Abstract

RFC 7983 defines a scheme for a Real-time Transport Protocol (RTP) receiver to demultiplex Datagram Transport Layer Security (DTLS), Session Traversal Utilities for NAT (STUN), Secure Real-time Transport Protocol (SRTP) / Secure Real-time Transport Control Protocol (SRTCP), ZRTP, and Traversal Using Relays around NAT (TURN) channel packets arriving on a single port. This document updates RFC 7983 and RFC 5764 to also allow QUIC packets to be multiplexed on a single receiving socket.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9443.

Copyright Notice

Copyright (c) 2023 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions
with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents
1. Introduction
   1.1. Terminology
2. Multiplexing of TURN Channels
3. Updates to RFC 7983
4. Security Considerations
5. IANA Considerations
6. References
   6.1. Normative References
   6.2. Informative References
Acknowledgments
Authors' Addresses

1. Introduction


The multiplexing scheme described in this document supports multiple use cases. In the WebRTC scenarios described in [P2P-QUIC] and [P2P-QUIC-TRIAL], SRTP transports audio and video while peer-to-peer QUIC is used for data exchange. For this use case, SRTP [RFC3711] is keyed using DTLS-SRTP [RFC5764]; therefore, SRTP/SRTCP [RFC3550], STUN, TURN, DTLS, and QUIC need to be multiplexed on the same port. Were SRTP to be keyed using QUIC-SRTP (not yet specified), SRTP/SRTCP, STUN, TURN, and QUIC would need to be multiplexed on the same port. Where QUIC is used for peer-to-peer transport of data as well as RTP/RTCP [RTP-OVER-QUIC], STUN, TURN, and QUIC need to be multiplexed on the same port.
While the scheme described in this document is compatible with QUIC version 2 [RFC9369], it is not compatible with QUIC bit greasing [RFC9287]. As a result, endpoints that wish to use multiplexing on their socket MUST NOT send the grease_quic_bit transport parameter.

1.1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Multiplexing of TURN Channels

TURN channels are an optimization where data packets are exchanged with a 4-byte prefix instead of the standard 36-byte STUN overhead (see Section 3.5 of [RFC8656]). [RFC7983] allocates the values from 64 to 79 in order to allow TURN channels to be demultiplexed when the TURN client does the channel binding request in combination with the demultiplexing scheme described in [RFC7983].

In the absence of QUIC bit greasing, the first octet of a QUIC packet (e.g. a short header packet in QUIC v1 or v2) may fall in the range 64 to 127, thereby overlapping with the allocated range for TURN channels of 64 to 79. However, in practice this overlap does not represent a problem. TURN channel packets will only be received from a TURN server to which TURN allocation and channel-binding requests have been sent. Therefore, a TURN client receiving packets from the source IP address and port of a TURN server only needs to disambiguate STUN (i.e., regular TURN) packets from TURN channel packets; (S)RTP, (S)RTCP, ZRTP, DTLS, or QUIC packets will not be sent from a source IP address and port that had previously responded to TURN allocation or channel-binding requests.

As a result, if the source IP address and port of a packet do not match that of a responding TURN server, a packet with a first octet of 64 to 127 can be unambiguously demultiplexed as QUIC.

3. Updates to RFC 7983

This document updates the text in Section 7 of [RFC7983] (which in turn updates [RFC5764]) as follows:

OLD TEXT

The process for demultiplexing a packet is as follows. The receiver looks at the first byte of the packet. If the value of this byte is in between 0 and 3 (inclusive), then the packet is STUN. If the value is between 16 and 19 (inclusive), then the packet is ZRTP. If the value is between 20 and 63 (inclusive), then the packet is DTLS. If the value is between 64 and 79 (inclusive), then the packet is TURN Channel. If the value is in between 128 and 191 (inclusive), then the packet is RTP (or RTCP, if both RTCP and RTP are being multiplexed.)
over the same destination port). If the value does not match any known range, then the packet **MUST** be dropped and an alert **MAY** be logged. This process is summarized in Figure 3.

```
+----------------+          +----------------+
|        [0..3] --+--> forward to STUN   | [128..191] --+--> forward to RTP/RTCP
|                |          |                |
|      [16..19] --+--> forward to ZRTP  |                |
|                |          |                |
|      [20..63] --+--> forward to DTLS  |
|                |          |                |
|      [64..79] --+--> forward to TURN Channel|
+----------------+          +----------------+
```

Figure 3: The DTLS-SRTP receiver’s packet demultiplexing algorithm.

The process for demultiplexing a packet is as follows. The receiver looks at the first byte of the packet. If the value of this byte is between 0 and 3 (inclusive), then the packet is STUN. If the value is between 16 and 19 (inclusive), then the packet is ZRTP. If the value is between 20 and 63 (inclusive), then the packet is DTLS. If the value is between 128 and 191 (inclusive), then the packet is RTP (or RTCP, if both RTCP and RTP are being multiplexed over the same destination port). If the value is between 80 and 127 (inclusive) or between 192 and 255 (inclusive), then the packet is QUIC. If the value is between 64 and 79 (inclusive) and the packet has a source IP address and port of a responding TURN server, then the packet is TURN channel; if the source IP address and port are not that of a responding TURN server, then the packet is QUIC.

If the value does not match any known range, then the packet **MUST** be dropped and an alert **MAY** be logged. This process is summarized in Figure 3.
Note: Endpoints that wish to demultiplex QUIC **MUST NOT** send the grease_quic_bit transport parameter, as described in [RFC9287].

---

### 4. Security Considerations

The solution discussed in this document could potentially introduce some additional security issues beyond those described in [RFC7983]. These additional concerns are described below.

In order to support multiplexing of QUIC, this document adds logic to the scheme defined in [RFC7983]. If misimplemented, the logic could potentially misclassify packets, exposing protocol handlers to unexpected input.

When QUIC is used solely for data exchange, the TLS-within-QUIC exchange [RFC9001] derives keys used solely to protect QUIC data packets. If properly implemented, this should not affect the transport of SRTP or the derivation of SRTP keys via DTLS-SRTP. However, if a future specification were to define use of the TLS-within-QUIC exchange to derive SRTP keys, both transport and SRTP key derivation could be adversely impacted by a vulnerability in the QUIC implementation.

### 5. IANA Considerations

In the "TLS ContentType" registry, IANA replaced references to [RFC7983] with references to this document.
6. References

6.1. Normative References


6.2. Informative References


Acknowledgments

We would like to thank Martin Thomson, Roni Even, Jonathan Lennox, and other participants in the IETF QUIC and AVTCORE Working Groups for their discussion of the QUIC multiplexing issue, and their input relating to potential solutions.

Authors' Addresses

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
United States of America
Email: bernard.aboba@gmail.com
**Gonzalo Salgueiro**
Cisco Systems
7200-12 Kit Creek Road
Research Triangle Park, NC 27709
United States of America
Email: gsalguei@cisco.com

**Colin Perkins**
School of Computing Science
University of Glasgow
Glasgow
G12 8QQ
United Kingdom
Email: csp@c sperkins.org