

Using **NETCONF over QUIC** connection

draft-ietf-netconf-over-quic-06

draft-ietf-netconf-over-quic-07

Jinyou Dai(Fiberhome/CICT)

Shaohua Yu(Pengcheng Laboratory)

_Weiqiang Cheng(China Mobile)

Marc Blanchet(Viagenie)

Per Andersson(Ionio Systems)

IETF 125, Shenzhen

Updates since Montreal (IETF 124)

Stream type code avoided (section 4 based on comment from the list)

Acronym	Stream Type
C-BD	Client-Initiated, Bidirectional
S-BD	Server-Initiated, Bidirectional
C-UN	Client-Initiated, Unidirectional
S-UN	Server-Initiated, Unidirectional

✓ **Notification streams (section 4.2 based on comment from the list)**

Notification messages are initiated by the server and no reply is needed from the client. So the messages used to exchange notification data **MUST** be mapped into one unidirectional stream whose acronym is 'S-UN' according to Table 1.

Updates since Montreal (IETF 124)

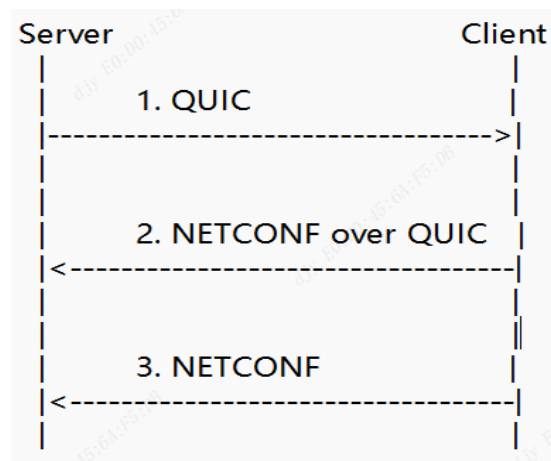
Chunked framing (section 7)

- ✓ In order to mitigate delimiter injection attacks chunked framing as defined in [RFC6242] is required for NETCONF over QUIC.
- ✓ The <hello> message MUST be followed by the character sequence RFC 5539 assumes that the end-of-message (EOM) sequence,]]>]]>>. Upon reception of the <hello> message, the receiving peer's QUIC layer conceptually passes the <hello> message to the Messages layer. If the :base:1.1 capability is advertised by both peers, the chunked framing mechanism defined in Section 4.2 of [[RFC6242]] is used for the remainder of the NETCONF session. Otherwise, the old end-of-message-based mechanism (see Section 4.3 of [[RFC6242]]) is used.

Updates since Montreal (IETF 124)

Call Home (section 5)

✓ Protocol-layer perspective



✓ specific case.

In the case of [RFC8071] Call home feature, where the NETCONF server initiates the transport connection to the NETCONF client, Table 1 will be used as follows: - the Client, referred in the Table, means the QUIC initiating party, therefore the NETCONF server and - the Server means the QUIC receiving party, therefore the NETCONF client.

Updates since Montreal (IETF 124)

'Session-stream mapping' (section 4.3)

- ✓ One NETCONF session is allowed per QUIC connection.
- ✓ The NETCONF session, except subscriptions, runs over a QUIC bidi-stream.
- ✓ NETCONF Notifications and Subscribed Notifications runs over one QUIC uni-stream per subscription.

Updates since Montreal (IETF 124)

Error codes (section 10)

✓ **Transport error code**

No new-added code.

✓ **Transport error code**

- * NO_NETCONF PROTOCOL ERROR (0x00): no NETCONF errors happens.
- * NETCONF CLOSE SESSION_ERROR (0x01): The peer tries to close a session which is not initiated by it.
- * NETCONF CLOSE STREAM ERROR (0x02): The peer tries to close a bidirectional stream when the NETCONF session is active.

Updates since Montreal (IETF 124)

➤ **Security considerations (Section 11)**

The security considerations described throughout [RFC8446] and [RFC6241] apply here as well. This document requires verification of server identity and client identity according to [RFC7589].

If invalid data or malformed messages are encountered, a robust implementation of this document **MUST** silently discard the message without further processing and then stop the NETCONF session.

➤ **References (Section 14)**

New-added references and modified references.

➤ **Nits fixing**

Remaining issues to be discussed

None

Updates for the next version

- **No confirmed further requirements for modification and clarification**
- **Elaborate the text if there are further feedbacks**

Next step

- Improve draft and address issues if any further comments or suggestions are going to be brought forward
- The authors would like to ask for WG last call after IETF 125 meeting

Thank you!