NAT requirements for ICMP (BEHAVE WG)

draft-srisuresh-behave-nat-icmp-01.txt

P.Srisuresh,

B.Ford

S.Sivakumar

S.Guha

Overview

- Objective is to make NATs ICMP processing predictable.
- 5 requirements listed.
- Applicable to all IP based applications traversing NAT
- Addresses the ICMP error message and query processing issues.
- Does not conflict with UDP/TCP drafts.

Discussion topic -1

- REQ-1: RECOMMEND allowing administrators to configure ICMP Query session timeout. (suggested value: 30 sec)
- Q1: Should the ICMP draft adapt similar wording as the UDP draft(Min. timeout, default timeout and configurability option)?
- Q2: Is there consensus on the suggested ICMP session timeout for Min./Default timeout?

Discussion topic -2

- REQ-2: NAT MUST transparently forward ICMP error packets.
- Question: Should the forwarding be restricted to ICMP Dest. Unreachable Messages only? If so, why?
- Clarification: NAPT MUST not change the ICMP error code (from Soft error to Hard error or vice versa). Do we have consensus on this?

Discussion topic -3

- REQ-2: When Src IP of ICMP error packet is from a node in private domain for which NAT has no mapping, NAT MUST use its own IP address to translate Src IP in the outer IP header.
- Comment from Fernando Gont: NAT SHOULD fix the IP, TCP and UDP checksums of the embedded packet prior to forwarding.
- Both are assumed in RFC 1812 (Sec 4.3.2.3, 4.3.2.4)
- Do we have consensus on these?

Discussion topic -4

- REQ-3: While processing an ICMP error packet, a NAT device MUST not refresh or delete the NAT Session that pertains to the embedded payload within the ICMP error packet .
- Change from the UDP draft:
  - Applies to all Error messages
  - NAT Session should not be refreshed.
- Do we have consensus on this?

Discussion topic -5

- REQ-4: When an outbound packet is prohibited by NAT due to resource constraint (or) failed authorization, NAT SHOULD send ICMP destination unreachable message, with a code of 10 (Communication with destination host administratively prohibited) to sender.
- This is a soft error. Sender should retry at another time.
- Do we have consensus on this?

Discussion topic -6

- REQ-5: If DF bit is set on a IP packet and NAT cannot forward the packet without fragmentation, NAT MUST send a "Packet too big" ICMP message with a suggested MTU back to sender.
- Change from the UDP draft:
  - UDP has this in discussion, but not in the final requirements list.

Discussion topic -7

- New Requirement (Thanks to Dan for suggesting): When a packet's TTL is decremented to 0 prior to forwarding, NAT MUST issue 'ttl exceeded' ICMP error message.
- In general, NAT SHOULD confirm to RFC 1812 w.r.t. generating or forwarding ICMP error messages as does any router.
- Do we have WG consensus to include as new requirement?

Discussion Topic -8

- Add new Requirement that NAT external Mapping for ICMP Queries SHOULD be endpoint independent?
- Most NAPT devices today assign external mapping that is endpoint dependent for ICMP Query Identifiers for each tuple of (Src IP, Query Identifier, Target IP).
- Recommending endpoint independent mapping would proactively support any future applications that may reuse the same identifier for multiple connections.

Open Issues

- Scope of the ICMP draft
  - Scope is set to ICMP Query & Error message processing by NATs.
  - Add a statement that ICMP requirements in the TCP/UDP drafts take precedence over the general ICMP requirements stated in the ICMP draft in case of conflict.
  - Any other scope issues?
- Do we have consensus on this?

Next steps

- Does it make sense to have an ICMP Behave draft as WG item?
- What is the WG consensus?