Guidance of Using Unique Local Addresses

draft-liu-v6ops-ula-usage-analysis-05

Bing Liu(speaker), Sheng Jiang, Cameron Byrne

IETF 86@Orlando, Mar 2013

Purposes of this draft

- Supplement to RFC4193 (ULA definition)
- Discussing ULA usage scenarios, making recommendations of some general/specific cases where could be benefit of adopting ULA
- Eliminating/preventing misunderstanding of ULA = RFC1918v6

✓ *migrating some successful practice/designs of RFC1918 to ULA in IPv6 is valid*

✓ *But never mapping RFC1918+NAT to ULA+NAT as default*

General Scenarios Analysis 1/3

- **Using ULA in isolated networks (Recommended in this draft)**
- Independent automatic generated address space without acquiring RIRs/LIRs
- Extremely low probability of collision when merged (section 3.2.3 in RFC4193)
- Compatible with adding global connectivity in the future
- Supporting multiple subnets

General Scenarios Analysis 2/3

- **ULA aside Global PA addresses (Recommended in this draft,** also regarding draft-ietf-v6ops-enterprise-incremental-ipv6**)**
- Configuring multiple addresses per interface, PA for global communication and ULA for local.
- A big advantage and difference to RFC1918, by utilizing multi-addresses-per-interface feature of IPv6
- Enabling stable local communications
- ✓ *internal-only nodes could be configured with ULA-only to avoid renumbering;*
- ✓ *When PAs renumbered, the separated local communications remain stable (recommended by RFC6879-IPv6 enterprise renumbering scenarios)*
- RFC6724 default address selection policy already support ULA

General Scenarios Analysis 3/3

ULA + Proxy

- Some information security sensitive networks, the endpoints are default disconnected and need the proxies to connect for central control.
- A common deployment model in IPv4 (RFC1918+proxies)
- It is natural to pick ULA in IPv6.

ULA + NPTv6

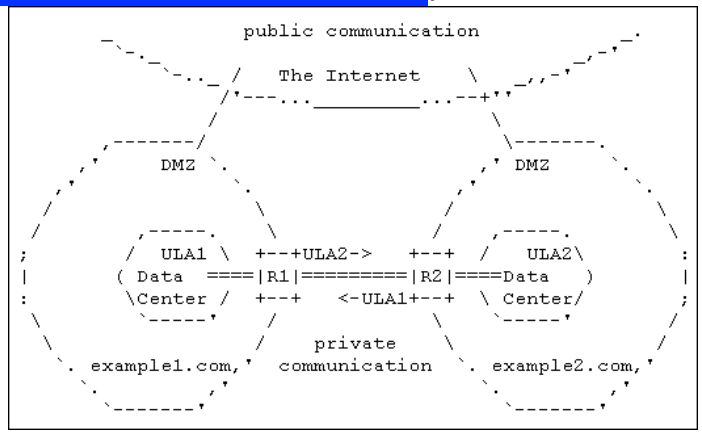
- Those who want independent address space without acquiring PI, can deploy this
- In NPTv6 specification (RFC6296), ULA+NPTv6 is also recoganized as a valid use case

(also regarding draft-ietf-v6ops-enterprise-incremental-ipv6)

Recommended Special Use Cases

- NAT64 pref64
  - ✓ *ensures that only local systems can use the translation resources of the nat64*
  - ✓ *helps clearly identify traffic that is locally contained*
- Upper layer identifier
  - ✓ *IPv6-compliant, easy to be grabbed from the stack*
  - ✓ *(quasi)uniqueness to avoid collision in most of the cases*
  - ✓ *assigned to the interface, stable and no need for the application to restore it*
  - ✓ *RFC6281 is one good example*
  - ✓ *But need to consider privacy issues*
- Private routing between two mutual trust sites

  (draft-baker-v6ops-b2b-private-routing)



A useful document? Adoption?

Thank you!

Backup Slides

ULA+NPTv6

- For IPv6 NAT, IETF already has opinions in RFC5902 (details in the next slide), so might not necessary to revisit it again in this specific draft
- For NPTv6, it is “a mechanism that has fewer architectural problems than merely implementing a traditional stateful Network Address Translator in an IPv6 environment. [RFC6296]” and recognized ULA +NPTv6 as a valid use case
- It is a necessary discussion of the proper ULA+NPTv6 use in this draft. Referring above points is sufficient for NAT/NPTv6 considerations in this specific ULA draft.

RFC5902 Summary

- “At present, the primary benefits one may receive from deploying NAT appear to be avoiding renumbering, facilitating multihoming without impacting routing scalability, and making edge consumer network configurations homogenous.” [RFC5902]
- In section 4, it discussed solution space for renumbering and multihoming without NAT. But they are not perfect, e.g. routing scalability issue of PI.
- That is to say, we do have other way to solve the problems, but it may also bring us other issues. In RFC5902, the IETF prefers working on the other ways by considering E2E transparency as the higher priority.

draft-ietf-v6ops-enterprise-incremental-ipv6

- “If using ULAs instead of Globally Unique Addressing for hosts, note that Network Prefix Translation will be required [RFC6296] for Internet based communication; the implications of which must be well understood before deploying. “
- “The use of ULAs may provide additional flexibility when an enterprise is using PA space, by providing an independent local prefix for internal use, while using the PA prefix externally in conjunction with NPTv6 [RFC6296].”

GUA in Isolated Networks

Some may argue that, since the network is isolated, arbitrarily picking a GUA range (without acquiring it from LIR/RIR) is also applicable. But please considering the following situations:

- ✓ *Some a node in the isolated network might move out to the Internet*
- ✓ *The isolated network might be added a global prefix to connect to the Internet in the future*
- ✓ *Different isolated networks merging*

Security Implication

- ULA itself doesn't contain any inner security features
- It is controversy whether ULA could benefit security designs/policies

✓ *A: It's a lot easier to filter/protect against a well known contiguous range*

✓ *Counter-A: There is no benefit to the range being well know outside of the filtering domain. A /48 carved out of one's GUA would serve equally well to a /48 from ULA.*

RFC6724 (default address selection) already supported ULA

- default policy table

Prefix	Precedence	Label
::1/128	50	0
::/0	40	1
::ffff:0:0/96	35	4
2002::/16	30	2
2001::/32	5	5
fc00::/7	3	13
::/96	1	3
fec0::/10	1	11
3ffe::/16	1	12