

Transport Options for UDP

draft-ietf-tsvwg-udp-options-22
(WG Chair Summary)

IETF TSVWG, San Francisco July 2023

IETF TSVWG, Yokohama March 2023

Joe's Proposed Five Basic Tenets

A.) UDP is stateless; UDP options do not change that

- Any state must be managed either by the application or a layer/library on behalf of the application
- Reassembly of fragments is a limited exception

B.) UDP is unidirectional; UDP options do not change that

- Responses to options are initiated by the application or a layer/library on behalf of the application
- Any mechanism that requires bidirectionally needs to be defined in a separate document

C.) UDP options have no length limit separate from that of the UDP packet itself

- Past experience confirms that static limits will always be exceeded
- Each implementation can limit how long/many options there are, but the spec should not

D.) UDP options should not replace or replicate other protocols

- This includes NTP, ICMP (notably echo), etc.

E.) UDP options are a framework

- Options may be defined even when the details are not sufficient to implement
- Uses of such options may then be described in other documents

There has been limited discussion of these points; is the WG on board with all of this?

Basic Three Issues from IETF 116

Fragmentation (Section 9.4)

- New acronym RDOS (for Reassembled Datagram Option Start) introduced
- Proposal to define new ICMP Time Exceeded code for UDP reassembly timeout introduced
- Mike Heard: changes from -18 to -19 that rendered the spec incoherent are not fixed in -22
- Erik Auerswald: unable to evaluate Section 9.4 as written in -22, will review next iteration
- Gorry Fairhurst: simplify by eliminating per-fragment options and ICMP error messages
- New text proposed by Mike Heard & reviewed by Erik Auerswald; no other discussion
- See github issues [1](#), [2](#), [3](#), [16](#)

Encryption

- Joe Touch: doc should contain option structure but not define algorithms, key derivations, etc.
- Avoid down-ref by “reserving” codepoint for encryption, rather than “assigning”
- See github issue [6](#)

Authentication (arguably very close to TCP-AO)

- Could do the same as for encryption (reserve it rather than assign it)
- Joe thinks this is much more mature by corollary to TCP-AO
- Sequence number added to AUTH (in -20) to allow for replay protection (not in TCP-AO)
- Could require replay ID starting values are coordinated out-of-band, similar to TCP WG
- See github issue [5](#)

These basic issues remain open, and further WG discussion is needed to come to a resolution.

Issues Requiring a Text Proposal

Mention potential for privacy exposure

- Security considerations should mention risk of privacy exposure if UDP options are used with upper layer protocols that protects privacy (e.g., QUIC)
- See github issue [8](#)
-

Should OCS be mandatory under circumstances other than UDP CS <> 0?

- The issue was raised by Tom Herbert and also by Carlos Pignataro during his INTAREA review
- Mike Heard defended the current normative requirements; Tom Herbert then proposed that there should be requirements in the draft similar to those of RFC6936 but specific to the risks and mitigation for a zero OCS. Mike Heard agreed and owes a text proposal.
- See github issue [12](#)

Specific text proposals and subsequent discussion should bring these issues to closure.

Issues Requiring Discussion

Resolution of discussion on timestamp RTT processing

- Should TIME be redesigned with three response fields to allow compensation for local delay?
- See github issue [4](#)

Does the document need to have more thorough discussion of middlebox traversal issues?

- There is discussion of how the design of OCS sidesteps one middlebox traversal issue
- If other discussion is needed, one suggestion is to add it to Section 16 and rename the section
- See github issue [7](#)

The inner "if" clauses in the pseudo-code of Section 12 seem to be inconsistent

- The issue was raised on the mailing list and answered but not resolved
- See github issue [10](#)

These issues are not as crucial as preceding ones, but still need discussion to obtain closure.

Issues Ready to be Resolved

Consistent use of ">>" as a marker

- The use of ">>" to mark paragraphs with BCP 14 nomenclature is not yet completely consistent.
- See github issue [9](#)

Section 22 should compare UDP options and TCP options

- There is a paragraph that inadvertently compares UDP options with UDP options
- See github issue [11](#)

Change "segment" to "datagram" in Section 9.6

- The section title is "Maximum Reassembled Datagram Size," but the text then defines that as "the largest reassembled UDP segment that can be received."
- See github issue [12](#)

Wordsmithing to text of Section 9.7

- These are clarifications to the definitions and usage of REQ and RES
- See github issues [14](#) and [15](#) (there is a pointer to proposed text in the latter)

These issues are purely editorial.