

IPv6 Unique Local Addresses: The Rant

Ted Hardie

What are ULAs?

- A way of permanently embedding routing policy in part of the unicast address range for IPv6
 - An opportunity for the Team Cymru bogon list to add a couple trillion /48s, give or take
 - A chance for folks who really enjoyed the happy times they had configuring RFC 1918 addresses and NATS to retain those joys into IPv6-land.
 - Basically, ULA is a TLA that decomposes into “Tragedy of the Commons”
-
-

No, really, what are ULAs?

- RFC 4913 sets aside FC00::/7 as a common prefix for unicast IPv6 addresses you can make up for yourself. There is a pseudo-random function provided, to avoid collisions. Chances of collision:

Connections	Probability
2	1.81×10^{-12}
10	4.54×10^{-11}
100	4.54×10^{-09}
1000	4.54×10^{-07}
10000	4.54×10^{-05}

- There are just a bit over 2 trillion /48s in the ULA /7. Half is used in the psuedo-random scheme. The other half is set aside for later specification.
-
-

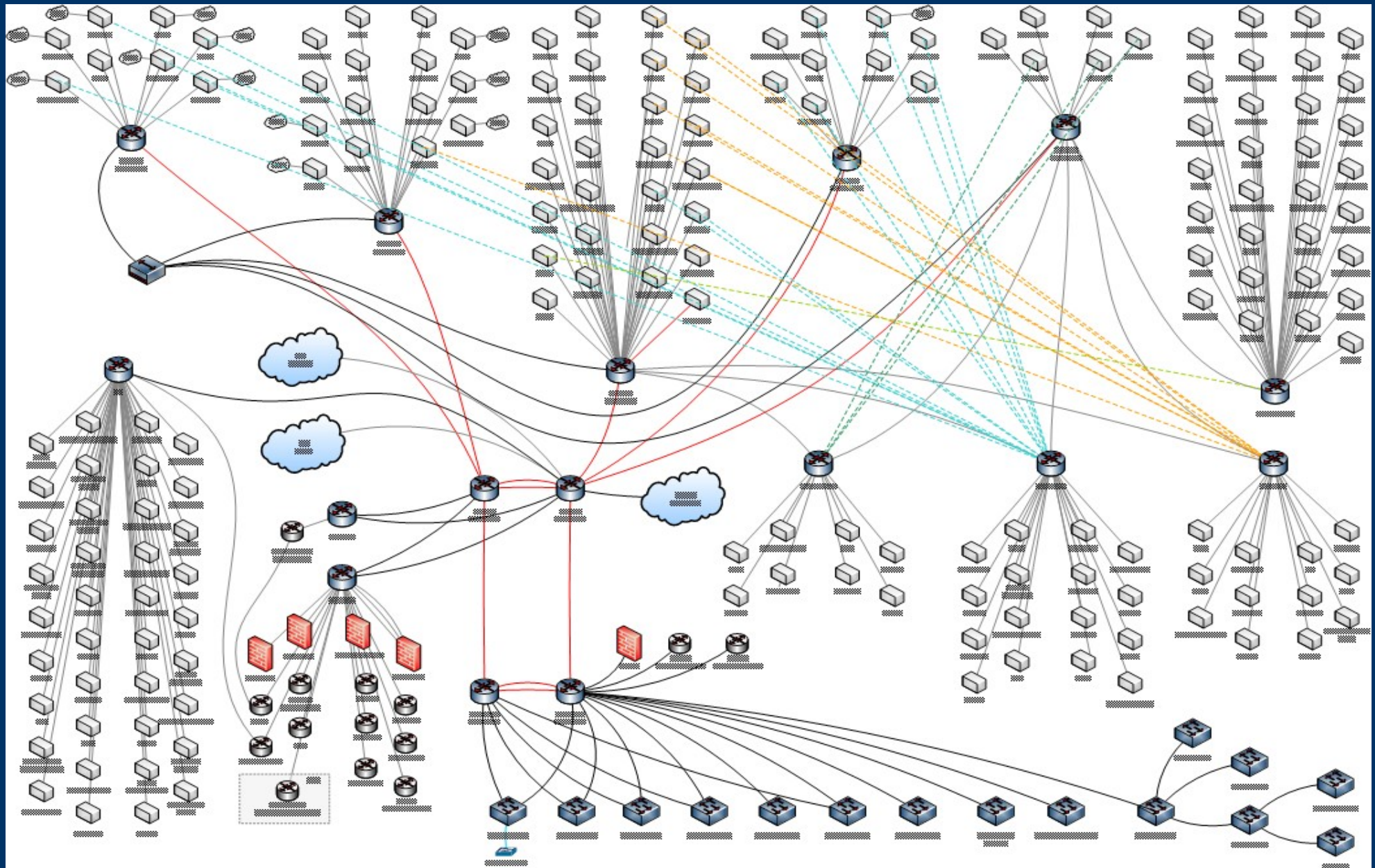
Why addresses you make up for yourself: some ancient history.

- The original IPv6 addressing architecture (RFC 1884) defined two types of local use unicast addresses: link-local and site-local. Link local was for links without a router and site-local for:
“sites or organizations that are not (yet) connected to the global Internet. They do not need to request or "steal" an address prefix from the global Internet address space. IPv6 site-local addresses can be used instead. When the organization connects to the global Internet, it can then form global addresses by replacing the site-local prefix with a subscriber prefix.”
 - Site-local stayed in RFC 2373 and 3513, but changed from a prefix for disconnected sites to one used above the link and below the Internet.
-
-

Since you have 128 bits of addresses, why not use more than one?

- A core assumption in modern v6 is that there are commonly multiple addresses associated with a physical interface. Link and global make sense.
 - “site” in the v6 architecture has never been well defined. There were years of arguments over it that just churned.
 - There is no necessary relationship between a “site” and anything in the routing system. The “site” is a latchkey child that resulted from a divorce between routing and addressing. That means whatever you define a site to be is arbitrary requires a lot of administrative work to maintain.
-
-

Ratemynetworkdiagram.com site



Site-local got killed, slowly

- The pain of RFC 1918 addresses convinced applications and operations folks that site-local was a bad, bad notion. After a lot of heated debate, plenary argument, appeals, and escalations, they won the argument inside the IETF and site-local was killed in RFC 3879.
 - 3879 identified several kinds of site-local pain: ambiguity & scope identifiers for applications; leakage for operators; complexity for routers.
 - The IPv6 folks were told to go back and try again.
 - ULAs are the result.
-
-

ULA: Son of site-local

- This design fixes one thing: ambiguity.
 - Fixing the ambiguity created some serious scope creep, though. Where “site-local” was theoretically filtered at the border of whatever a site meant, ULAs are now defined to allow interconnect among sites, as long as the routes to do so don't traverse the public Internet.
 - In other words, this ties a routing policy to a portion of the address space which is otherwise indistinguishable from the global scope.
-
-

In other other words, ULAs=PI space

- ULAs are “provider independent” at a very basic level—you generate them yourself, rather than getting them from an upstream or RIR.
 - They are not PI space in the sense we usually mean, in that holders of ULAs theoretically do not have the ability to announce these or implement their own routing policies.
 - But the only thing keeping them from being “PI space” in both senses is upstreams' unwillingness to announce these /48s into the IPv6 DFZ.
-
-

Why should you be unwilling?

- Because you don't want to accept other folks' announcements of ULAs. There is no policy check here. Once the dam breaks, your competitor can sell your routing slot for one at whatever price he wants, and tragedy of the commons pricing will hurt everyone, fast. Eaten any good cod, lately?
 - Even if you're getting a cut, this is a bad choice as ULAs can't ever be aggregated. Current ARIN PI policy has a minimum direct assignment of /48, but out of blocks reserved up to /44.
 - For connected sites, ULAs are mostly in addition to global addresses. Adding interface addresses hurts applications. See ICE for a scary example.
-
-

Conclusion:

- ULAs are globally unique unicast addresses with a built-in routing policy. There is nothing you can do with them that you can't do with normal global-scope addresses and your own policies.
 - What you should do:
 - Disallow FC00::/7 from peers now.
 - Discourage any customers you have from using it. Show them how to split their global address space into routed and unrouted if you need to.
 - Tell them you will filter ULAs if they are announced to you, and do so.
 - Praise your local RIR for having PI space for customers available under known policies.
-
-

Is there anything good about ULAs?

- You can generate a ULA and list it in your posts to Digg, Fark, or Slashdot without causing heartburn for Jay Adelson, Drew Curtis, or CmdrTaco.
 - Reading one aloud is less likely to hurt your vocal cords than an actual ululation.
 - Breaking open a package covered by one does not limit anyone's liability, extend anyone's copyright, or constitute an agreement to sell your soul at a discount price.
 - That's about it.
-
-