Shim6 protocol changes

draft-ietf-shim6-proto-04.txt

Erik Nordmark
erik.nordmark@sun.com

Marcelo Bagnulo

Overview

- Changes from 03 to 04
  - Based on mailing list feedback
- Changes from 02 to 03
  - Based on open issues discussed at IETF64
- Are we done?

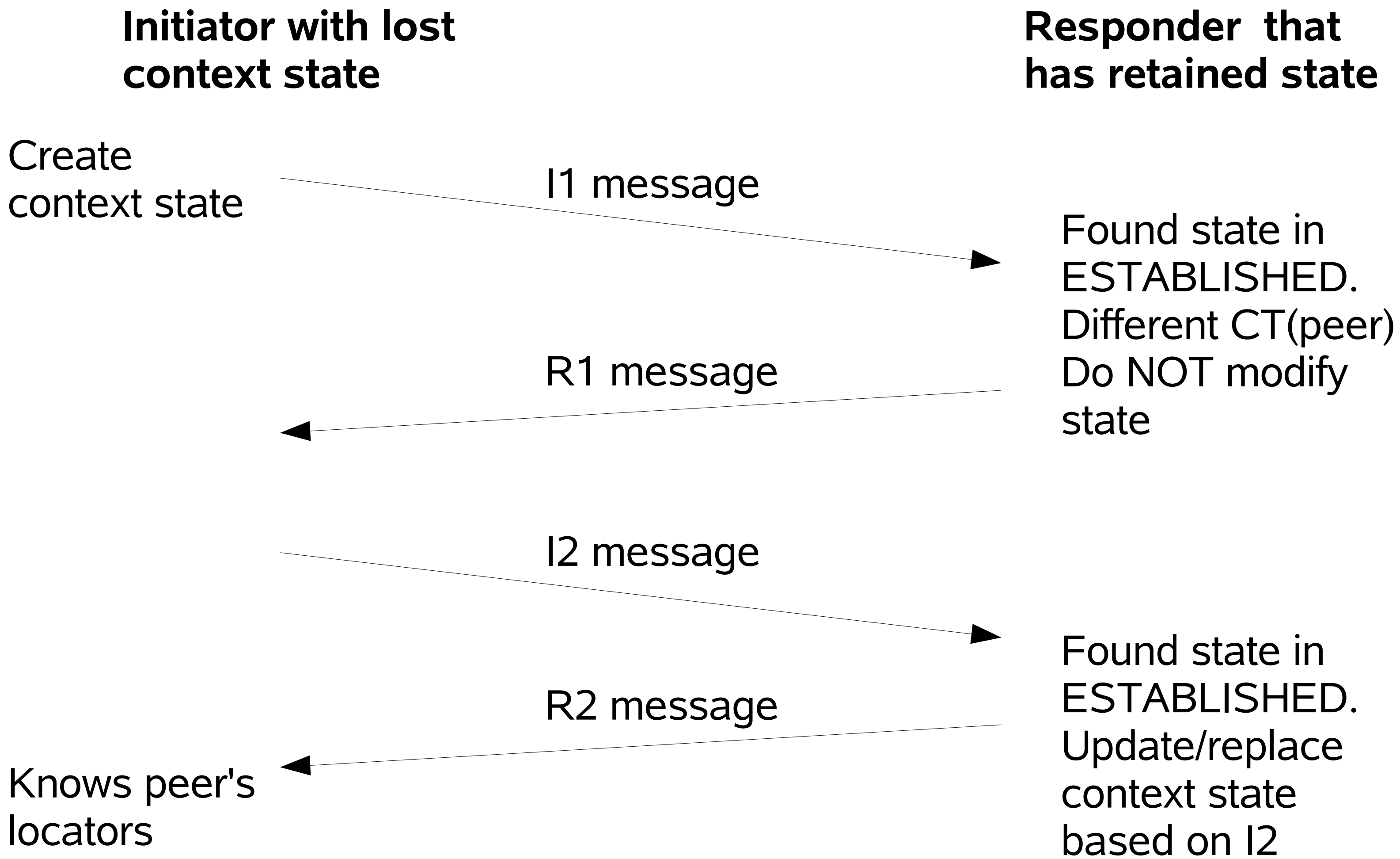
Changes from 03 to 04 (1)

- Editorial clarifications based on comments from Geoff, Shinta, and Jari
- Added "no IPv6 NATs” as an explicit assumption
- Moved some text out of the Introduction and Overview sections to remove all SHOULDs and MUSTs from the overview.
- Added requirement that any Locator Preference options with “element length” greater than 3 octets must have flags, priority and weight in first 3 octets
  - ensures that host can interpret the “base” 3 octets

Changes from 03 to 04 (2)

- Added retransmission rules for I2bis (copied from I2 rules)
- Fixed security hole where a single message (I1) could cause CT(peer) to be updated. Now a three-way handshake is required before CT(peer) is updated for an existing context
- Implies 4 message context recovery in one case that had two messages before
  - Next slide

Context Recovery



Initiator with lost context state

Responder that has retained state

Create context state

I1 message

Found state in ESTABLISHED. Different CT(peer) Do NOT modify state

R1 message

I2 message

Found state in ESTABLISHED. Update/replace context state based on I2

R2 message

Knows peer's locators

Changes from 02 to 03 (1)

- Context recovery redone
  - Replaced the Context Error message with the R1bis message.
  - Removed the Packet In Error option, since it was only used in the Context Error message.
  - Introduced a I2bis message which is sent in response to an I1bis message, since the responders processing is quite different in this case than in the regular R1 case.

Changes from 02 to 03 (2)

- Expanded the context tag from 32 to 47 bits.
- Modified the dispatching of payload extension header to only compare CT(local) i.e., not compare the source and destination IPv6 address fields.
- Specified that “enough” locators need to be included in I2 and R2 messages. Specified that the HBA/CGA verification must be performed when the locator set is received.

Changes from 02 to 03 (3)

- Specified how context recovery and forked contexts work together
  - This required the introduction of a Forked Instance option to be able to tell which of possibly forked instances is being recovered.
- Specified that ICMP parameter problem errors are sent in certain error cases, for instance when the verification method is unknown to the receiver, or there is an unknown message type or option type.

Changes from 02 to 03 (4)

- Picked some initial retransmit timers for I1 and I2; 4 seconds.
- Added timer values as protocol constants. The retransmit timers use binary exponential backoff and randomization (between .5 and 1.5 of the nominal value).
- Require that the R1/R1bis verifiers be usable for some minimum time so that the initiator knows for how long time it can safely retransmit I2 before it needs to go back to sending I1 again.
  - Picked 30 seconds

Changes from 02 to 03 (5)

- Split the message type codes into 0-63, which will not generate R1bis messages, and 64-127 which will generate R1bis messages.
  - allows extensibility of the protocol with new message types while being able to control when R1bis is generated.

Editorial from 02 to 03 (1)

- Removed the packet formats for the Keepalive/ Probe types and Event option. Kept the message type values and option type value.
- Removed the unused message types
- Renamed the "host-pair context" to be "ULID-pair context"
- Renamed "payload message" to be "payload extension header"
- Added state machine description as an appendix
- Many editorial clarifications from Geoff

Next Steps

- Ready for last call?