



DEPARTMENT OF INFORMATICS

Technische Universität München

MASTER'S THESIS IN INFORMATICS

**AUTOMATED IETF QUIC
INTEROPERABILITY MATRIX**

Angelin Rashmi Antony Rajan



DEPARTMENT OF INFORMATICS

Technische Universität München

MASTER'S THESIS IN INFORMATICS

AUTOMATED IETF QUIC INTEROPERABILITY MATRIX

Author:	Angelin Rashmi Antony Rajan
Supervisor:	Prof. Dr. -Ing Jrg Ott
Advisor:	M.Sc. Teemu Krkkinen
Submission Date:	August 1st, 2018

I hereby declare that this thesis is entirely the result of my own work except where otherwise indicated. I have only used the resources given in the list of references.

August 1st, 2018

Angelin Rashmi Antony Rajan

Acknowledgments

If someone helped you or supported you through your studies, this page is a good place to tell them how thankful you are.

Abstract

With the rapid growth of web based application and mobile revolution in recent years the main deciding factor for user experience is low latency. Quick UDP Internet Connections(QUIC) which runs on top of User Datagram Protocol(UDP) is a new transport protocol developed to overcome delay and also provide security to the data traffic. It is currently under development by IETF working group. Since QUIC runs on user space it is easy to deploy and each party can develop their own implementation from the specification. This thesis deals with analyzing the various IETF QUIC implementation and running various interoperability tests between them. Interoperability is the ability for two or more networks, systems, devices or applications to communicate.

Contents

Acknowledgements	vii
Abstract	ix
1. Introduction	1
1.1. Goals of the thesis	1
1.2. Outline of the thesis	1
2. Background	3
2.1. QUIC	3
2.2. IETF Implementation of QUIC	3
3. Design	5
3.1. Proposed Setup	5
3.2. Proposed Framework	5
3.3. Test Scenario	5
3.3.1. Version Negotiation	5
3.3.2. Handshake	6
3.3.3. Stream Data	7
3.3.4. Connection Close	7
3.3.5. Resumption	7
3.3.6. 0-RTT	7
3.3.7. Stateless Retry	7
4. Implementation	9
5. Evaluation	11
6. Conclusion	13
Appendix	17
A. Detailed Descriptions	17
Bibliography	19

1. Introduction

1.1. Goals of the thesis

The primary goal of this thesis is to design and implement an automated system that compiles, builds and run interoperability tests between all the QUIC IETF implementations. The results of the interoperability test is displayed in a matrix.

1.2. Outline of the thesis

In Chapter 2 we see how QUIC protocol works, objectives and problems in interoperability testing. In Chapter 3 we see the proposed setup for interoperability testing as well as the proposed framework. In chapter 4 and 5 we see the implementation of the proposed design and evaluation of it respectively.

2. Background

In this chapter we will look briefly on how QUIC protocol works and the various implementations which currently participate in IETF QUIC interop testing. In addition we will also see why we need inter-operability testing, objectives and problems in interoperability testing.

2.1. QUIC

QUIC protocol relays on TLS 1.3 for agreeing on cryptographic protocols and exchanging ephemeral keys. Draft-11 is under development.

2.2. IETF Implementation of QUIC

In the below table we can see the various quic implementations in different languages. Currently only 11 out of 13 implementations participate in interoperability test.

Implementation	Language	Public	Dependency	Current Draft
picoquic	C	Yes	picotls	
ngtcp2	C	Yes	picotls	
quant	C11	Yes	picotls	
mozquic	C++ with C interface	Yes		
quicly	C	Yes	picotls	
ATS	C++	Yes	picotls	
winquic	C	No		
pandora	C	Yes		
ngx-quic	C	No		
applequic	C, Objective C	No		
mvfst	C++	No		
minq	Go	Yes		
quicker	NodeJS/Typescript	Yes		

Table 2.1.: IETF QUIC Implementations

3. Design

In this chapter, the proposed setup for running intereoperability test and the frameowrk is discussed. We also see the test plan to test some features of QUIC protocol. We cover only the basic few test scenarios in this thesis.

3.1. Proposed Setup

The proposed design for running interoperability testing between a client and a server is shown in Figure 3.1. From the figure we can see that we can collect logs at two levels, capture the packets exchanged between them. These details can be used to validate the test cases

- Using Kernel Logs
- Using Server and Client QUIC Logs

Each implementation logs the states, packet sent/received, error message in their own way. There is no standard strucrure followed in these implementations. Thus, they require a lot of time in understanding how each implementation follow their logging mechanism.

- Using Wireshark

The current stable version of wireshark is 2.4.5. This still supports only Google QUIC. The latest development version 2.5.1 supports IETF QUIC. 0-RTT decryption is still not supported, so we will not be able to use Wireshark for testing that. For testing version negotiation, handhsake, and stream data wire shark packet capture can be used. This way of validating is not much useful because the QUIC payload is encrypted.

3.2. Proposed Framework

3.3. Test Scenario

3.3.1. Version Negotiation

QUIC Version Negotiation packet is sent by the server to the client in response to a client packet that contains a version which the server does not support. This test scenario can be

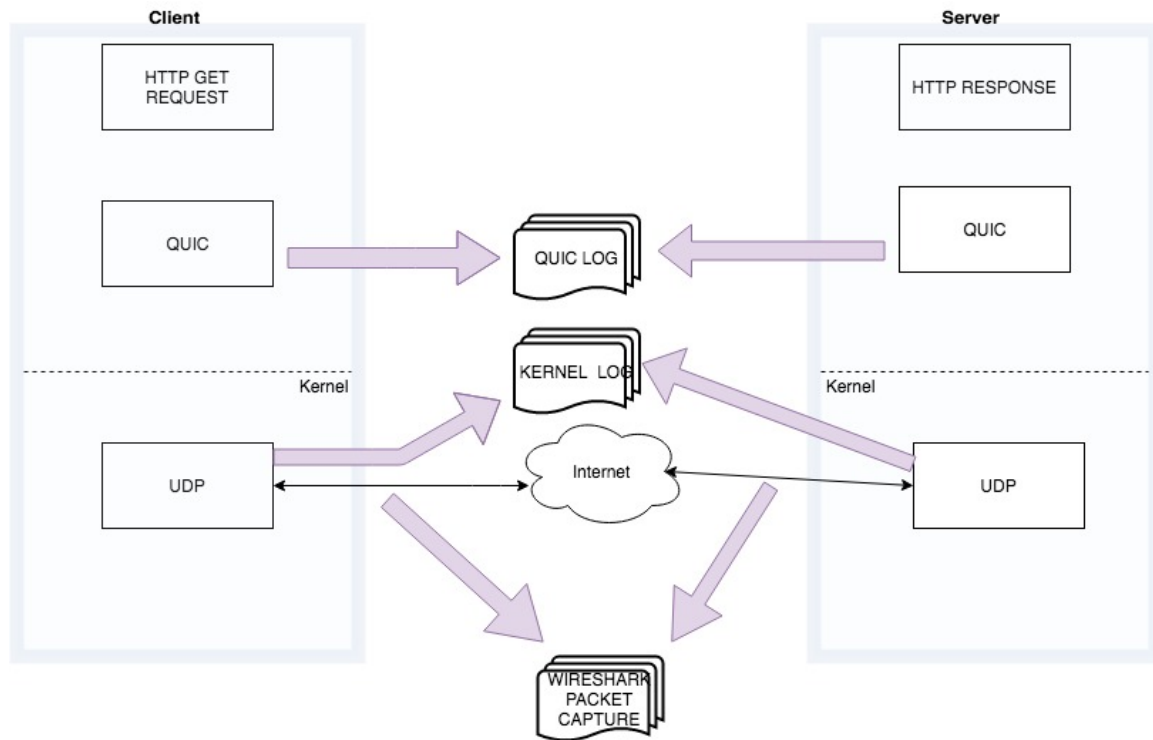


Figure 3.1.: Design

made by explicitly setting a version by the client which the server does not support and wait for the version negotiation packet from the server. Since version negotiation packets are not encrypted, it is possible to do validate this test case from wireshark capture as well. This can be done by checking if the packet is long header. Each implementation development happens at a different pace i.e. one implementation can be much more complete than other implementation. This makes the testing process difficult. Most(?) of the QUIC implementations are not backward compatible. So if implementation1 currently supports only draft-09 and implementation2 supports draft-10, then they cannot be tested against each other as the Version Negotiation always fails. This is bound to happen when both the draft specification and implementation are continuously evolving.

3.3.2. Handshake

Cryptographic Handshake packet is used by the server and client to exchange cryptographic keys after agreeing on the QUIC version. The first cryptographic message is sent to the server from client in Initial Packet.

3.3.3. Stream Data

3.3.4. Connection Close

CONNECTION_CLOSE frame is used to terminate a connection immediately. If there are any open streams in the connection that are not explicitly closed, they are implicitly closed when a connection is closed. The connection close frame has an error code which says why the connection was closed. For example, the server sets the error code as 0x02 when the server is busy and closes the connection. 0x01 specifies it is an internal error and cannot continue with the connection. 0x00 says that the connection is closed abruptly without any error.

3.3.5. Resumption

3.3.6. 0-RTT

ngtcp2 provides a way to resume a session and send 0-RTT packets in their example/client implementation. This is done by first establishing a connection with a server using the below command

```
./examples/client 127.0.0.1 4444 --session-file /Users/Rashmi/Documents/workspace/sample/ngtcp2-tp-file /Users/Rashmi/Documents/workspace/sample/ngtcp2/tp.txt
```

The above command stores the transport parameter and session ticket locally. This can later be used for resuming the session and sending 0-RTT packets.

3.3.7. Stateless Retry

4. Implementation

5. Evaluation

6. Conclusion

Appendix

A. Detailed Descriptions
