Mapping of Address and Port using Translation (MAP-T). Draft -03

2013-07-30

Main changes since last draft

- Number of editorial changes/additions:
  - Use of consistent terminology (Rule, Rule set, etc)
  - Easier reading (reversed order of Section 5)
  - “Easier” math (eliminated p variable by substitution)
  - Correction of ICMPv6 handling (previous text cited encapsulation)

Discussion

- Added Section 12 – Security Considerations text on ICMP Flood (following mailing list exchange):
  - *ICMP Flood: Given the necessity to process and translate ICMP and ICMPv6 messages by the BR and CE nodes, a foreseeable attack vector is that of a flood of such messages leading to a saturation of the nodes' compute resources. This attack vector is not specific to MAP, and its mitigation lies a combination of policing the rate of ICMP messages, policing the rate at which such messages can get processed by the MAP nodes, and of course identifying and blocking off the source(s) of such traffic.*

Next steps

- Draft is ready for WG last call.

More references

- MAP Testing Results
  - https://datatracker.ietf.org/doc/draft-xli-softwire-map-testing/
- Experience from MAP-T Testing
  - https://datatracker.ietf.org/doc/draft-cordeiro-softwire-experience-mapt/
- Uses cases for MAP-T
  - https://datatracker.ietf.org/doc/draft-maglione-softwire-map-t-scenarios/
- Experience from Double Translation and Encapsulation (MAP) Testing
  - https://datatracker.ietf.org/doc/draft-liu-softwire-experience-map/