Individual Submission
Internet-Draft
Expires: February 26, 2004

G. Huston
Telstra

August 28, 2003

Commentary on Distribution Mechanisms for Unique Local IPv6 Unicast Addresses
draft-huston-ipv6-local-use-comments-01.txt

Abstract

This memorandum examines the characteristics of Unique Local IPv6 Unicast addresses, as well as the requirements for address distribution mechanisms for this class of addresses. It is intended as a commentary on an Internet Draft currently under consideration in the IPv6 Working Group of the IETF.

Table of Contents

1. Introduction

Current work within the IETF IPv6 working includes the drafting of a proposal to define part of the IPv6 unicast address space for local use. This is currently IETF work in progress being considered by the IPv6 Working Group, documented in an Internet draft, "draft-ietf-ipv6-unique-local-addr-00.txt" [1]. These addresses are intended for various forms of local communications and are not expected to be routable on the global Internet. The proposal refers to such addresses as "Unique Local IPv6 Unicast Addresses".

There are a number of characteristics of such addresses that have been proposed in order to ensure that they can fulfill the role of a local-use address, and there are also a number of considerations relating to the distribution mechanisms for these addresses that distinguish them from globally routable unicast addresses. This document explores these intended characteristics in further detail as well as the associated distribution mechanisms.

2. Characteristics of Local Use Addresses

The characteristics listed in the draft proposal for such addresses are:

1. Globally unique prefix.
2. Well known prefix to allow for easy filtering at site boundaries.
3. Allows sites to be combined or privately interconnected without creating any address conflicts or require renumbering of interfaces using these prefixes.
4. Internet Service Provider independent and can be used for communications inside of a site without having any permanent or intermittent Internet connectivity.
5. If accidentally leaked outside of a site via routing or DNS, there is no conflict with any other addresses.
6. In practice, applications may treat these address like global scoped addresses.

It could be argued that, strictly, the third and fifth characteristics are a consequence of the first, as they can be all grouped under the overall characteristic of "use of a common unique

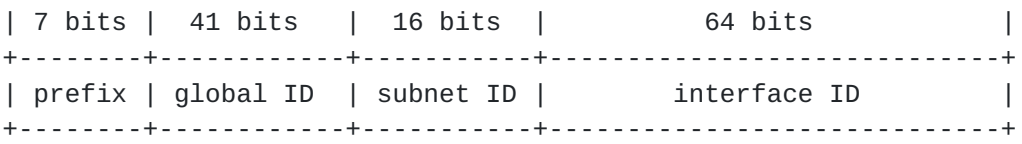
prefix". The second, forth and sixth characteristics commonly refer to unique use of a local address block drawn from the global unicast address pool.

Restating this list of characteristics gives:

1. Exclusive use of a common prefix drawn from the global unicast address space for all local use addresses.

2. Unique assignment of local use address blocks from within the pool of addresses defined by this prefix.

Section 3.1 of the Internet Draft proposal further refines the set of characteristics, by describing the address as a four part object:



where:

prefix: prefix to identify Local IPv6 unicast addresses. (FC00::/7)

global ID: global identifier used to create a globally unique prefix.

subnet ID: 16-bit subnet ID is an identifier of a subnet within the site.

interface ID: 64-bit Interface ID.

The length of the prefix + global ID part is 48 bits in length, allowing 16 bits for local assignation of subnet IDs and 64 bits for the interface ID. This allows for 2,199,023,255,552 assignable local use address blocks.

There is a further characteristic of the address block defined in this section of the draft, namely:

3. There is no internal structure within the global ID, and these global IDs cannot be aggregated in a routing context.

The proposal splits this address pool into two halves: locally and centrally assigned prefixes. These will be considered in the following sections.

3. Locally Assigned Global IDs

One half of the Local Use address space, using the common prefix FD00::/8, is described as being "locally assigned". The proposal indicates that such locally assigned global IDs must be generated with a pseudo-random algorithm. The proposal notes that there is a very low probability that the prefix will conflict with another locally generated prefix (section 11.2 of the draft proposal). Analysis of the probability involved here indicates that the probability of a collision in the space using a random draw function exceeds 0.5 after 1.24 million random draws. The general solution of the probability of a collision after d draws from n possible values is given by:

$$P = 1 - ((n!) / ((n^{**}d)((n-d)!)))$$

Given that the value for n is 2.199,023,255,552, then the objective is to find the lowest value of d for which P is greater than or equal to 0.5. In this case the value for d is some 1.24 million. This value is likely to be too small a value for any assured level of uniqueness, particularly if there is some consideration that no address conflicts would arise as a result of private interconnection. While the draft proposal asserts that collisions of locally assigned Global IDs "can be ignored for all practical purposes" (section 11.2), the actual probability of a clash is one where there will a probable clash after 1.24 mission random draws. If this approach is used on a widespread basis then the risk of clashing Global IDs is far greater that the "theoretical" risk described in the proposal. Some further consideration should be given to this part of the proposal.

It is observed that this 'random draw' is an inadequate response to item 2 of the required characteristics for Local Use addresses. A probability of uniqueness is tangibly different to the property of assured uniqueness. If assurred uniqueness is an essential characteristic of all elements of this address space, then it is necessary to drop the random self-selection mechanism from the draft proposal, and that all Local-Use addresses be distributed in such a manner that uniqueness is assured in every case.

4. Centrally Assigned Global IDs

The other half of the local use space is proposed in the draft to be "centrally assigned" using fixed size /48 blocks. This refines the second characteristic to read:

> 2. Unique assignment of fixed size local use address blocks from within the pool of addresses defined by this prefix, using a

Global ID as the block prefix.

The proposal notes that these assignments can be escrowed to resolve any disputes regarding duplicate assignments. It is noted that escrow is a specific solution to a more general characteristic, and the desired characteristic being defined here is:

4. The assignment information must be recorded and stored in a reliable manner.

The assignment function is described in the proposal as one that treats sequential allocations in a random fashion, and explicitly notes that they should not be assigned accordingly to any particular structure, and therefore they cannot be aggregated in a routing environment.

5. Local Use Addresses are not intended to be passed within the global routing environment

The complete list of characteristics of this Centrally Assigned Local Use IPv6 Unicast address space is:

1. Exclusive use of a common prefix drawn from the global unicast address space for all local use addresses.

2. Unique assignment of fixed size local use address blocks from within the pool of addresses defined by this prefix, using a Global ID as the block prefix.

3. There is no internal structure within the global ID, and these global IDs cannot be aggregated in a routing context.

4. The assignment information must be recorded and stored in a reliable manner.

5. Local Use Addresses are not intended to be passed within the global routing environment

The potential for use of this address in end-to-end solutions relating to multi-homing is limited to the extent that this identity space is unstructured, so it cannot be used as a lookup key in any mapping system that maps identities into locators. If the intended use is through a sequence of mappings from domain name to identifier to current locator, then the last mapping (from identifier to locator) is not feasible in an unstructured identifier space. In this sense the role of such an address is limited to an assertion of a

fixed, globally unique label that can be used in conjunction with dynamic change of location-based address to provide some form of transport session resiliency in a multi-homed environment.

5. Local Use Address Distribution Mechanisms

The proposal notes that:

> The requirements for centrally assigned global ID allocations are:
>
> * Available to anyone in an unbiased manner.
>
> * Permanent with no periodic fees.
>
> * One time non-refundable allocation fee in the order of 10 Euros per allocation.
>
> * The ownership of each individual allocation should be private, but should be escrowed.

The unstated implication from the first requirement is that this is undertaken without consideration of the current or intended level of use of the address block, so that there are no qualifications regarding assignment of a Local Use Address block. The proposal also notes that such availability should include non-Internet access mechanisms as a desired additional mechanism.

The second and third aspects of this proposed distribution mechanism describe the use of a one-time fee for a one-time service transaction that has enduring consequences.

5.1 Allocation Fees

The first aspect here is the consideration of the allocation fee. The draft motivates this payment as a means of prevention of hoarding of blocks from within this pool by imposing a financial impost. While there are many forms of control over a distribution mechanism to prevent distortions such as hoarding, this pricing approach is seen as a lightweight and effective mechanism that has the potential to address the identified problem. However, there are some consequences of this aspect of the draft proposal that should be examined in further detail. The imposition of a charge without relation to service cost is seen in many regulatory regimes as an imposition that is likened to a monopoly rental or a form of taxation. Such forms of charges have no valid role, and should be avoided. It is more reasonable to allow the operator(s) of this distribution mechanism to be able to account for their costs in operating this service, and allow the operator to determine a service fee that is based on these

costs.

The operator needs to consider that if this is to be a one-time fee for an unbounded service (so called 'cemetery plot' fees), the fee should cover both the processing component and the subsequent record maintenance component of the service.

5.2 Allocation Period

The proposal explicitly indicates that the allocation should be 'permanent'. This implies that there is no concept of return of a Local Use prefix once it has been allocated from the central registry, and that there is no concept of a registry-recorded transfer of an allocation. The implication of this service model is that there is no form of reuse of blocks from this address space. The implicit assumption here is that for the entire useful lifetime of the technology, under all conceivable allocation demand scenarios, that there will be adequate available address space to continue to meet demand from the Local Use address pool. Without any form of periodic renewal or similar opportunity to alter the terms of use of this address space then, if exhaustion of the space is considered to be a potential risk, the observations made in 1994 regarding the possible outcomes of the (then) IPv4 address allocation practices are once more relevant here:

> "It is perhaps a sad reflection of the conflict of short term objectives and longer term considerations that the evident short term motivations of ready and equitable access to the IPv4 address (which were the motivational factors in determining the current Internet address allocation policies) run the consequent risk of monopoly- based restrictive trade and barrier-based pricing as a longer term outcome of unallocated address space exhaustion." [2]

Of course if there is a high degree of confidence that exhaustion of the Local Use address pool is not a remotely possible eventuality, then such address prefixes can be considered in the same terms as a single-use disposable facility, and these considerations are not directly relevant.

5.3 Choice in Service Models

It is possible that clients of this allocation service want the choice between a single one-time permanent allocation (and a one-time service fee) and a defined period renewable service, where, at the end of the defined period the client has the choice of renewing the allocation or allowing it to lapse back to the pool. Given the central nature of the described distribution mechanism, allowing the client some choice in the form of service, rather than imposing a

single service model is seen as a reasonable measure.

The model also proposes a single layer of distribution, where end clients interact with a proposed single central registry. Again this is an area where a different structure used for the distribution of many other forms of goods or resources, typically using some form of hierarchy in distribution with wholesale and retail roles. Such hierarchies often allow for a more efficient form of overall distribution than a single entity attempting to service a global consumer base. Current regulatory environments also look to competition as a means of ensuring that service regimes operate efficiently and that no single player can distort the price of the service through the imposition of monopoly rentals, artificial scarcity or selective servicing.

5.4 Recording Allocations

The proposal indicates that information relating to the 'ownership' of each individual allocation be private. This is not an easily achieved outcome, given that 'ownership' is a public claim to the unique ability to access and exploit the resource. Furthermore, this implies that the resource itself is a form of property, and that property can be traded, swapped or otherwise disposed of at the discretion of the owner, inferring that the address block, is in some form, an asset of the holder. It is unclear that this interpretation of the status of an address is the actual intent of the proponents of this approach, and that other forms of expression of unique and enduring interest in the address resource may be more appropriate for this resource. This observation is made in the context of the characterization of the larger protocol address space as a public good that is distinguished from concepts of ownership or the inferring of aspects of property and asset into this resource.

5.5 Reverse Mapping Local Use Addresses in ip6.arpa

It is unclear from the proposal whether Local Use Addresses could or should be entered into the ip6.arpa reverse mapping domain space. as a delegated domain.

Locally assigned prefixes cannot be entered into this domain space because of the lack of a condition of assured uniqueness.

The situation with respect to centrally assigned prefixes is not so clear. The considerations include:

- The potential size of the domain zone. Because of the lack of any structure beyond the 8th bit of the prefix, there is no ability to impose a hierarchy of zone files, and the reverse zone would need

to list all assigned local use prefixes and their delegation points. There are obvious implications in terms of the potential size of this zone file. and some consideration as to the efficiency of operation of a zone of such a potential size.

- The desired characteristic of Local Use prefixes where the "ownership" of the prefix is not public information. If the domain zone operator was distinct from the central registry operator, then the privacy of the address allocation information could preclude the domain operator from validating a delegation request for a Local Use address block.

- The potential use of these addresses in some classes of end-point identification may imply the need for an external entity, using the global DNS to be map from the local use identifier to a global use address, and one way to perform this mapping in the DNS is to use the reverse domain to map from the end point local use address to a global DNS name, and then map forward from this name to a global address. Precluding local use addresses from the global DNS would preclude this form of mapping.

For local use, a so called "two-faced" DNS can be configured to provide a local reverse mapping service for the local site.

6. Management Requirements for Local Use Addresses

In summary, the characteristics of the management of this space is where:

1. Every applicant may obtain an address block in this prefix space without providing any form of justification to the registry operator.

2. Every assigned Local-Use block is of the same size, namely a /48.

3. Each block is uniquely assigned to the applicant.

4. Each assignment is a randomly selected block from the entire remaining pool.

5. Each applicant may obtain an enduring assignment without further need to contact the registry or to pay further service fees (one-off service).

6. Any service fee, if used, should be high enough to make massive seizure financially undesirable, yet low enough to make it readily accessible to individuals as well as corporate entities

on a global scale.

7. Any service fee, if used, should be clearly attributable to the costs associated with the provision of the service function for the lifetime of the provided service.

8. The service model is not restricted to a one-off assignment model, with the proviso that any other associated service models must have similar attributes of ease of accessibility.

9. The association of the assigned space and the identity of the applicant is not to be made public.

10. The assignment information is to be held in a way that is reliable and enduring.

7. Distribution Mechanisms

Under the current arrangements, IANA is the IETF-selected registry for IPv4 global unicast and IPv6 global unicast address space, and the RIRs undertake the associated distribution function, using policies that have been developed by an open process within each region.

A complete consideration of the various regulatory and logistical considerations is considered to be well beyond the appropriate scope of the Internet Engineering Task Force to undertake within the defined scope and mission, and a more general statement of intent would be more fitting in this context.

An enumeration of the desired attributes of a distribution system is:

The adopted distribution mechanism should be:

* efficient,

* fair,

* generally accessible and imposing no barrier to access,

* undertaken in a manner that preserves the desired characteristics of the Local Use address space,

* one that uses a fee structure that fairly reflects the costs of efficient service delivery mechanisms,

* one that allows a choice of service models where feasible,

* one that prevents distortions of the distribution function through behaviours such as hoarding or selective reselling,

* one that does not place the operator(s) in contravention to various regulatory frameworks, and

* attuned to the long-term stable use of specific instances of this resource by consumers

8. IANA Considerations

The Local Use Address draft proposes that:

> The IANA is instructed to allocate the FC00::/7 prefix for Unique Local IPv6 unicast addresses.
>
> The IANA is instructed to delegate, within a reasonable time, the prefix FC00::/8 to an allocation authority for Unique Local IPv6 Unicast prefixes of length /48. This allocation authority shall comply with the requirements described in section 3.2 of this document, including in particular the charging of a modest one-time fee, with any profit being used for the public good in connection with the Internet.

It is noted that there are significant problems with this proposed approach to directions to IANA, particularly with the noted concept that this is a for-profit activity and IANA is, in effect, being directed to be in the position of selecting a global monopoly operator. The indeterminate nature of a fair, open and reasonable definition of "the public good" is also a problem in the context of these instructions to IANA. Some of the lessons learned from DNS administration over the past decade would indicate that this is not a sensible directive to pass to IANA, as it is unlikely to be reasonably implemented in this precise form.

9. Relationship with Existing Address Distribution Mechanisms

The Local Use proposal's desire to operate the address space without any form of discernable structure by having all block assignments be drawn from a random selection from across the entire managed space precludes the reuse of the current distribution mechanism of an IANA allocation to each of the RIRs to service their particular region. In the context of assuming that the RIRs undertake this function, the proposed mechanism would see FD00::/8 allocated to the RIRs and managed via a single registry maintained by the RIRs working together. Each RIR would lodge a "draw request" for a block from this registry in response to individual customer requests, and the

registry would respond with the selected block, using a random draw function.

The potential areas of difference between the current RIR practice and the requirements here are:

- the absence of any form of justification for the allocation,
- a fixed size of allocation,
- the potential to make extensive use of automated mechanisms in the registry allocation function
- public reporting of allocations from this space only in summary form (no detailed reports, such as currently published via Whois servers)
- consideration of adoption of a service model or models relating to the terms of the assignment.
- consideration of various forms of renewable allocations and the issue of whether permanent allocations are suitable for this intended role.
- determining a fee schedule where the registry service is operated in a manner that is cost neutral to the membership.
- adoption of a transaction-based fee-for service model (as distinct from a membership service model)
- specific consideration relating to long term reliable storage of individual allocation information

In this context, if the RIRs were to develop this as a supported process, then the areas of RIR liaison with the IETF would appear to be in understanding the role of coordinated RIR policies in this area, and the role of the IETF. As an example, the nomination of a fee schedule and a service model in the draft proposal would normally seen as prescribing matters that would normally be determined by the RIRs through the adoption of policy proposals rather than a matter for the IETF to determine, while the consideration of permanent allocations would be a matter that would entail some substantive consideration by the IETF.

On a purely pragmatic level there is no practical way that the IETF or the adopted distribution mechanism can totally prevent these address prefixes from leaking into the IPv6 global routing space. What is, or is not, carried in the routing space is largely a matter

of convention from within the operator community. If the decision is taken not to publish the details of individual Local Use unique allocations, then this would be a factor in determining whether or not blocks drawn from this space may be carried in the global routing system, but it would not absolutely prevent such use.

The service model is again a relatively challenging concept. The original IPv4 address allocation system worked on a similar basis of enduring allocations, and this has proved to be problematic in terms of recovery of unused space in more recent times. While the draft proposal is explicit about attempting to prevent short term distortions such as hoarding, there is little doubt that any form of finite unmanaged resource will be placed under consumption pressures eventually. Attempting to set a global price that makes the resource generally accessible, while still attempting to make the price a deterrent to hoarding is not a completely reasonable exercise in global terms. What would be regarded as a trivially small fee within some economies would be seen as a prohibitively expensive price in other economies. More worryingly, the concept of an enduring assignment is that there is no opportunity to make any form of correction in later times to the extant assignments, and, as in IPv4, there is the distinct risk of giving early adopters a long term advantage that may not be enjoyed by later players who may be working under more restrictive allocation polices. A shorter term lease arrangement (such as 2 - 5 years) allows for regular renewal of the relationship with the registrar, allowing for assignment information to be updated to reflect the current state of the assignee, but would entail greater levels of registry activity. As this entire operation is intended to be sufficiently low in cost that it is generally accessible, and that the value here is not in routeable address space, but in the attribute of assurred uniqueness for the address space, the consideration of the level of registry activity is a critical one. It may be that the distribution mechanism adopts both service models, allowing an enduring application to be undertaken at any time at one fee level, and a shorter identity-validated application and renewal to be undertaken on a biannual basis at a lower fee, This is obviously a matter for further consideration.

10. Security Considerations

The considerations listed in the draft proposal are:

> Local IPv6 addresses do not provide any inherent security to the nodes that use them. They may be used with filters at site boundaries to keep Local IPv6 traffic inside of the site, but this is no more or less secure than filtering any other type of global IPv6 unicast addresses.

Local IPv6 addresses do allow for address-based security mechanisms, including IPSEC, across end to end VPN connections.

It is noted that in the latter case, where end to end VPN connections are being used, across local use address blocks there is a strong requirement for uniqueness of the Local Use address prefix.

11. Acknowledgements

The author acknowledges the helpful comments of Alain Durand, Paul Wilson, Anne Lord and George Michaelson in preparing this memo.

References

[1] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", Internet-Drafts draft-ietf-ipv6-unique-local-addr-00.txt, August 2003, <http://www.ietf.org/internet-drafts/draft-ietf-ipv6-unique-local-addr-00.txt>.

[2] Huston, G., "Observations on the Management of the Internet Address Space", RFC 1744, December 1994.

Author's Address

Geoff Huston
Telstra

Intellectual Property Statement

Full Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.