Large Scale NAT Requirements

https://datatracker.ietf.org/doc/draft-ietf-behave-lsn-requirements/

and https://datatracker.ietf.org/doc/draft-shirasaki-nat444/

I. Yamagata, Y. Shirasaki, and S. Miyakawa (NTT Communications)
J. Yamaguchi (IIJ), A. Nakagawa (JPIX), H. Ashida (ITSCOM)

IETF79 @ Beijing, China
2010 November
LSN requirements

• became BEHAVE WG draft at IETF78th
  – Now the name has been changed from draft-nishitani-cgn to draft-behave-lsn-requirements

• recent changes
  – delete some requirements which are included in RFCs already exist
  – add requirements which comply with RFC4787, RFC5382 and RFC5508
Comments from ML and/or off-line

- However we do not want to change the name so often to avoid confusions and misunderstandings,
  - Large Scale NAT(LSN) → What name is good?
    - We’d like to point out the COMMON PART of the NAT444, DS-LITE and so on which essentially a NAT which provide multiple entity (users, organizations and/or subscribers…) with fair connections
    - Some people said that it must not be Large. Dave suggested to me use the word “multi entity”… fmmm
    - Of course, if so, CPE -> Entity

- How do you think?
  - Can we use (and settled down) its name as Multi Entity NAT(MEN) ?????
    - MEN + NAT at CPE -> NAT444
    - MEN + v4 over v6 Tunnel -> DS-Lite
Con’t

• Which means that Draft’s title and many text in I-D should use this term
  – Requirements for Multi Entity NAT

• Also all the related text must use MEN to express the notion
High availability

- written in “NAT Redundancy Requirements and Framework”
- We think to merge or refer in our draft
- We think high-availability is not always necessary. So “SHOULD” is appropriated (or keep separated draft, maybe)

- We’d like to know about how WG feel?
NAT translation log

• written in some drafts about port assignment and logging
  – Issues with IP Address Sharing
  – NAT44 with Pre-allcoated Ports
  – Port Management To Reduce Logging In Large-Scale NATs
  – Logging recommendations for Internet facing servers
    And more…

• Should we create another text about logging or not?
  – If so, we could delete the portion describing how to assign address/port (maybe) and what LSN(or MEN) logs from our draft and create references to the dedicated text

• We’d like to know how we should do?
Session limitations

• We have already discussed about the maximum speed of the creation of the new TCP sessions at LSN

• We also may need to discussed about the speed for UDP and ICMP as well

• We think so too but how about this?
About over subscription

• At least, we must guarantee the numbers of the ports (or sessions) which are assigned to each CPE (or “entity”).

• Then, we could allow over subscription or to reduce the log cost, we may not allow do so in some case.

• We should know a good text for this
Port Randomizations

• Should LSN use randomized source port towards outside? Or statically assigned port?

• We believe that
  – Randomized Source Port is good for security
  – But that increases log

• How do you think this too?
Enforcement of some BEHAVE RFCs

• We agree with that RFC4787, 5382, 5508 (mostly about transparent)
  – SHOULD -> MUST

• Or should not we do so?
And others?

• Please provide us with your comments on the mailing list so that we can achieve better text for next IETF meeting

• We’d like to finish the text by next IETF and will ask the last call at Prague
(optional) NAT444

• Still we’d like to have some text describing what the NAT444 model is
  – Double NAT NW model of MEN(LSN) and CPE
• Please allow us to create the I-D as WG ID or should we work on this in other area?
We have no strong opinion for now 😊