General Issues Affecting Multiple Working Group Drafts

draft-ford-behave-gen-01.txt
draft-sivakumar-behave-nat-tcp-req-01.txt
draft-ietf-behave-nat-udp-03.txt

Presenter: Bryan Ford
Co-authors: P.Srisuresh, S.Sivakumar, K.Biswas

IETF 63, Paris

Outstanding Issues

- Transport-independent requirements placement
- NAT Operating Principles
- Alignment of terminology
  - Mappings vs Bindings/Sessions/NAT Sessions
  - Relationship of new vs old terminology
- Specific transport-independent issues:
  - Processing out-of-order fragmented IP packets
  - DHCP-configured NATs
- Adoption of drafts as WG documents

Transport-Independent Requirements - Placement

- Examples:
  - Basic NAT principles and terminology
  - Port mapping/binding behavior
  - Filtering of incoming traffic
  - Fragmented IP packets
  - Hairpin translation
  - DHCP-configured NAT behavior
  - ICMP error packet handling
- Only **2 of 13** REQs currently in nat-udp-03 are obviously UDP-specific (REQ-4,5).

Transport-Independent Requirements - Placement, #2

- Relevant WG milestones on existing roadmap:
  - May 05: Behavioral requirements for Unicast UDP
  - Sep 05: Behavioral requirements for TCP
  - Nov 05: Behavioral requirements for ICMP
- Currently no obvious place for transport-independent requirements.

Transport-Independent Requirements - Placement, #3

- **Proposal 1:** Reinterpret ICMP milestone as “generic requirements including ICMP”, move forward to publish concurrently with UDP.
- **Proposal 2:** Reorganize nat-udp-03 to separate generic from UDP-specific content, allowing unambiguous cross-references from TCP/ICMP drafts.
- **Proposal 3:** Keep all documents separate, duplicating generic content in each.

NAT Operating Principles

- draft-ford-behave-gen-01 (sec 2) describes operating principles important to design of BEHAVE-compliant NATs:
  - Reviews established NAT terms and abstract architectural entities in BEHAVE context:
    - Address/port maps (admin-configured)
    - Address/port bindings (static or dynamic)
    - NAT sessions (dynamic)
  - Precisely specifies relevant types of sessions
    - Inbound, Outbound, Hairpin (new!)
- Question: Keep, Delete, or Move Elsewhere?

Terminology: Issue #1

- draft-ford-behave-gen-01 uses existing terms:
  - **Binding** := (internal IP:port, external IP:port)
  - **NAT Session** := (internal session, external session)
  - precedent: RFCs 2663, 3022, 4008
- draft-ietf-behave-udp-nat-03 uses "**mapping**":
  - defined as "translation between an external address and port and an internal address and port"
  - refers to "bindings" in some places (e.g., mapping behavior), "NAT sessions" in others (e.g., timers)
  - precedent: ???

Terminology: Issue #2

- draft-ford-behave-gen-01 (2.4) clarifies relationship of new behavior terminology to deprecated “Cone/Symmetric” terms.
- draft-ietf-behave-udp-nat-03 does not.
- Question: keep/delete/move elsewhere?

Processing Out-of-order Fragments

- draft-ford-behave-gen-01 (REQ-3):
  - MUST be able to process all fragments of an IP datagram, in- or out-of-order.
  - MUST process fragmented packets that assemble to datagrams up to 8300 bytes in size.
- draft-ietf-behave-udp-nat-03 (REQ-13):
  - MUST be able to process in-order fragments
  - MAY be able to process out-of-order fragments
  - no mention of datagram size

DHCP-configured NATs

- Most consumer NATs get their “public” IP address via DHCP.
  - NAT's dynamic “public” IP may be a private address assigned by an upstream NAT (Twice NAT).
  - Intermediate and private IP address domains may numerically conflict – *not preventable by user*
- draft-ford-behave-gen-01 (REQ-6):
  - DHCP-configured NATs MUST operate correctly even in presence of such address conflicts.
- Not addressed by draft-ietf-behave-udp-nat-03

Adoption of WG Documents

- Adopt (appropriately edited) version of **draft-ford-behave-gen-01** as WG document for (potentially revised) ICMP milestone?