RADIUS over QUIC

draft-yl-radext-quic-transport-01

Presenter : Shengnan Yue (China Mobile)
Changwang Lin (New H3C)
Feng Yang (China Mobile)

IETF-123, July 2025

Why does RADIUS protocol need QUIC?

- **TCP is used as a transport protocol for RADIUS when requires confidentiality and security (i.e., TLS or IPsec) in inter-server communications scenarios, such as inter-domain communication between proxies [RFC6631]**

- **QUIC could replace TCP as the transport protocol for RADIUS.**

Why does RADIUS protocol need QUIC?

- **High Efficiency**

  - **QUIC supports multiple simultaneous streams to carry data, which allowing each stream to transmit data concurrently.**
  - **QUIC could avoid head-of-line blocking and improve overall performance.**

- **Connection Migration**

  - **The ability of QUIC to handle connection migrations seamlessly could enhance user mobility without disrupting RADIUS authentication sessions.**

- **Enhanced Security**

  - **QUIC provides transport security with build-in encryption and authentication.**

Connection Management

- **Connection Establishment**
  - **RADIUSoQUIC support is indicated by selecting ALPN token in the TLS handshake.**
  - **The RADIUS client (or Proxy as client) is the initiator of the QUIC connection. The RADIUS server (or Proxy as server) acts as the connection acceptor.**
- **Connection Termination**
  - **QUIC connection termination process refer to RFC9000.**
  - **Some RADIUSoQUIC considerations for connection termination.**

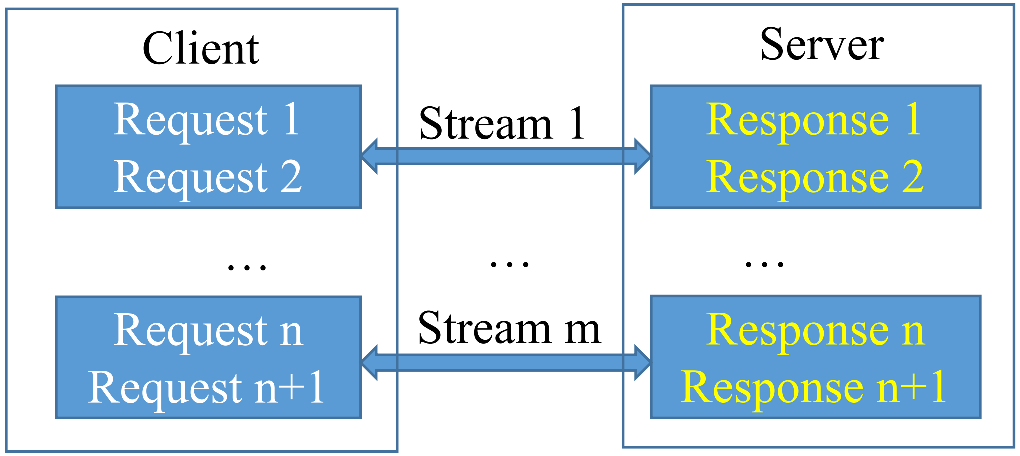
Stream mapping and usage

- **Bidirectional Stream between Client and Server**

When a RADIUS request packet is carried via transport protocol from the Client to the Server, a RADIUS response packet is needed to be sent from Server to Client in response to the RADIUS request packet. RADIUS messages MAY be mapped into one or more bidirectional streams whose stream type is 0x0.

- **Multiple Streams between Client and Server**

If there are a large number of RADIUS request packets, the multiple streams could be created to carry the packet, and the request message and its corresponding response message must be on the same stream to ensure their correlation.



Endpoint Authentication

- **Using TLS handshake authentication**
- **Using third-party authentication**

Operational Considerations

- **Provide a configuration mechanism to enable RADIUSoQUIC on the RADIUS session.**

- **As QUIC is a reliable transport, if there is no response to a RADIUS packet over one QUIC connection, that packet MUST NOT be retransmitted over a different QUIC connection to the same destination IP address and port, while the first connection is in the OKAY state.**

IANA Considerations

- **A new registration for the identification of RADIUSoQUIC in the "Application Layer Protocol Negotiation (ALPN) " Protocol IDs registry established in [RFC7301].**

  The "RADIUSoQ" string identifies RADIUSoQUIC:

  * Protocol: RADIUSoQUIC

  * Identification Sequence: 0x52 0x41 0x44 0x49 0x55 0x53 0x6f 0x51 ("RADIUSoQ")

  * Specification: This document

- **Also request IANA to reserve a UDP port (TBD) for the "RADIUS over QUIC".**

Next Steps

- **Request more review to improve the draft.**
- **Any comments are welcomed.**