Use of /127 IPv6 Prefix Length on P2P Links Not Considered Harmful

draft-kohno-ipv6-prefixlen-p2p-00.txt

Miya Kohno, Juniper Networks, Keio Univ.
Becca Nitzan, Juniper Networks
Randy Bush, IIJ
Yoshinobu Matsuzaki, IIJ

With contributions from
Pekka Savola, Netcore and Chris Morrow, Google
Background

• As technologies get deployed, we sometimes find a variance between the spec and reality

• From a security perspective, /127 for IPv6 p2p links is useful in practice

  – Yoshinobu Matsuzaki @IIJ, APNIC26 (August 2008)

  – Lorenzo Colitti & Angus Lees @Google, IETF72 IPv6 plenary (July 2008)
Why /127 was regarded as harmful?

- RFC4291 says unicast address Interface IDs are required to be 64 bits long.
- It also defines Subnet-Router anycast address, which is intended to be used to communicate with any one set of routers.
- RFC3627 indicated that the use of /127 was harmful, based on the condition that Subnet-Router anycast address was a mandatory requirement (/127 conflicts with the Subnet-Router anycast addressing).
The reality

- Subnet-Router anycast is not useful, nor is it widely deployed.
- RFC4443 fix for ping-pong is not widely deployed.
- /64 leaves huge unused space for p2p links.
Rationales for using /127

• How to avoid pingpong issues
  – 1. use link-local only
  – 2. with messy access filter
  – 3. rfc4443
  – 4. use /127 for the p2p links

Rationales for using /127 (and other long prefixes)

• With the use of /127, the interface IDs are simpler and easier to remember (e.g., the Interface ID is 1 or 0).

• Though address space conservation doesn't carry much weight today in the case of IPv6, it may be desirable to use the minimum amount needed.

• Considering that the IPv4 "Darknet" is drawing a lot of malware traffic [RFC4948], it is safer to narrow down the unused space.
Goal of the draft

• If it is meaningful and useful to treat particular link types differently, operators should be free to make this determination as assign suitable prefix length, e.g. /127
Appendix

- Neighbor Discovery [RFC4861] and SLAAC [RFC4862] can be a point of vulnerability as mentioned in [RFC3756], therefore, it MAY be safer to disable them when they are not required.