Multiplexing Scheme Updates for SRTP Extension for DTLS

draft-petithuguenin-avtcore-rfc5764-mux-fixes

IETF-90

Toronto, July 23, 2014

Marc Petit-Huguenin, Gonzalo Salgueiro

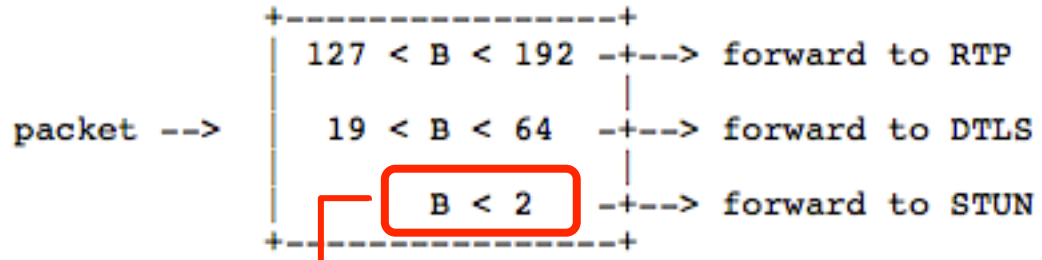
IETF

Overview

- Identifies 3 issues with multiplexing scheme defined in RFC 5764 Section 5.1.2

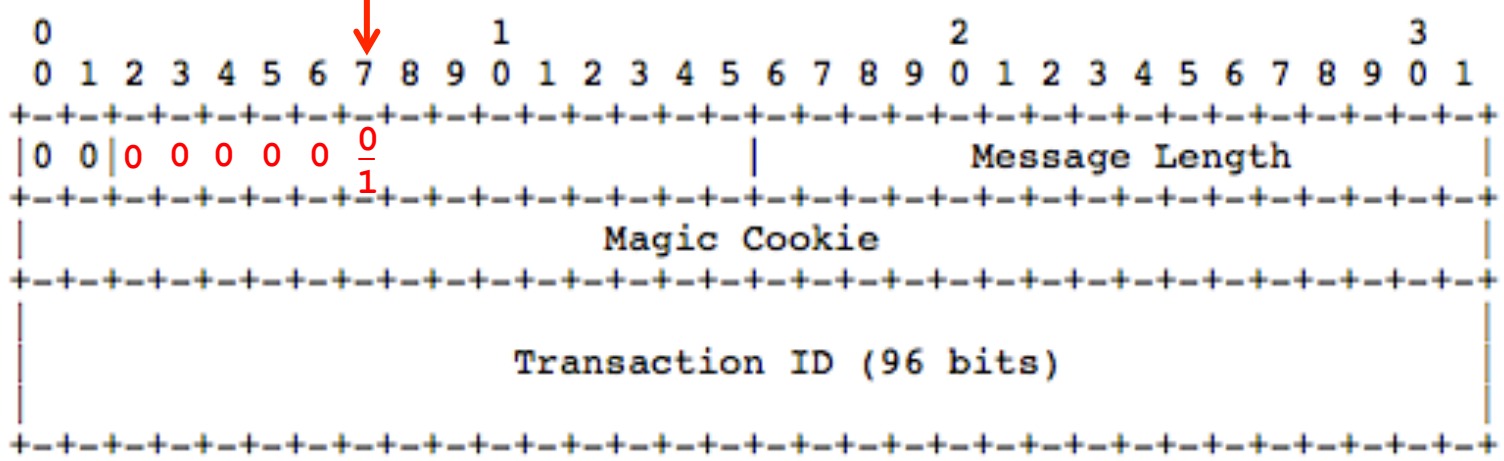
1. Implicit allocation of codepoints for new STUN methods with no IANA registry
2. Implicit allocation of codepoints for new TLS ContentTypes with no IANA registry
3. Didn't account for TURN usage of STUN can create TURN channels that also need demuxing with other explicitly mentioned packet types

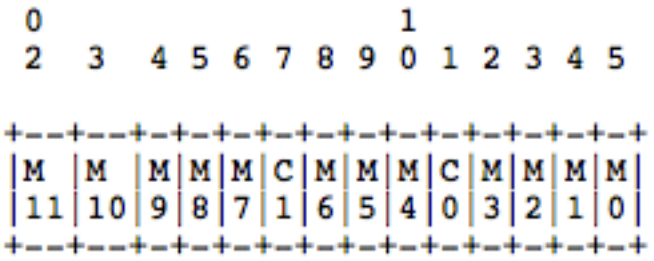
Problem 1: STUN Methods



Current packet identification scheme: if first byte is 0 or 1, the packet is STUN

Restricts STUN methods to values 0x000 – 0x07F





Range

Min:	MMMMMCMMMCMMMM 0b0000000000000000	**method = 0x000** class = 0b00
Max:	MMMMMCMMMCMMMM 0b0000000111111111	**method = 0x07F** class = 0b11

IETF

Proposed Solution

- Update RFC 5764 packet identification algorithm to expand range assigned to STUN from 0-1 to 0-19 (values 2-19 currently unused)
- Proposed changes to the STUN Method Registry is:

OLD:

0x000-0x7FF	IETF Review
0x800-0xFFF	Designated Expert

NEW:

0x000-0x27F	IETF Review
0x280-0x4FF	Designated Expert
0x500-0xFFF	Reserved

IETF

Next Steps

- RFC 5764 updates will be discussed in AVTCORE
- Coordinated effort of 3 different WGs (TRAM, TLS, AVTCORE)
- Do we create a WG milestone for updating the STUN Methods Registry?
- Can we adopt as WG doc to satisfy this?