Using NETCONF over QUIC connection

draft-dai-netconf-quic-netconf-over-quic-02

IETF 114, Philadelphia

Jinyou Dai(Fiberhome/CICT)
Xueshun Wang(Fiberhome/CICT)
Yang Kou(Fiberhome/CICT)
Lifen Zhou(Fiberhome/CICT)
Connection management

➢ Draft Version Identification

➢ Connection setup
  • Version negotiation
  • Connection establishment

➢ Connection Closure

  • QUIC connection termination mode
  • NETCONFoQUIC consideration for connection termination
Stream mapping and usage-Netconf protocol layer

- **Layer**
  - (4) Content
  - (3) Operations
  - (2) Messages
  - (1) Secure Transport

- **Example**
  - Configuration data
    - <edit-config>
  - Notification data
    - <notification>
  - SSH, TLS, BEEP/TLS, SOAP/HTTP/TLS, ...
Stream mapping and usage-Uni&Bidirectional stream

Bidirectional stream between manager and agent

The NETCONF protocol uses an RPC-based communication model. So, the configuration data from manager to agent is exchanged based on '<RPC>' (the manager initiating) and '<RPC-Reply>' (sent by the agent) and so on. So the messages used to exchange configuration data should be mapped into one or more bidirectional stream whose stream type is 0.

Unidirectional stream from agent to manager

There are some notification data exchanged between the agent and the manager. Notification is a server-initiated message indicating that a certain event has been recognized by the server.

Notification messages are initiated by the agent and no reply is needed from the manager. So the messages used to exchange configuration data should be mapped into one unidirectional stream whose stream type is 3.
Endpoint Authentication

➢ Using QUIC handshake authentication
  • Server Identity
  • Client Identity

➢ Using third-party authentication
Server Identity

- The client MUST use the server hostname it used to open the connection (or the hostname specified in the TLS "server_name" extension [RFC5246]) as the value to compare against the server name as expressed in the server certificate. The client MUST NOT use any form of the server hostname derived from an insecure remote source.

- If a subjectAltName extension of type dNSName is present in the certificate, it MUST be used as the source of the server's identity.

- Matching is case-insensitive.

- A "*" wildcard character MAY be used as the leftmost name component in the certificate. For example, *.example.com would match a.example.com, foo.example.com, etc., but would not match example.com.

- If the certificate contains multiple names then a match with any one of the fields is considered acceptable.
IANA Considerations

➢ ALPN
A new registration for the identification of NETCONFoQUIC in the "Application Layer Protocol Negotiation (ALPN) Protocol IDs" registry established in [RFC7301].
    The "noq" string identifies NETCONFoQUIC:

    Protocol:  NETCONFoQUIC

    Identification Sequence:  0x6e 0x6f 0x71 ("noq")

    Specification:  This document

➢ UPD PORT
It is requested for IANA to reserve a UDP port TBD for 'NETCONF over QUIC'.
Thank you!