacy applications. This also points to possibly adding new fields to the hostent structure which will at least help new IPv6 applications and legacy IPv4 applications to change to act in a well behaved manner.

- Specification needs a design example to get packets from the IPv6 node to an egress IPv4 router.

  PARTIALLY RESOLVED - 3/98 Draft added Design Section discussing tunneling mechanisms to be used and added Tunnel End Point address supplied by the AIIH DHCPv6 Server. Still needs more discussion.

- NNAT name does not state what the specification does.

  RESOLVED - 3/98 Draft changed name to AIIH.

Appendix B - Draft Changes and Rationale History

Prior to January 1999:

- Changed the name of the draft from NNAT to AIIH. This also was done to prevent any perceived antagonism towards the NAT IETF work, which is not an objective of this work.

- Changed the Introduction to be more descriptive of the task at hand.

- Added IPv4 Global Address definition to terminology section.

- Added tunnel routability discussion to Design Model and a diagram abstraction to be used by the specification as a point of reference.

- Added to the architecture the ability for an IPv6 node to request an IPv4 Global Address from an AIIH DHCPv6 Server. This will permit AIIH to not only be useful for incoming IPv4 host communications with IPv6 hosts but also for outgoing IPv4 communications to the Internet from IPv6 hosts and for Intranet enterprise communications between an IPv6 host and IPv4 host.

- Hinted that AIIH could be used in future work to define the capability for two IPv6 hosts separated by an IPv4 cloud to to communicate thru tunnels, like thru a production 6bone network on the Internet.

- Added new section to define how an IPv6 host can request an IPv4 Global Address.

- Defined new mechanism for DNS query processing when an IPv6 host is looked for from an IPv4 host, thru the use of CNAME and NS records. This also permits IPv4 host Intranet queries too now.

- New text clarifying that within the Intranet processing AIIH must only be used with IPv4 Global Addresses and Private IPv4 addresses should be retrieved from DHCPv4, via the IPv6 hosts IPv4 stack.

- Added new text defining the AIIH Server and the interaction with DHCPv6 and DNS applications. Also further refined the requirements of the AIIH Server model.

- Expanded the section on the new DHCPv6 Section defining the required Server and Client behavior. Added support to permit AIIH to be used for Intranet and Internet communications from within the site.

- Changed the DHCPv6 Extension for IPv4 Global Addresses to make it an extension which defines the next extension to be a request for AIIH processing relative to DHCPv6.

- Added a Tunnel End Point address to the new extension so IPv6 hosts can configure tunnels to communicate with the egress router to transmit or reply with IPv4 on the Internet or within the Intranet.

- Defined the AIIH side affect requirements for IPv6 hosts using this mechanism with DHCPv6.

- Updated and added to the Acknowledgment and References Section.

- Updated the Open Issues from December 1997 draft and noted the status of each issue as STILL OPEN, RESOLVED, or PARTIALLY RESOLVED.

- Updated the Changes from this draft.

January 1999:

- Updated References.

- Fixed Edit Issues

- Added new Open Issues.

- Removed all terms of NNAT except for History.

Acknowledgments

The author would like to thank Erik Nordmark for spending time reviewing with him this idea and suggesting the use of the DHCPv6 Reconfigure Message, Richard Johnson for suggesting the use of the DNS CNAME Record, and Robert Watson who suggested that the AIIH DHCPv6 and DNS Server be co-located. George Tsirtsis who suggested using AIIH to assign IPv4 Global Addresses to IPv6 hosts in general. Richard Draves and Jack McCann who have provided many helpful technical suggestions, and the NGTRANS working group for taking the time to work on AIIH.

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-dhcpv6-13.txt March 1998 (work in progress).

[5] C. Perkins. Extensions for the Dynamic host Configuration Protocol for IPv6. draft-ietf-dhc-dhcpv6ext-10.txt March 1998. (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 S vign Cedex
Phone : +33 2 99 12 70 26
Email : Laurent.Toutain@enst-bretagne.fr

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