Tunnel End-point Discovery (anycast perspective)

draft-palet-v6ops-tun-auto-disc-03.txt

IPv6-in-IPv4 TEP Discovery

- Is this something we absolutely have to provide?
  - A different discussion..
- Scope of the Discovery
  - Only in network of the ISP where the user attaches to
    - "Third party" discovery is out of scope
- Assumptions
  - Must work through a (non-upgraded) NAT/router
  - The user may have his own NAT/router box(es)
  - IP addresses may be private and/or dynamic
- Main solution candidates
  - Well-known unicast address ("anycast") for initial discovery
  - DNS (in forward or reverse tree)

TEP discovery - anycast

- Main properties
  - Well-known v4 unicast address ("anycast")
  - Only for initial discovery of the "real" unicast address
    - Only the first packet of the discovery would be sent to the anycast address
    - I.e., no state to be kept between packets, comparable to DNS w/ UDP
  - Typically only internal to the ISP
    - Often would not be advertised in eBGP
  - As specified in draft-ietf-mboned-auto-multicast-04.txt (sect 5.[12])

TEP discovery - anycast (2/2)

- Advantages
  - Works through NATs, etc. very well
  - Seems to work based on DNS root anycast and 6to4 anycast
- Disadvantages
  - ISPs need to be careful in filtering the prefix to prevent hijacks
    - Applies to those ISPs who provide the service
  - Routing operations may be more difficult e.g. in enterprises than changing DNS
- Discussion
  - Issue: the security of the discovery process is weak
    - The client has no means of verifying whose advertisement is active
    - In other mechanisms, the discovery could in theory be secured e.g. with DNSSEC
    - But even with DNSSEC or manual config the validity of the endpoint is not guaranteed (route hijacks, misconfiguration etc.)
    - The correct way to deal with the security is IMHO at the configuration protocol itself
    - Though in discovery there need to be methods to mitigate the problems

TEP Discovery - Summary/Discussion

- What's left?
  - Well-known unicast address
  - [Reverse DNS prepopulation]
  - Manual configuration.. (obviously)
- Comments from grow community especially on:
  - Do you have concerns about using anycast for discovery?
  - The first reply to discovery needs to come from the anycast address
    - (For NAT traversal) -- is that an issue?