# Multiplexing Scheme Updates for SRTP Extension for DTLS

draft-petithuguenin-avtcore-rfc5764-mux-fixes

Marc Petit-Huguenin, Gonzalo Salgueiro


IETF-92

Dallas, March 24, 2015

# Proposed Solution

- Update RFC5764 packet identification algorithm to expand range assigned to STUN from 0-1 to 0-3
- Proposed changes to the STUN Method registry are:

OLD:

0x000 – 0x7FF IETF Review

0x800 – 0xFFF Designated Expert

NEW:

0x000 – 0x07F IETF Review

0x080 – 0x0FF Designated Expert

0x100 – 0xFFF Reserved

(MUST be allocated with IETF Review

# Proposed Solution (cont'd)

- Update RFC5764 packet identification algorithm to add SCTP using the value 5
- STUNbis will be updated accordingly

# Proposed Solution (cont'd)

- Explicitly reserves the TLS ContentType codepoints from 0-19 and from 64-255. They can still be allocated, but require IETF Review to properly evaluate the risk of an assignment overlapping with other registries.
- Proposed changes to TLS ContentTypes Registry are:

OLD:

0-19 Unassigned
20 change_cipher_spec
21 alert
22 handshake
23 application_data
24 heartbeat
25-255 Unassigned

NEW:

0-19 Reserved (May be allocated with IETF Review)
20 change_cipher_spec
21 alert
22 handshake
23 application_data
24 heartbeat
25-63 Unassigned
64-255 Reserved (May be allocated with IETF Review)

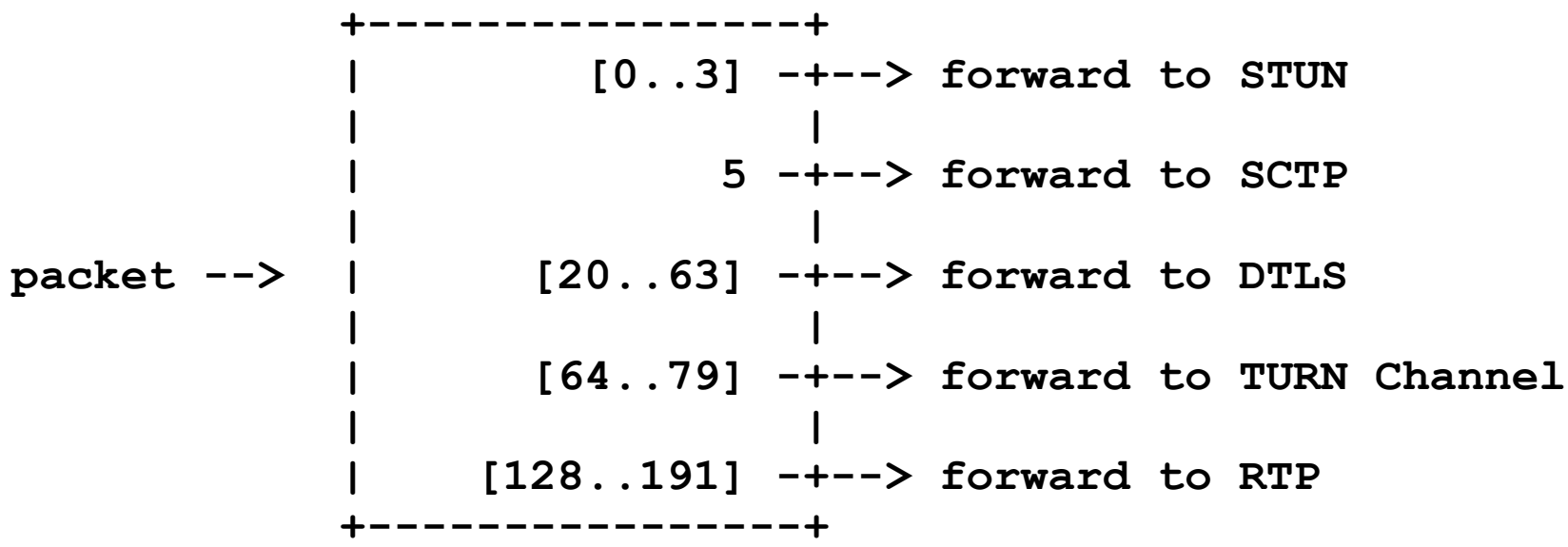
# Proposed Solution (cont'd)

- Modify the RFC 5764 demux algorithm to properly account for TURN channels by allocating values from 64 to 79 (included).
- An implementation that uses the source IP address and port to identifies TURN channel messages does not need to restricts the channel numbers to the range above.
- TURNbis to be updated accordingly.
- Proposed changes to the TURN Channel Number registry is:


Value: 0x5000-0xFFFF
Name: Reserved
Reference: RFCXXXX

# Proposed Solution (cont'd)

- When new values or ranges are added, they MUST be tested in ascending order.




IETF

# Next Steps

- This work will need to be a coordinated effort between 3 WG (AVTCORE, TRAM, TLS)
- Initial WG version submitted after this meeting
- An -01 version submitted immediately after with proposed solution discussed here
- Additional reviews requested
- WGLC ???

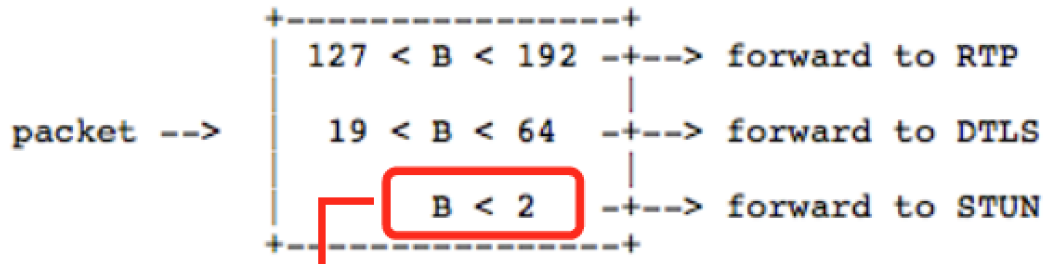
# BACK-UP SLIDES

# Overview

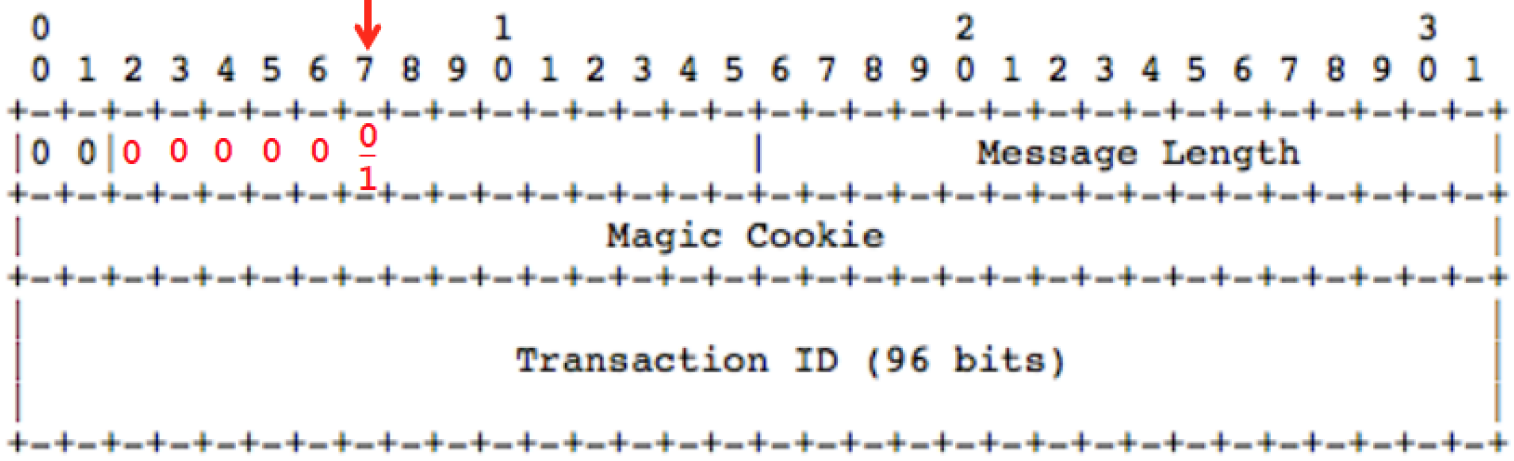
- Identifies 3 issues with multiplexing scheme defined in RFC 5764 Section 5.1.2

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

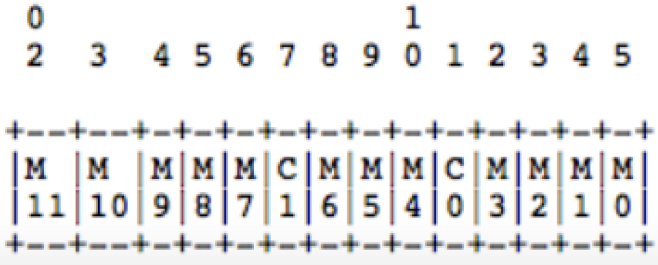
# Problem 1: STUN Methods




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<br>0b0000000000000000 | **method = 0x000**<br>class = 0b00 |
| Max: | MMMMMCMMMCMMMM<br>0b0000000111111111 | **method = 0x07F**<br>class = 0b11 |

I E T F