RPKI to Router (RTR) Protocol over QUIC

draft-liu-sidrops-rpki-rtr-over-quic-02

Presenter: Jishnu Roy (Juniper)

Co-Authors:
Shengnan Yue(China Mobile)
Changwang Lin (New H3C)
Jishnu Roy (Juniper)
Di Ma (ZDNS)
Yisong Liu (China Mobile)

IETF-124, November 2025

Why does RTR protocol need QUIC?

Advantages for QUIC (Compared to TCP/SSHv2/TLS currently supported by RTR):

1. **Has reliability and congestion control similar to TCP ;**
2. **Offers end-to-end security to ensure data confidentiality and integrity ;**
   - **QUIC has built-in TLS encryption (typically TLS 1.3); Encryption for TCP, requires additional protocols such as IPsec, increasing configuration complexity.**
3. **Allows multiple data streams to be multiplexed within a single connection;**
   - **QUIC supports multi-streaming for improving performance, and each stream transmits data independently, avoiding the head-of-line blocking issue found in TCP.**
4. **Has a faster connection establishment speed;**
   - **QUIC requires only 1–2 handshakes.**
5. **Can easily maintain sessions seamlessly even when IP addresses change in mobile networks;**
   - **QUIC supports connection migration feature.**

So, RTR over QUIC (RTRoQUIC) can be used as an option to carry the RTR protocol !

Connection Management

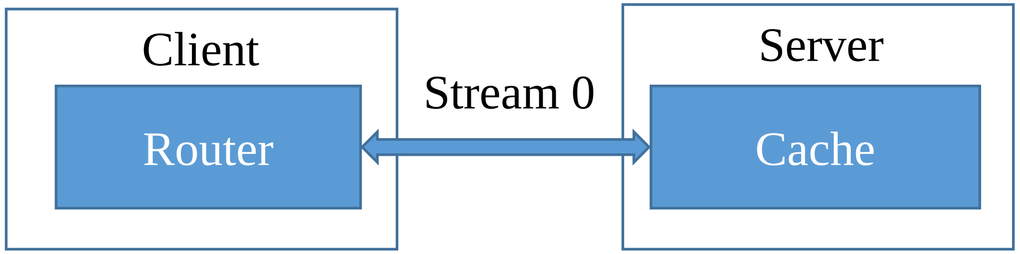
- **Connection Establishment**
  - **RTRoQUIC support is indicated by selecting ALPN token in the TLS handshake.**
  - **The router MUST act as the client meanwhile the cache must act as the server.**
- **Connection Termination**
  - **Apply QUIC connection termination process described in RFC9000.**
  - **List some considerations for RTRoQUIC connection termination, such as disabling the idle timeout to keep the QUIC connection persistent, closing the RTR session when unmatched RTR support version between router and cache.**

Stream mapping and usage

Currently, there are eleven kinds of RTR Protocol Data Units (PDUs), namely **Serial Notify PDU**, **Serial Query PDU**, **Reset Query PDU**, **Cache Response PDU**, **IPv4 Prefix PDU**, **IPv6 Prefix PDU**, **End of Data PDU**, **Cache Reset PDU**, **Router Key PDU**, **Error Report PDU** and **ASPA PDU**.

Among them, The IPv4 Prefix PDU, IPv6 Prefix PDU, Router Key PDU and ASPA PDU belong to the **Payload PDUs**.

Because of existing PDUs from Cache to Router and PDUs from Router to Cache, all RTR PDUs can be simply mapped into **one bidirectional QUIC stream** initiated by router.



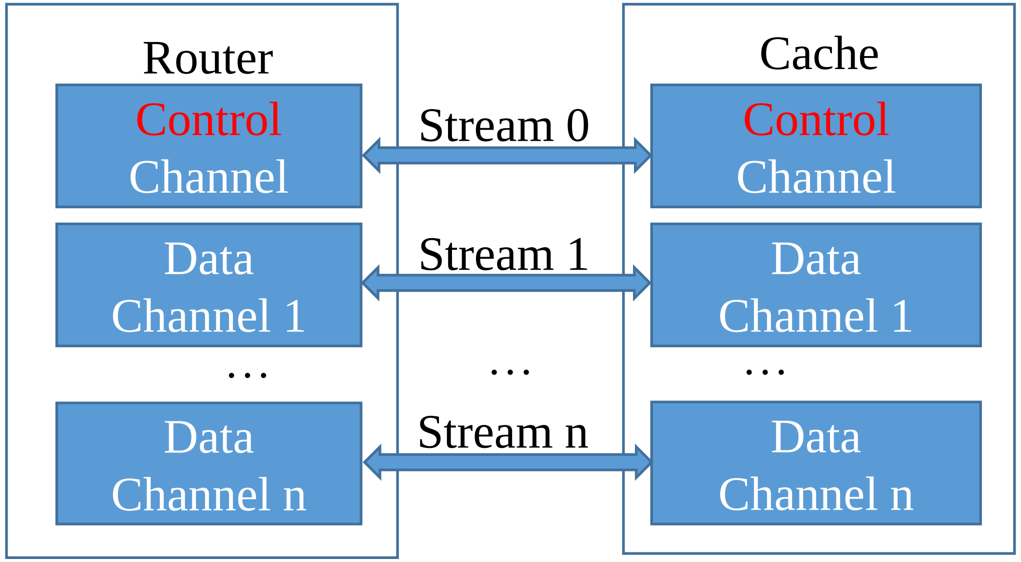
Stream mapping and usage

◆ **Multiple Streams Usage**

To improve transmission efficiency, RTR PDUs also can be mapped into multiple QUIC streams. A Control Channel and multiple Data Channels can be created.

The **Control Channel** is a bidirectional stream to transmit Serial Notify PDU, Serial Query PDU, Reset Query PDU, Cache Reset PDU and Error Report PDU, called Data PDUs. The **Control Channel** MUST be created immediately by the router after the connection establishment is done.

The **Data Channel** can be unidirectional or bidirectional stream to carry the Cache Response PDU, the payload PDUs and the End of Data PDU from the cache to the router in an orderly manner.



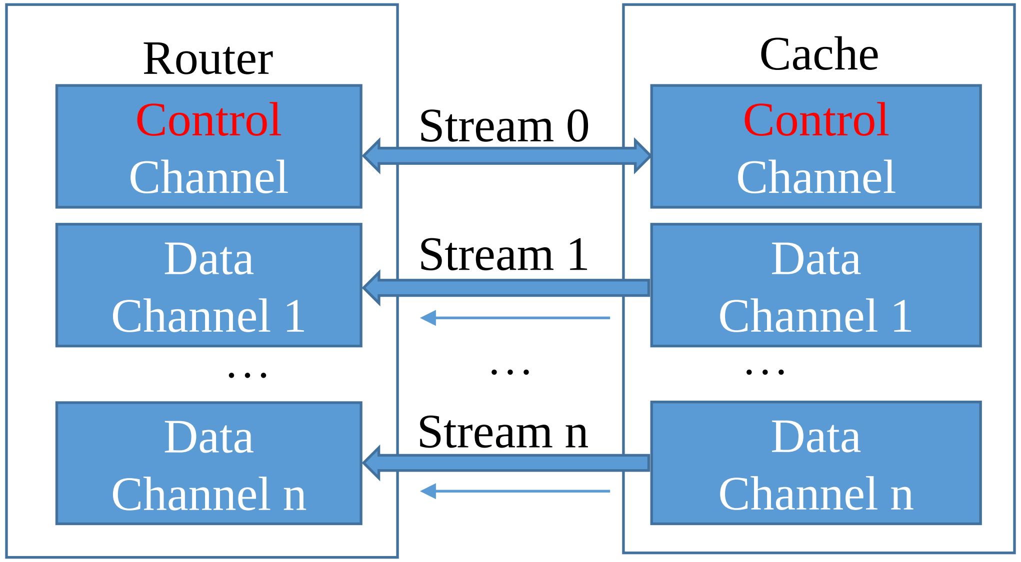
Stream mapping and usage

◆ **Multiple Streams Usage**

For the order of Data Channel PDUs, Cache Response PDU and End of Data PDU MUST be sent to all Data Channels (streams). The first-received Cache Response PDU and the last-received End of Data PDU from cache is valid. There are **two ways** to use the Data Channel.

Option 1:

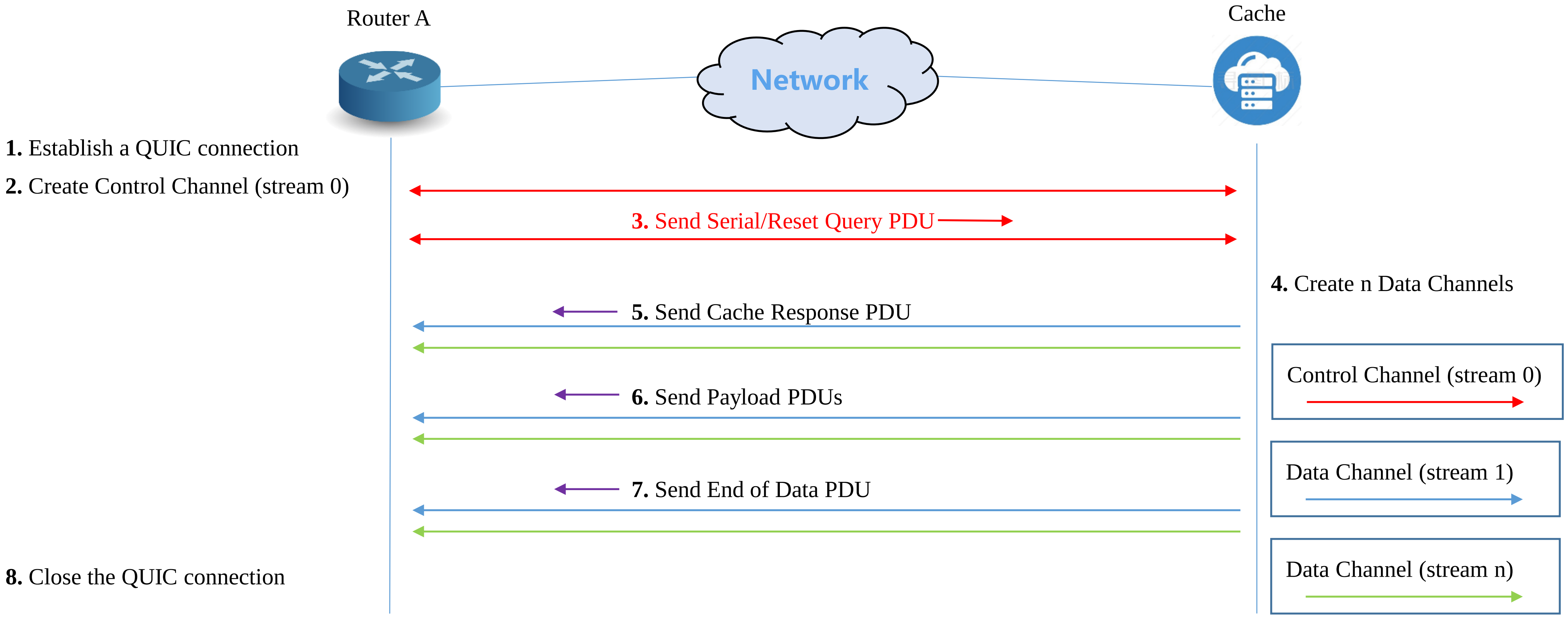
All Data Channel PDUs are mapped into one or more unidirectional stream initiated by the cache. These unidirectional streams SHOULD be created before the Cache sends the Cache Response PDU.



Stream mapping and usage

- **Multiple Streams Usage**

Option 1 -- Example:



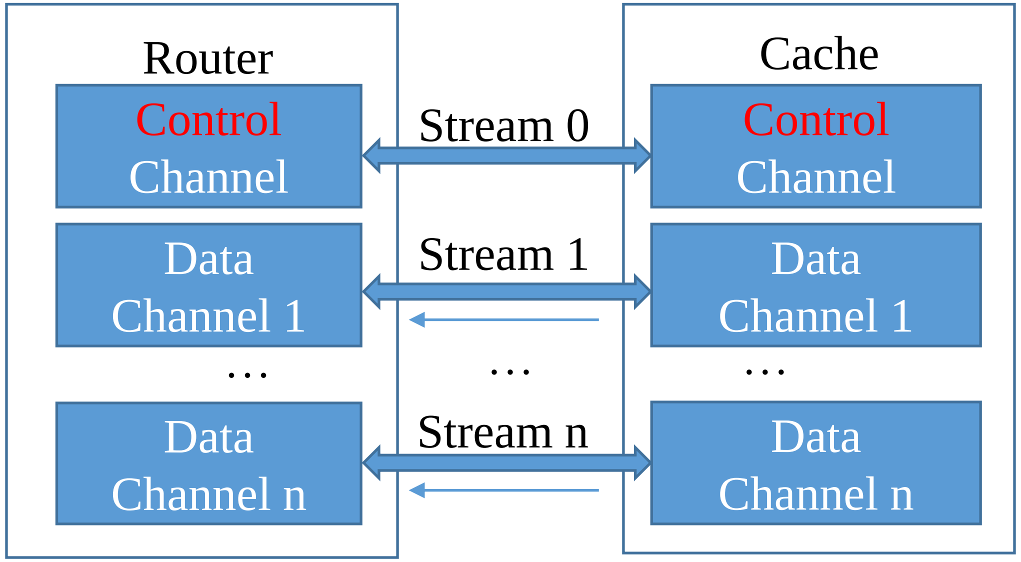
Stream mapping and usage

◆ **Multiple Streams Usage**

Option 2:

To improve operational flexibility, All Data Channel PDUs can be mapped into one or more bidirectional stream initiated by the router.

These bidirectional streams SHOULD be created before the Router sends the Serial or Reset Query over the Control Channel. The bidirectional data channels could be closed when the Router receives the End of Data which is the last of all Data Channels.



Stream mapping and usage

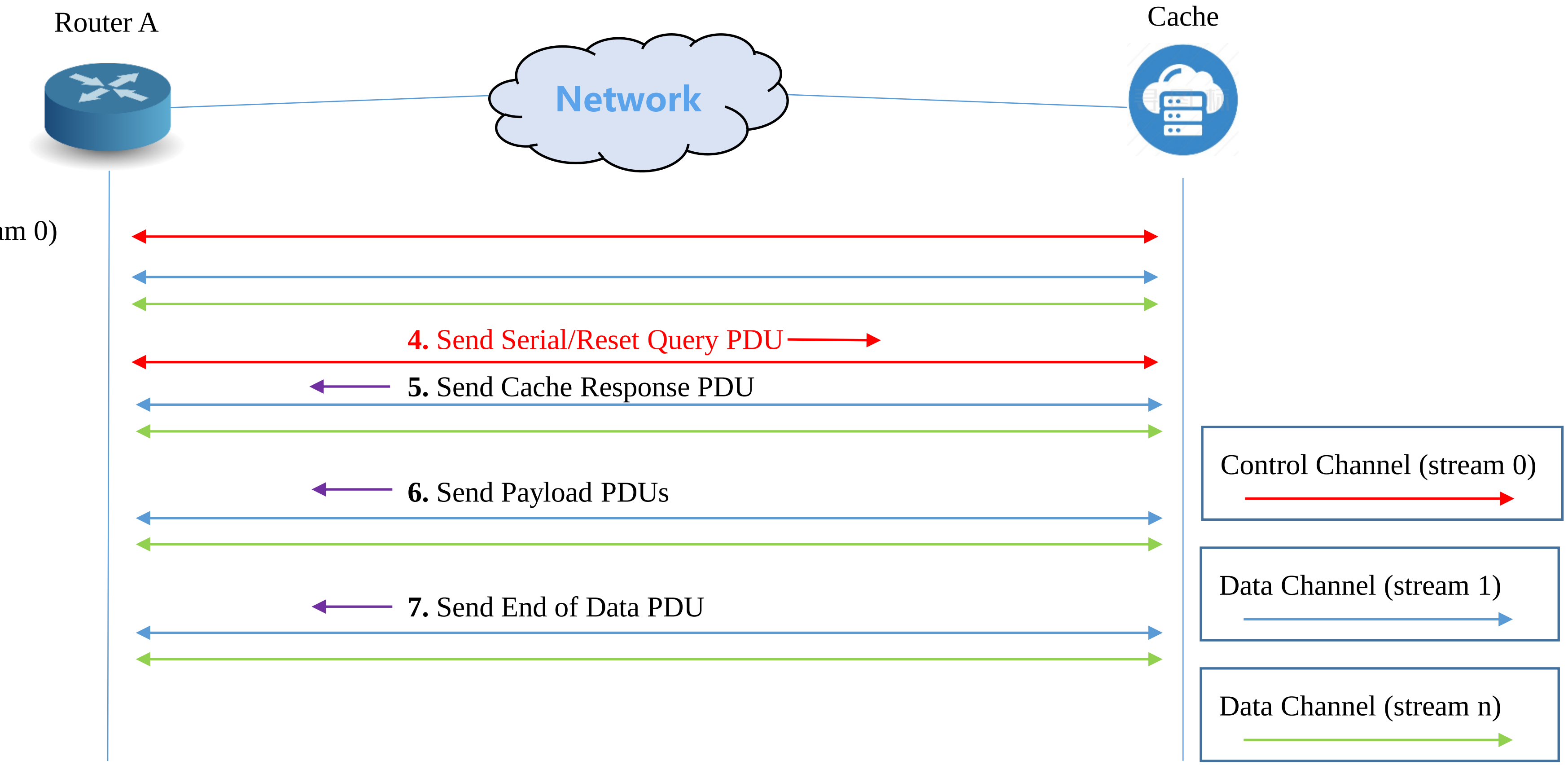
- **Multiple Streams Usage**

  Option 2 -- Example:

1. Establish a QUIC connection

2. Create Control Channel (stream 0)

3. Create n Data Channels



8. Destroy All Data Channels

9. Close the QUIC connection

Endpoint Authentication

- **Use TLS handshake authentication**
- **Apply third-party authentication**

Operational Considerations

- ✓ **Should provide a configuration mechanism to enable RTRoQUIC as optional transmission protocol on the RTR session. If QUIC connection is failed, the Router SHOULD attempt to establish an RTR session via other transport protocols.**

- ✓ **A configuration should be implemented to select single-stream or multi-stream QUIC transmission for RTR messages.**

- ✓ **For multi-stream QUIC transmission, the number of data channel SHOULD be configured by the Router or Cache according to actual performance requirements.**

IANA Considerations

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

  The “RTRoQ" string identifies RTRoQUIC:

  * Protocol: RTRoQUIC

  * Identification Sequence: 0x52 0x54 0x52 0x6f 0x51 ("RTRoQ")

Next Steps

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

Thanks!