INTERNET-DRAFT   R. Hinden, Nokia
June 23, 2004   B. Haberman, Caspian

Centrally Assigned
Unique Local IPv6 Unicast Addresses

<draft-ietf-ipv6-ula-central-00.txt>

Status of this Memo

Abstract

   This document defines Centrally allocated IPv6 Unique Local
   addresses. These addresses are globally unique and are intended for
   local communications, usually inside of a site. They are not
   expected to be routable on the global Internet.

Table of Contents

1.0 Introduction

This document defines an Centrally allocated IPv6 unicast address
format that is globally unique and is intended for local
communications [IPV6]. These addresses are called Unique Local IPv6
Unicast Addresses and are abbreviated in this document as Local IPv6
addresses. They are not expected to be routable on the global
Internet. They are routable inside of a more limited area such as a
site. They may also be routed between a limited set of sites.

This document defines the characteristics and technical allocation
requirements for centrally assigned Local IPv6 addresses in the
framework defined in [ULA].

Local IPv6 unicast addresses, as defined in [ULA], have the following
characteristics:

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

This document defines the the characteristics and technical
allocation requirements for centrally assigned Local IPv6 addresses.

Topics that are general to all Local IPv6 address can be found in the
following sections of [ULA]:

    3.3 Scope Definition
    4.0 Routing
    5.0 Renumbering and Site Merging
    6.0 Site Border Router and Firewall Packet Filtering
    7.0 DNS Issues
    8.0 Application and Higher Level Protocol Issues
    9.0 Use of Local IPv6 Addresses for Local Communications
    10.0 Use of Local IPv6 Addresses with VPNs
    11.0 Advantages and Disadvantages

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
document are to be interpreted as described in [RFC 2119].

2.0 Acknowledgments

The underlying idea of creating Local IPv6 addresses described in
this document been proposed a number of times by a variety of people.
The authors of this draft do not claim exclusive credit. Credit goes
to Brian Carpenter, Christian Huitema, Aidan Williams, Andrew White,
Charlie Perkins, and many others. The authors would also like to
thank Brian Carpenter, Charlie Perkins, Harald Alvestrand, Keith
Moore, Margaret Wasserman, Shannon Behrens, Alan Beard, Hans Kruse,
Geoff Huston, Pekka Savola, Christian Huitema, and Tim Chown for
their comments and suggestions on this document.

3.0 Centrally Assigned Local IPv6 Unicast Addresses

3.1 Format

The Centrally assigned Local IPv6 addresses are created using a
pseudo-random global ID. They have the following format:

    | 8 bits | 40 bits | 16 bits | 64 bits |
    +--------+------------+-----------+------------------------------+
    | prefix | global ID | subnet ID | interface ID |
    +--------+------------+-----------+------------------------------+

Where:

     prefix   FC00::/8 prefix to identify centrally assigned
                         Local IPv6 unicast addresses.

     global ID   40-bit global identifier used to create a
                         globally unique prefix. See section 3.2 for
                         additional information.

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

     interface ID   64-bit interface ID as defined in [ADDARCH].

3.2 Global ID

   The allocation of global IDs should be pseudo-random [RANDOM].   They
   should not be assigned sequentially or with well known numbers.   This
   is to ensure that there is not any relationship between allocations
   and to help clarify that these prefixes are not intended to be routed
   globally.   Specifically, these prefixes are designed to not
   aggregate.

   The major difference between the locally assigned Unique local
   addresses as defined in [ULA] and the centrally assigned local
   addresses defined in this document is that they are uniquely assigned
   and the assignments can be escrowed to resolve any disputes regarding
   duplicate assignments.

   It is expected that large managed sites will prefer central
   assignments and small or disconnected sites will prefer local
   assignments.   It is recommended that sites planning to use Local IPv6
   addresses for extensive inter-site communication, initially or as a
   future possibility, use a centrally assigned prefix as there is no
   possibility of assignment conflicts.   Sites are free to choose either
   approach.

3.2.1 Centrally Assigned Global IDs

   Centrally assigned global IDs MUST be generated with a pseudo-random
   algorithm consistent with [RANDOM].   They should not be assigned
   sequentially or by locality.   This is to ensure that there is no
   relationship between allocations and to help clarify that these
   prefixes are not intended to be routed globally by eliminating the
   possibility of aggregation.   Specifically, these prefixes are
   designed to not aggregate.

   Global IDs should be assigned under the authority of a single

   allocation organization because they are pseudo-random and without
   any structure. This is easiest to accomplish if there is a single
   authority for the assignments.

   The requirements for centrally assigned global ID allocations are:

     - Available to anyone in an unbiased manner.
     - Permanent with no periodic fees.
     - Allocation on a permanent basis, without any need for renewal
       and without any procedure for de-allocation.
     - Provide mechanisms that prevent hoarding of these allocations.
     - The ownership of each individual allocation should be private,
       but should be escrowed.

   The allocation authority should permit allocations to be obtained
   without having any sort of Internet connectivity. For example in
   addition to web based registration they should support some methods
   like telephone, postal mail, fax, etc.

   The allocation service should include sufficient provisions to avoid
   hoarding of numbers. This can be accomplished by various ways, for
   example, requiring an exchange of documents, a verbal contact, or a
   proof that the request is on behalf of a human rather than a machine.
   The service may charge a small fee in order to cover its costs, but
   the fee should be low enough to not create a barrier to anyone
   needing one. The precise mechanisms should be decided by the
   registration authority.

   The ownership of the allocations is not needed to be public since the
   resulting addresses are intended to be used for local communication.
   It is escrowed to ensure there are no duplicate allocations and in
   case it is needed in the future (e.g., to resolve duplicate
   allocation disputes, or to support a change of the central allocation
   authority).

   Note, there are many possible ways of of creating an allocation
   authority. It is important to keep in mind when reviewing
   alternatives that the goal is to pick one that can do the job. It
   doesn't have to be perfect, only good enough to do the job at hand.

   This document directs the IANA, in section 5.0, to delegate the
   FC00::/8 prefix to an allocation authority to allocate centrally
   assigned /48 prefixes consistent with the requirements defined in
   this section.

3.2.2 Sample Code for Pseudo-Random Global ID Algorithm

The algorithm described below is intended to be used for centrally
assigned Global IDs. In each case the resulting global ID will be
used in the appropriate prefix as defined in section 3.2.

  1) Obtain the current time of day in 64-bit NTP format [NTP].
  2) Obtain an EUI-64 identifier from the system running this
     algorithm. If an EUI-64 does not exist, one can be created from
     a 48-bit MAC address as specified in [ADDARCH]. If an EUI-64
     cannot be obtained or created, a suitably unique identifier,
     local to the node, should be used (e.g. system serial number).
  3) Concatenate the time of day with the system-specific identifier
     creating a key.
  4) Compute an MD5 digest on the key as specified in [MD5DIG].
  5) Use the least significant 40 bits as the Global ID.
  6) Verify that the computed global ID is not in the escrow. If it
     is, discard the value and rerun the algorithm.

This algorithm will result in a global ID that is unique and can be
used as a Global ID.

4.0 Security Considerations

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.

5.0 IANA Considerations

The IANA is instructed to assign the FC00::/8 prefix for Centrally
assigned 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 allocation on a permanent basis and
with sufficient provisions to avoid hoarding of numbers. If deemed
appropriate, the authority may also consist of multiple organizations
performing the authority duties.

6.0 **References**

6.1 **Normative References**

[ADDARCH] Hinden, R., S. Deering, S., "IP Version 6 Addressing
          Architecture", RFC 3515, April 2003.

[GLOBAL] Hinden, R., S. Deering, E. Nordmark, "IPv6 Global Unicast
          Address Format", RFC 3587, August 2003.

[ICMPV6] Conta, A., S. Deering, "Internet Control Message Protocol
          (ICMPv6) for the Internet Protocol Version 6 (IPv6)
          Specification", RFC2463, December 1998.

[IPV6]   Deering, S., R. Hinden, "Internet Protocol, Version 6
          (IPv6) Specification", RFC 2460, December 1998.

[MD5DIG] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321,
          April 1992.

[NTP]   Mills, David L., "Network Time Protocol (Version 3)
          Specification, Implementation and Analysis", RFC 1305,
          March 1992.

[POPUL]   Population Reference Bureau, "World Population Data Sheet
          of the Population Reference Bureau 2002", August 2002.

[RANDOM] Eastlake, D. 3rd, S. Crocker, J. Schiller, "Randomness
          Recommendations for Security", RFC 1750, December 1994.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
          Requirement Levels", RFC 2119, BCP14, March 1997.

[ULA]   Hinden, R., B. Haberman, "Unique Local IPv6 Unicast
          Addresses", Internet Draft <draft-ietf-ipv6-unique-local-
          addr-05.txt>, June 2004.

6.2 **Informative References**

[ADDAUTO] Thomson, S., T. Narten, "IPv6 Stateless Address
          Autoconfiguration", RFC 2462, December 1998.

[ADDSEL] Draves, R., "Default Address Selection for Internet
          Protocol version 6 (IPv6)", RFC 3484, February 2003.

   [DHCP6]   Droms, R., et. al., "Dynamic Host Configuration Protocol
              for IPv6 (DHCPv6)", RFC3315, July 2003.

   [RTP]   Schulzrinne, H., S. Casner, R. Frederick, V. Jacobson,
              "RTP: A Transport Protocol for Real-Time Applications"
              RFC3550, July 2003.

7.0 Authors' Addresses

   Robert M. Hinden
   Nokia
   313 Fairchild Drive
   Mountain View, CA 94043
   USA

   phone: +1 650 625-2004
   email: bob.hinden@nokia.com

   Brian Haberman
   Caspian Networks
   1 Park Drive, Suite 300
   Research Triangle Park, NC 27709
   USA

   phone: +1-929-949-4828
   email: brian@innovationslab.net

8.0 **Change Log**

   Draft <draft-hinden-ipv6-global-local-addr-00.txt>

      o Initial Draft created from [ULA]. This draft defines the
        centrally assigned Local IPv6 addresses.