

# STUN Protocol for Embedding DTLS

draft-hancke-webrtc-sped-00

Justin Uberti  
IETF 125 Shenzhen  
18 March 2026



# draft-hancke-webrtc-sped-00

- WebRTC uses ICE and DTLS, but serializes steps
  - Also DTLS handshake can be very slow with packet loss (b/c exp backoff)
- Solution: piggyback the DTLS handshake onto the STUN packets
  - Saves 1RTT in ideal conditions
  - Works with DTLS 1.2, 1.3, and 1.3/PQC
  - With DTLS 1.3, delivers performance on-par with SDES!
  - Also improves reliability under packet loss
- Downside: larger STUN packets
  - in particular with DTLS 1.3/PQC client hello (~1KB)

# draft-hancke-webrtc-sped-00

```
Client                               Server
|                                   |
|----- SDP Offer ----->|
|<-1----- SDP Answer (a=setup:passive) -----|
|                                   |
|----- STUN BindingRequest ----->|
|<-2----- STUN BindingResponse -----|
|                                   |
|----- DTLS F1: ClientHello ----->|
|<-3----- DTLS F2: ServerHello, etc-----|
|----- DTLS F3: Finished, etc ----->|
|<-4----- DTLS F4: Finished, etc -----|
|----- Application data ----->|
```

```
Client                               Server
|                                   |
|----- SDP Offer ----->|
|<-1----- SDP Answer (a=setup:passive)-----|
|                                   |
|----- BindingRequest/DTLS F1 ----->|
|<-2----- BindingResponse/DTLS F2 -----|
|                                   |
|----- DTLS F3: Finished ----->|
|<-3----- DTLS F4: Finished -----|
|----- Application data ----->|
```

Left: DTLS 1.2

Right: DTLS 1.2 with SPED (saves 1 RTT)

# draft-hancke-webrtc-sped-00

```
Client                                     Server
|                                         |
|----- SDP Offer ----->|
|<-1----- SDP Answer (a=setup:passive) -----|
|                                         |
|----- STUN BindingRequest ----->|
|<-2----- STUN BindingResponse -----|
|                                         |
|----- DTLS F1: ClientHello ----->|
|<-3----- DTLS F2: ServerHello, etc -----|
|----- DTLS F3: Finished ----->|
|----- Application data ----->|
|<----- DTLS ACK -----|
```

```
Client                                     Server
|                                         |
|----- SDP Offer ----->|
|<-1----- SDP Answer (a=setup:passive) -----|
|                                         |
|----- BindingRequest/DTLS F1 ----->|
|<-2----- BindingResponse/DTLS F2 -----|
|                                         |
|----- DTLS F3: Finished ----->|
|----- Application data ----->|
|<----- DTLS ACK -----|
```

Left: DTLS 1.3

Right: DTLS 1.3 with SPED (saves 1 RTT)

# draft-hancke-webrtc-sped-00

- New STUN attribute for carrying DTLS packet
  - Pending DTLS packets are sent round-robin in ICE checks
- New STUN attribute for explicit ACK indicator
  - Received packets are ACKed in ensuing ICE checks
- Negotiation is done in-band (no offer-answer)
  - If you get an ICE check without the attribs, it's not supported
- A few open [questions](#), among them, what is the right working group?
  - Needs input from STUN, congestion control and DTLS (e.g. ACK mechanism)