Passive IP Addresses

draft-baker-opsec-passive-ip-address

Problem

- It is possible to use a traceroute to identify routers on a path
  - More generally, ICMP and other traffic from routers identifies them to equipment that has no primary need to know
  - As a result, such equipment is subject to attacks

Principle of Least Privilege

- Folks that have **no need to know** something shouldn’t know it.

Possible solutions

- draft-behringer-lla-only
  - Use only link-local addresses
  - Send ICMP from the loopback address
  - But now I can attack the loopback address
- Use a ULA
  - BCP 38 issue – PMTU fails

Desirements

- I’d like to say “requirements”
- It would be nice to be able to have a remote network identify which operator to ask a question of
- Router addresses SHOULD be in ipv6.arpa
- It would be nice to have a way to not attack the router so identified

Passive IPv6 Addresses

- Two attributes on an interface address:
  - Should I respond using it in ICMP?
  - Should I process messages sent to it?
- An address that I send to folks who have no need to know my address “should be used” and “should not be processed”
- An address my operator uses to manage me “should not be used” and “should be processed”

"That's all Folks!"