Large-Scale(Carrier Grade) NAT Requirements

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

IETF80 @ Prague, Czech
2011 March
CGN draft update

• Update(00⇒01) : followed Chairs’ recommendations mostly
  – An editor joined to the authors, Thanks !
    • Simon Perreault at Viagenie
  – Changed terminology from LSN to CGN
  – removed some REQs duplicated from other RFCs
  – Added “bulk port allocation” (or “bin”)
• We’d like to have the last-call as soon as possible toward RFC
Comments and questions

• After update, we have some comments and questions about CGN from ML
  – PCP support
  – Spam filter
  – High Availability
  – Blacklisting for private IP
  – Bandwidth fair-usage
  – Port static allocation
  – Configurable hold-down timer

...
Policy of CGN draft

• Our goal is only the basic requirements which are Fairness among the users
Dan’s comment on the scoping from ML

• The general theme for the document is that the CGN should be "fair".
  – That was the reason for the initial CGN-specific requirement which is that a subscriber be limited to a certain number of IPv4 ports -- to prevent one user from denying service to other legitimate users.

• Dave and I have discussed the organization of the document in the past, and the following two tenets seem pretty valuable in scoping the document:

• if a requirement is specific to a Carrier Grade NAT, it should be a new requirement in the document. For example, restricting a user to a certain number of ports.

• if a requirement is not specific to a Carrier Grade NAT, it should not be a _new_ requirement in the document. Instead, the document should reference an existing requirement. For example, the TCP behavior of a CGN can be described by BEHAVE's existing TCP behavior document, RFC5382.
  – For example, hold-down timers is not specific to a CGN (because existing NAPT would have similar or identical requirements), and TCP/25 filtering is not specific to a CGN (as evidenced by ISPs filtering TCP/25 without deploying a CGN).
  – For example, new logging requirements caused by IPv4 address sharing is well-described by other IETF documents which can be cited.
CGN definition

• Carrier-Grade NAT (CGN) in -01
  – NAT device placed between a subscriber and the Internet in an ISP's network. A CGN translates IP addresses and transport-protocol port numbers in the packets that it forwards across the border between the internal and external realms.

• There are some comments (thanks Mohamed)
  – Do not use “device”. CGN is function.
  – Avoid topology related definitions of CGN

• So, we will change to:

• Carrier-Grade NAT (CGN):
  – NAT-based [RFC2663] Functional Element operated by an administrative entity (e.g., operator) to share the same address among several subscribers. CGN is managed by the administrative entity, not the subscribers.
Then...

• We will update CGN draft (-02) after this IETF
• And after chairs’ check, we want to have last call