RADIUS over QUIC

draft-yl-radext-quic-transport-03

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

IETF-124, November 2025

Updates from Last Version

- Presented at IETF 123 • Valuable feedback received during the meeting is appreciated;

- **Updates from v01 to v03**

1. Clarify ambiguous descriptions based on the feedback;
2. Add a use case using Multiple QUIC Streams;
3. Add some operation descriptions;

Why does RADIUS protocol need QUIC?

Updates 1

➢ **High Efficiency**

- QUIC supports multiple simultaneous streams to carry RADIUS data concurrently, which can **alleviate the congestion problem of large-scale authentication messages.**
- QUIC provides **faster handshake** to reduces connection establishment time.

➢ **Connection Migration**

- The ability of QUIC to handle connection migrations seamlessly could enhance **RADIUS network mobility between client (such as NAS) and server,** allowing client to change networks without disrupting RADIUS authentication sessions.

Why does RADIUS protocol need QUIC?

Updates 1

- **Enhanced Security**
  - QUIC provides transport security with build-in encryption and authentication.
  - TCP is used as a transport protocol for RADIUS only when a transport layer such as TLS or IPsec provides confidentiality and security in inter-server communications scenarios.
  - The build-in encryption can greatly **simplify security-related configurations.**

QUIC can be used as an **optional transport protocol** for RADIUS.

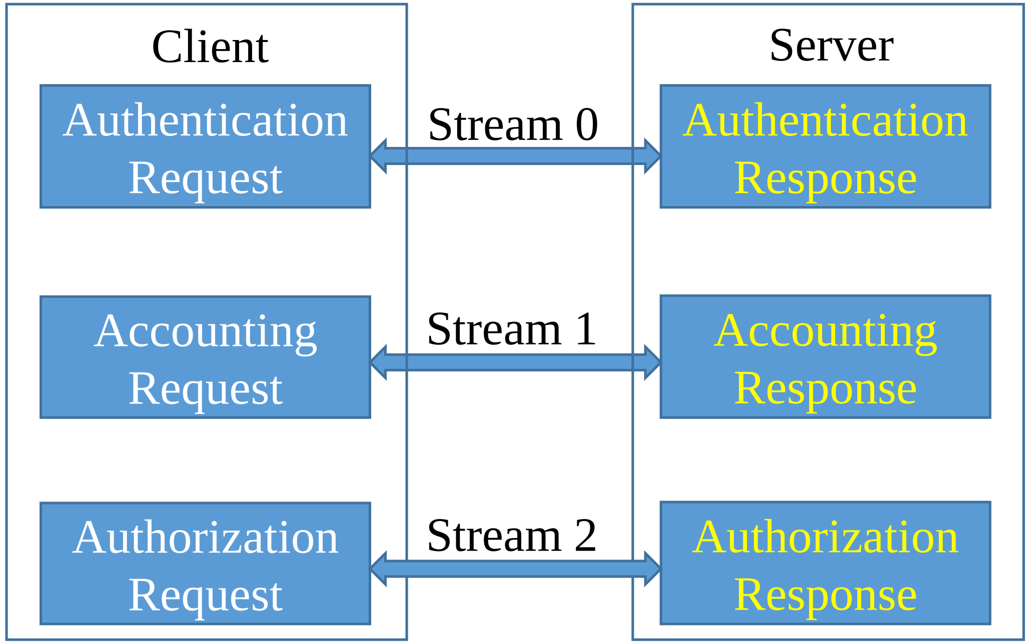
Stream mapping and usage

Updates 2

- **Multiple Streams Use Case**

RADIUS transactions includes **Authentication** transactions, **Accounting** transactions, and **Dynamic Authorization** transactions.

Therefore**, three bidirectional streams** can be created to carry these **three transactions.** Stream 0 is used for authentication, stream 1 for accounting, and stream 2 for authorization transactions.



Operational Considerations

Updates 3

Configuration Parameters:

- ✓ **A configuration option** SHOULD be provided to enable the **use of multiple streams**, and the number of streams also SHOULD be configurable.

Packet Format:

- ✓ RADIUSoQUIC MUST fully **maintain all existing RADIUS specifications**, keeping the original packet format, attribute encoding, and security calculations unchanged.
- ✓ The modifications for implementing RADIUSoQUIC mainly impact RADIUS's network packet **transmission and reception components.**

Operational Considerations

Updates 3

Port:

- ✓ RADIUSoQUIC uses a single IANA-assigned UDP port (TBD) for all functions (authentication, accounting, and authorization), while source ports can be freely selected.

Management Information Base (MIB):

- ✓ The current RADIUS MIB modules only support UDP transport and cannot monitor RADIUSoQUIC connections.
- ✓ They lack capabilities to track QUIC-specific features like multi-streaming. **New MIB specifications** will be needed for RADIUSoQUIC monitoring.

Operational Considerations

Updates 3

Detecting Live Servers:

- ✓ The RADIUS proxy architecture allows clients to only perceive the status of the direct proxy and not the status of the backend server.
- ✓ When a request is unresponsive, the fault location is ambiguous because it may be caused by any of the following factors: packet loss, proxy failure, or actual server outages, and there is a lack of diagnostic mechanisms.
- ✓ When using RADIUSoQUIC, **the RADIUS server should only be declared unresponsive** when: (1) All existing QUIC connections have terminated, and (2) No new connections can be established using remaining Connection IDs.
- ✓ RADIUSoQUIC permits clients to forcibly close connections or administratively mark servers DOWN.

Operational Considerations

Updates 3

Malformed Packets Handling:

- ✓ RADIUSoQUIC implementations MUST immediately terminate the affected QUIC stream upon meeting serious closure conditions, and MAY optionally close the entire QUIC connection per local policy.
- ✓ RADIUSoQUIC also applies the silent discard behavior in some exceptional cases (invalid codes or unmatched responses).
- ✓ Implementations may terminate just the faulty stream or the entire QUIC connection – maintaining security while isolating stream failures to preserve other transactions.

Operational Considerations

Updates 3

Limitations of one-octet RADIUS ID:

- ✓ The one-octet RADIUS ID restricts each QUIC connection to 256 concurrent in-flight transactions in RADIUSoQUIC.
- ✓ To exceed 256 concurrent RADIUS transactions, implementations should create additional QUIC connections. QUIC's lower overhead makes multiple connections more viable than with TCP.

Extensible Authentication Protocol (EAP) Sessions:

- ✓ RADIUSoQUIC clients should use a single QUIC stream per EAP session to preserve ordering and isolation.
- ✓ EAP-level retransmissions never cause RADIUS packet retransmissions over the same QUIC stream; QUIC automatically handles transport-layer retransmission needs.
- ✓ use alternate streams/connections if the original fails.

Next Steps

- **Request more review and feedback.**
- **Request for WG adoption.**

Thanks!