draft-yourtchenko-opsec-humansafe-ipv6

Human-Safe IPv6

cryptographic transformation of hostnames

for secure and manageable addressing

{ayourtch,sasad}@cisco.com
mircea.pisica@bt.com

Background

- IPv6 addresses are unbearably long
- People can not pronounce them, let alone remember
  - (Test: 2001:db8:123:123:7804:66ff:23cd:1d4e)
- People use simple addressing schemes
  - 2001:db8::53, 2001:db8::80
  - 2001:db8::192.168.1.1

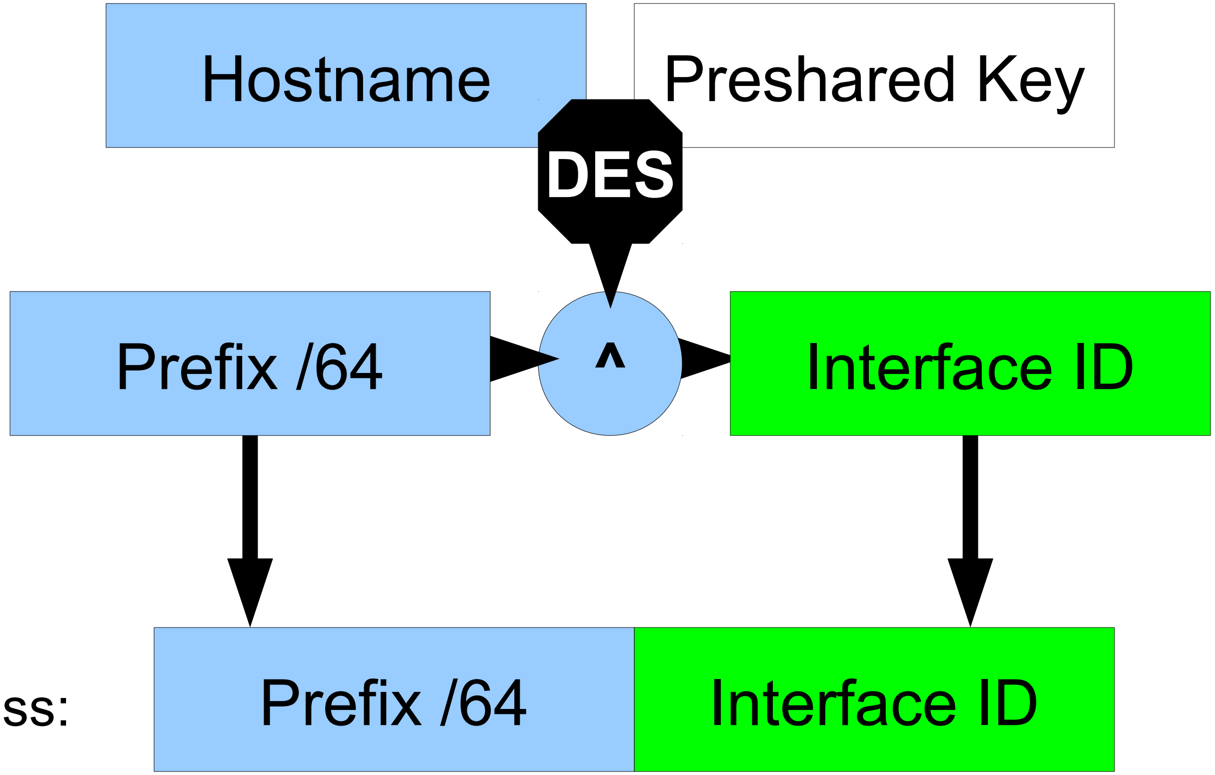
64-bit subnets space becomes much easier to map remotely

Problem: conflicting goals

- Need to **increase the randomness** in interface ID as much as possible (to protect from scanning)
- Need to **decrease the randomness** in interface ID as much as possible (to protect from brain explosion)

Proposal

- InterfaceID = encrypt(hostname8char, key) ^ prefix



- Address:

Example

- Prefix 2001:db8:123:123::/64
- Hostname: “mailhost”
- Preshared key: “cisco123”
- Address: 2001:db8:123:123:7804:66ff:23cd:1d4e
  - This is the hard to remember address from the slide#2 !

Properties

- Random Interface ID
- NOC staff can know hostname based on address
  - (not FQDN, so no, we're not reinventing DNS)
- Error protection

- Non-NOC can know hostname based on address, if they know the preshared key
  - The target is blind remote attackers => the assumption is it will be hard for them.

Scope of applicability

- Does NOT replace any of the existing mechanisms
- Servers / Routers (= static addresses)
- Link-local only environments
  - Hostnames in the routing table for next hops

Next steps

- Try the code (yes, the -00 draft has the running code!)
- Comments
- Adopt as a WG item