

FORMAL SPECIFICATION AND TESTING OF QUIC

Name : Raghav Gade

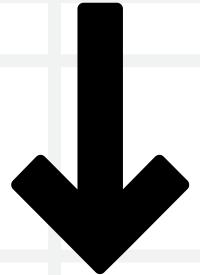
Roll no. : 20CS02003

Supervisor : Dr. Srinivas Pinisetty

School of Electrical and Computer Sciences

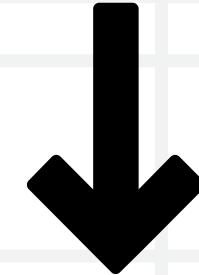


MOTIVATION



TCP & EVOLUTION

TCP/IP suite has been running the internet since TCP was standardized as RFC 761 in 1980. TCP evolution is slow due to kernel integration requiring widespread OS updates.



WHY QUIC?

QUIC is a new transport protocol that aims to be widely used over the Internet. It will serve as a basis to HTTP/3.

TCP+TLS+HTTP/2 STACK

- TCP provides connection-oriented, ordered communication with guaranteed delivery, retransmissions, and error correction.
- TLS encrypts data transmitted over TCP, ensuring confidentiality, integrity, and authentication.
- HTTP/2 runs over TLS and optimizes web performance by multiplexing multiple streams over a single connection.

1969

1981

1994

1999

2008

2015

ARPANET

TCP Standard

SSL

TLS 1.0

TLS 1.2

HTTP/2

QUIC+UDP+HTTP/3 STACK

- QUIC was designed to combine the speed of UDP with the reliability and security features typically associated with TCP, along with the encryption capabilities of TLS-1.3.
- It runs on top of UDP.
- UDP is just IP with ports.
- HTTP/3 runs over QUIC and improves upon HTTP/2 by removing reliance on TCP.

2013

Google develops QUIC

2016

QUIC submitted to IETF

2018

Draft-18

2020

Draft-29

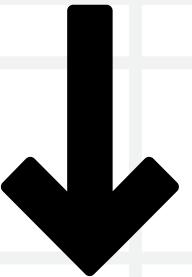
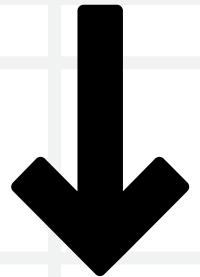
2021

QUIC & HTTP/3 standardised

2018+

Adoption by Facebook, Apple, Netflix Cloudflare

PROBLEM STATEMENT



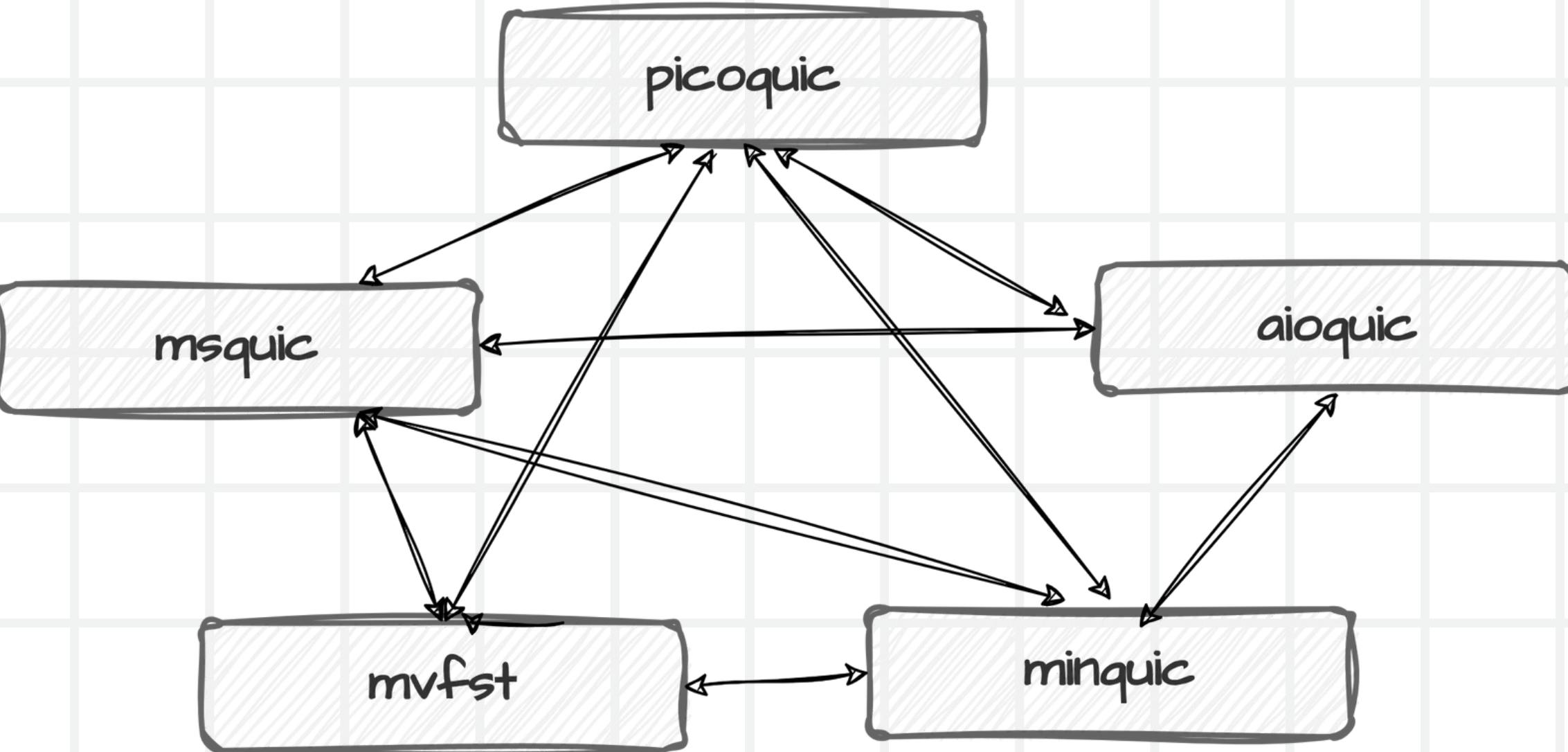
WHY DO WE NEED FORMAL SPECIFICATION?

Isn't checking interoperability of QUIC implementations enough.

WHAT KIND OF TESTING IS REQUIRED?

Isn't checking performance across different conditions with parameters like with parameters like throughput, latency, percentage of packet loss enough.

INTEROPERABILITY



Test QUIC traffic through different network setups with middleboxes, such as corporate firewalls, home routers, mobile networks across different implementations to check compatibility and performance

TESTING IMPLEMENTATIONS OF QUIC

Implementation	Language	Description
picoquic + picotls	C	Minimal implementation of QUIC aligned with IETF specifications. One of the best performers in interoperability testing. Needs picotls for encryption.
minquic + mint	go	Minq is a minimal implementation of QUIC which partly implements QUIC draft-05 with TLS 1.3 draft-20 or draft-21.
aioquic	Python	Library featuring an I/O-free API suitable for embedding in both clients and servers.

Given implementations are chosen as they were supposed to work with Ivy Model as mentioned in the paper.

PICOQUIC

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	::1	::1	QUIC	1294	Initial, DCID=579f4aa3c5bedf5c, SCID=6e09ac272a35a111, PKN: 72152, PING, CRYPTO, PADDING
4	0.002377673	::1	::1	QUIC	465	Protected Payload (KP0), DCID=171672a6d7c4f53f
5	0.002403875	::1	::1	QUIC	245	Protected Payload (KP0), DCID=171672a6d7c4f53f
7	0.002763798	::1	::1	QUIC	245	Protected Payload (KP0), DCID=171672a6d7c4f53f
9	0.003128148	::1	::1	QUIC	245	Protected Payload (KP0), DCID=171672a6d7c4f53f
11	0.004005863	::1	::1	QUIC	117	Protected Payload (KP0), DCID=171672a6d7c4f53f
12	0.004042017	::1	::1	QUIC	117	Protected Payload (KP0), DCID=171672a6d7c4f53f
14	0.005003174	::1	::1	QUIC	117	Protected Payload (KP0), DCID=171672a6d7c4f53f
15	0.005081826	::1	::1	QUIC	117	Protected Payload (KP0), DCID=171672a6d7c4f53f
16	0.005154639	::1	::1	QUIC	117	Protected Payload (KP0), DCID=171672a6d7c4f53f
18	0.005900219	::1	::1	QUIC	117	Protected Payload (KP0), DCID=171672a6d7c4f53f
19	0.005980797	::1	::1	QUIC	117	Protected Payload (KP0), DCID=171672a6d7c4f53f
21	0.007359339	::1	::1	QUIC	117	Protected Payload (KP0), DCID=171672a6d7c4f53f
22	0.007504182	::1	::1	QUIC	117	Protected Payload (KP0), DCID=171672a6d7c4f53f
23	0.007765908	::1	::1	QUIC	117	Protected Payload (KP0), DCID=171672a6d7c4f53f
24	0.007864310	::1	::1	QUIC	117	Protected Payload (KP0), DCID=171672a6d7c4f53f
26	0.009193263	::1	::1	QUIC	117	Protected Payload (KP0), DCID=171672a6d7c4f53f
27	0.009331928	::1	::1	QUIC	117	Protected Payload (KP0), DCID=171672a6d7c4f53f
28	0.010451752	::1	::1	QUIC	117	Protected Payload (KP0), DCID=171672a6d7c4f53f
30	0.011773808	::1	::1	QUIC	117	Protected Payload (KP0), DCID=171672a6d7c4f53f
31	0.012896243	::1	::1	QUIC	117	Protected Payload (KP0), DCID=171672a6d7c4f53f
33	0.013820161	::1	::1	QUIC	117	Protected Payload (KP0), DCID=171672a6d7c4f53f
34	0.014944166	::1	::1	QUIC	117	Protected Payload (KP0), DCID=171672a6d7c4f53f

QUIC IETF

- > QUIC Connection information
- [Packet Length: 92]
- 1.... = Header Form: Long Header (1)
- .0... = Fixed Bit: False
- ..10 = Packet Type: Handshake (2)
- Version: 1 (0x00000001)
- Destination Connection ID Length: 8
- Destination Connection ID: 171672a6d7c4f53f
- Source Connection ID Length: 8
- Source Connection ID: 6e09ac272a35a111
- Length: 67
- > [Expert Info (Warning/Decryption): Failed to create decryption context: Secrets are not available]
- Remaining Payload: 117c73d97a944728b4db6fce955c76244f5baeed1f82e56ef9e315da81e4dbc2a272e551...

QUIC IETF

- [Packet Length: 311]
- > QUIC Short Header DCID=171672a6d7c4f53f
- Remaining Payload: e5225235ac23126ea1224e24f10d424c0864c8b07da89e9060400869298f52ea61fe3ae7...

Loopback: lo <live capture in progress>

Packets: 337 · Displayed: 337 (100.0%)

Profile: Default

0-RTT TEST BETWEEN AIOQUIC AND PICOQUIC

No.	Time	Source	Destination	Protocol	Length	Info
24	0.267950	fe80::9c98:f5ff:fe4... ff02::16		ICMPv6	90	Multicast Listener Report Message v2
25	0.415995	193.167.0.100	193.167.100.100	QUIC	1242	Initial, DCID=f574cf66efdbf3fd, SCID=d97db3666c381b49, PKN: 0, CRYPTO
26	0.454342	193.167.100.100	193.167.0.100	QUIC	1294	Handshake, DCID=d97db3666c381b49, SCID=46c8d4109e7e8b36
27	0.454688	193.167.100.100	193.167.0.100	QUIC	481	Protected Payload (KPO), DCID=d97db3666c381b49
28	0.455869	193.167.100.100	193.167.0.100	QUIC	1482	Protected Payload (KPO), DCID=d97db3666c381b49
29	0.457271	193.167.0.100	193.167.100.100	QUIC	1242	Protected Payload (KPO), DCID=46c8d4109e7e8b36
30	0.459335	193.167.0.100	193.167.100.100	QUIC	75	Protected Payload (KPO), DCID=46c8d4109e7e8b36
31	0.489091	193.167.100.100	193.167.0.100	QUIC	225	Protected Payload (KPO), DCID=d97db3666c381b49
32	0.490288	193.167.0.100	193.167.100.100	QUIC	73	Protected Payload (KPO), DCID=46c8d4109e7e8b36
33	0.499195	193.167.100.100	193.167.0.100	QUIC	225	Protected Payload (KPO), DCID=d97db3666c381b49
34	0.509227	193.167.100.100	193.167.0.100	QUIC	225	Protected Payload (KPO), DCID=d97db3666c381b49
35	0.511947	fe80::42:c1ff:fea7:... ff02::16		ICMPv6	110	Multicast Listener Report Message v2
36	0.519326	193.167.100.100	193.167.0.100	QUIC	225	Protected Payload (KPO), DCID=d97db3666c381b49
37	0.520685	193.167.100.100	193.167.0.100	QUIC	72	Protected Payload (KPO), DCID=d97db3666c381b49
38	0.671968	fe80::42:c1ff:fea7:2 ff02::16		ICMPv6	110	Multicast Listener Report Message v2
39	0.672016	fe80::42:c1ff:fea7:2 ff02::2		ICMPv6	70	Router Solicitation from 02:42:c1:a7:00:02
40	0.767978	fe80::9c98:f5ff:fe4... ff02::16		ICMPv6	130	Multicast Listener Report Message v2
41	0.903964	fe80::42:c1ff:fea7:2 ff02::16		ICMPv6	110	Multicast Listener Report Message v2
42	1.023105	193.167.0.100	193.167.100.100	QUIC	1242	0-RTT, DCID=f90dd39df12caa51, SCID=c40e7e96bd5315a6
43	1.023337	193.167.0.100	193.167.100.100	QUIC	346	0-RTT, DCID=f90dd39df12caa51, SCID=c40e7e96bd5315a6
44	1.023526	193.167.0.100	193.167.100.100	QUIC	346	0-RTT, DCID=f90dd39df12caa51, SCID=c40e7e96bd5315a6
45	1.023701	193.167.0.100	193.167.100.100	QUIC	346	0-RTT, DCID=f90dd39df12caa51, SCID=c40e7e96bd5315a6
46	1.023877	193.167.0.100	193.167.100.100	QUIC	346	0-RTT, DCID=f90dd39df12caa51, SCID=c40e7e96bd5315a6

> User Datagram Protocol, Src Port: 53469, Dst Port: 443	0000 02 42 c1 a7 00 02 02 42 c1 a7 00 64 08 00 45 00 B
└ QUIC IETF	0010 04 cc f0 3d 40 00 40 11 5d cc c1 a7 00 64 c1 a7 ..
└ QUIC Connection information	0020 64 64 d0 dd 01 bb 04 b8 e9 11 c1 00 00 00 01 08 dd
[Packet Length: 721]	0030 f9 0d d3 9d f1 2c aa 51 08 c4 0e 7e 96 bd 53 15 ..
1... = Header Form: Long Header (1)	0040 a6 00 42 b7 ae f1 e4 2d 6b c6 5f 95 52 f7 c5 77 ..
.1... = Fixed Bit: True	0050 94 87 79 9f 1c 8f ba a4 8b 45 40 90 20 9b e1 fd ..
..00 = Packet Type: Initial (0)	0060 a5 a6 06 c9 a2 ad 65 7c 8f 69 d8 53 53 bb a3 7e ..
[.... 00.. = Reserved: 0]	0070 82 d2 bb 4b 56 0b ec d4 77 c5 7a 20 77 1e c6 0a ..
[.... .01 = Packet Number Length: 2 bytes (1)]	0080 6d d6 fb 71 43 83 33 f2 5b 35 28 c2 19 65 3a 3a m..
Version: 1 (0x00000001)	0090 5e da df d3 ee aa a2 82 54 41 6a f5 75 ff c4 da ..
Destination Connection ID Length: 8	00a0 a3 6b fe a5 3a ff 28 7b c3 7f c8 56 b0 b5 81 92 k..
Destination Connection ID: f90dd39df12caa51	00b0 30 97 42 23 0c ac 78 68 1f 29 cb ce c7 68 85 46 0..
Source Connection ID Length: 8	00c0 58 73 e1 41 75 ee 68 42 3e 43 51 25 bb a6 18 f3 Xs..
Source Connection ID: c40e7e96bd5315a6	00d0 31 73 89 60 d2 00 f4 f8 c5 10 2c a2 ac c9 58 1s..
Token Length: 0	00e0 68 d1 6c 82 26 c7 5b 35 a7 09 0b ad 16 a0 7f 86 h..
Length: 695	00f0 f1 dd fe 74 c4 68 20 aa f4 f3 f1 36 1e 16 9c 15 ..
[Packet Number: 0]	0100 6f 56 1e 88 92 df 8e b6 3e 43 51 25 bb a6 18 f3 oV..
Payload: e42d6bc65f9552f7c5779487799f1c8fbba48b454090209be1fda5a606c9a2ad657c8f69...	0110 b3 4b 2c 30 b7 d8 9c a7 bb 7b bc 41 36 4f aa 8e K..
	0120 d6 53 76 d6 ef fa 41 5c 0f 90 ee 3e be 18 44 S..
	0130 dd c1 0e 18 34 af 77 4f f1 bc 27 16 d2 25 4c 32 ..
	0140 78 6d bc a5 24 d7 1e f8 0b d4 9b da c3 e0 c2 03 xm..
	0150 8e bc 39 0c a1 48 7e ac 68 34 bc d0 66 76 68 95 ..

Frame (1242 bytes) Decrypted QUIC (677 bytes)

LITERATURE SURVEY

TAKING A LONG LOOK AT QUIC (2017)

by M. Kakhki, S. Jero

Performance evaluation and discusses performance comparisons between TCP and QUIC.

FORMAL SPECIFICATION AND TESTING OF QUIC (2019)

by K. L. McMillan and L. D. Zuck,
Verification of QUIC -draft 18 was done by
using a
methodology called "Network-centric
Compositional testing" using IVy.



VERIFYING QUIC IMPLEMENTATIONS USING IVY(2021)

by C. Crochet, T. Rousseaux

Extension to McMillan's work by using same methodology to produce formal model for draft-29 of QUIC

FORMAL ANALYSIS OF QUIC HANDSHAKE PROTOCOL USING SYMBOLIC MODEL CHECKING (2021)

by J. Zhang, X. Gao,
Security analysis of the
QUIC handshake protocol
based on symbolic
model checking using
ProVerif and Verifpal

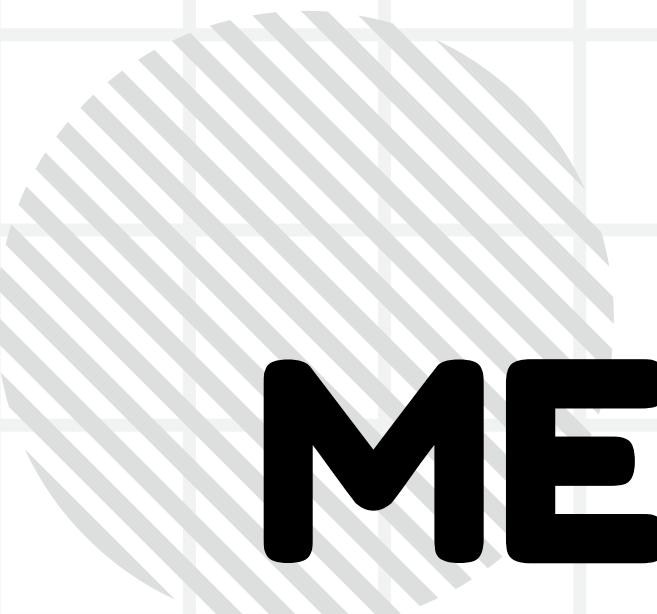
FORMAL VERIFICATION USING IVY

Safety Properties

- State that nothing bad should happen during the execution.
- An endpoint in the closing state MUST either discard packets received from an unvalidated address.
- Senders MUST NOT coalesce QUIC packets with different connection IDs into a single UDP datagram.

Liveness Properties

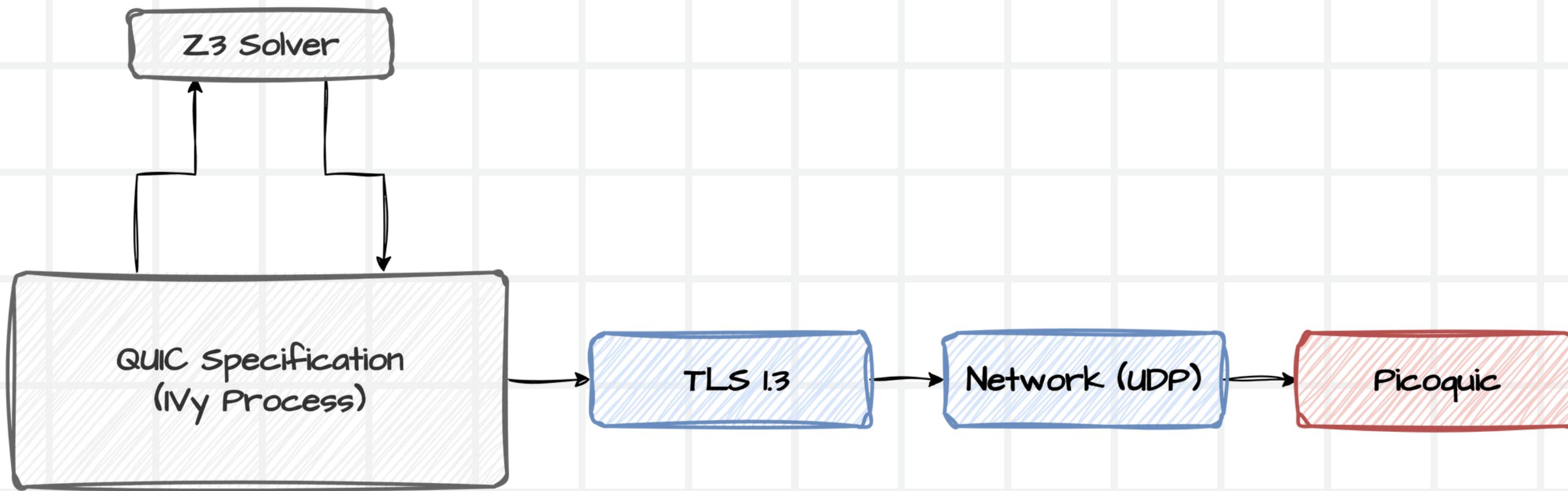
- Idle timeout or sending PING frames.
- Sending of PATH_CHALLENGE frames to get a PATH_MATCHING response. This is done for liveness check as well as connection migration.
- An endpoint should retransmit a lost packet.



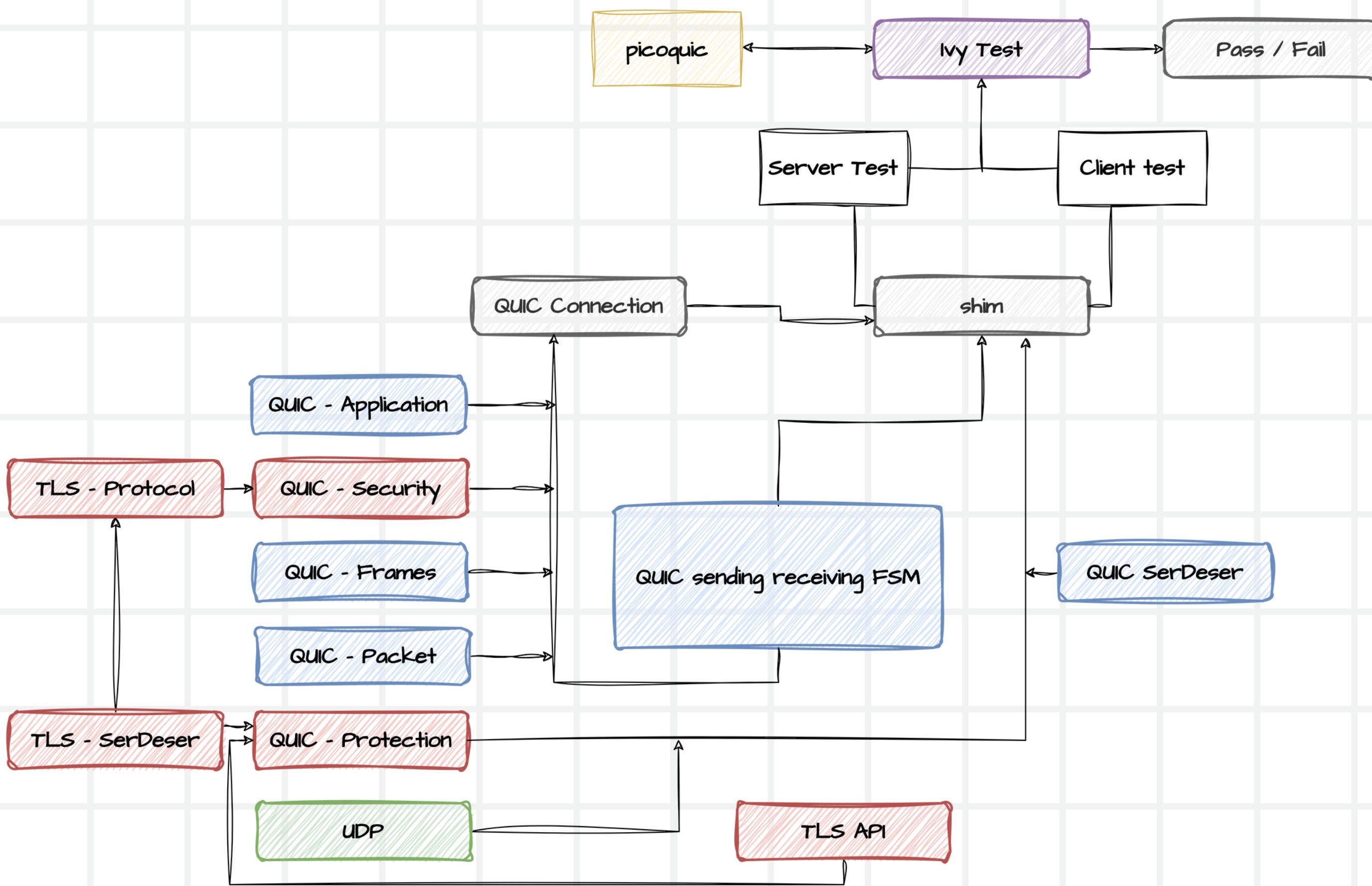
METHODOLOGY



FORMAL SPECIFICATION IN IVY



FORMAL SPECIFICATION IN IVY



RESULTS

- They listed a total of 268 `MUST` properties in the RFC out of which 82 are implemented by combining two researches.
- The reason why so many RFC properties are not verified because because either that statements are ambiguous, access to internal state of implementation or undecidable properties.
- The results are obtained through client and server tests written for implementations.
- If the process that we are testing is sending a message that will break the specification, we conclude that it is either its fault or that the specification is too weak.

COMPARISONS

Dafny

- Dafny is more suited for program correctness rather than protocol behavior.
- Harder to model time-dependent failures or concurrent packet exchanges.
- It requires you to define functions precisely, whereas QUIC needs non-determinism

TLA +

- TLA+ is more suited for specification & model checking.
- Verifying both safety and liveness properties.
- Specification can be extended to work for different network conditions.
- Developer community.

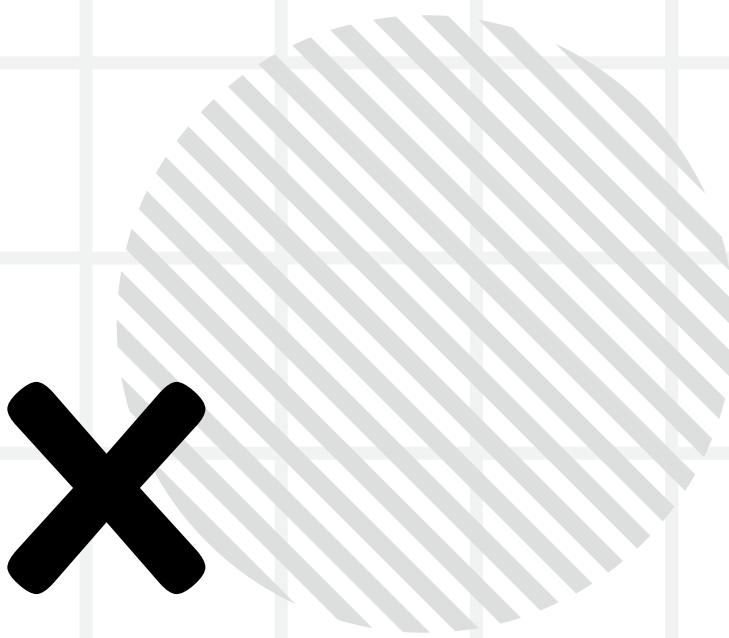
REFERENCES

- K. L. McMillan and L. D. Zuck, “Formal specification and testing of quic,” in Proceedings of the ACM Special Interest Group on Data Communication (SIGCOMM ’19). New York, NY, USA: Association for Computing Machinery, 2019, pp. 227–240. [Online]. Available: <https://doi.org/10.1145/3341302.3342087>
- C. Crochet, T. Rousseaux, M. Piraux, J.-F. Sambon, and A. Legay, “Verifying quic implementations using ivy,” in Proceedings of the 2021 Workshop on Evolution, Performance and Interoperability of QUIC (EPIQ ’21). New York, NY, USA: Association for Computing Machinery, December 2021, pp. 35–41. [Online]. Available: <https://doi.org/10.1145/3488660.3493803>
- A. M. Kakhki, S. Jero, D. Choffnes, C. Nita-Rotaru, and A. Mislove, “Taking a long look at quic: An approach for rigorous evaluation of rapidly evolving transport protocols,” in Proceedings of the 2017 Internet Measurement Conference (IMC ’17). New York, NY, USA: Association for Computing Machinery, November 2017, pp. 290–303. [Online]. Available: <https://doi.org/10.1145/3131365.3131368>
- J. Zhang, X. Gao, L. Yang, T. Feng, D. Li, and Q. Wang, “A systematic approach to formal analysis of quic handshake protocol using symbolic model checking,” *Security and Communication Networks*, vol. 2021, pp. 1–13, August 2021, academic Editor: Ruhul Amin. [Online]. Available: <https://doi.org/10.1155/2021/1630223>
- X. Zhang, S. Jin, Y. He, A. Hassan, Z. M. Mao, F. Qian, and Z.-L. Zhang, “Quic is not quick enough over fast internet,” in Proceedings of the ACM Web Conference 2024 (WWW ’24). New York, NY, USA: Association for Computing Machinery, May 2024, pp. 2713–2722. [Online]. Available: <https://doi.org/10.1145/3589334.3645323>

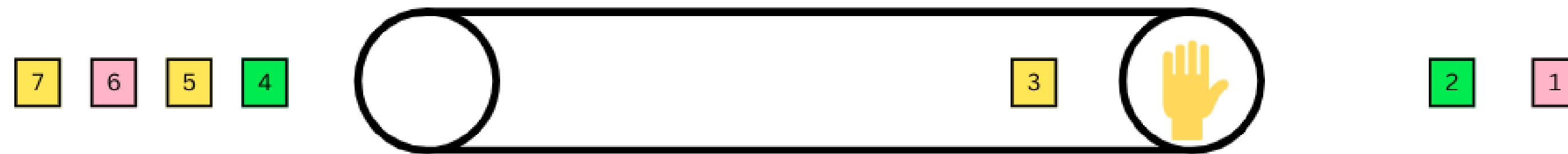
THANK YOU



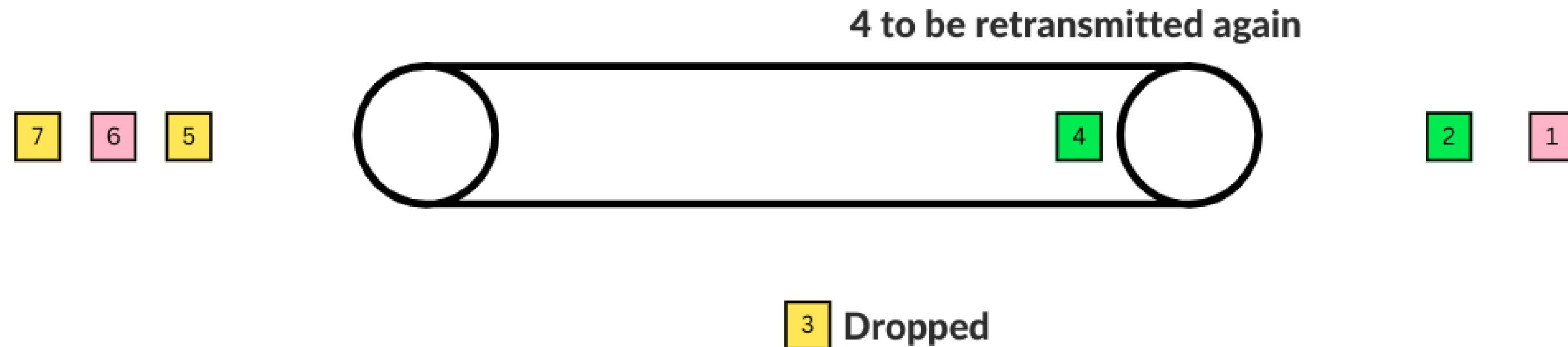
APPENDIX



TCP HEAD OF LINE BLOCKING



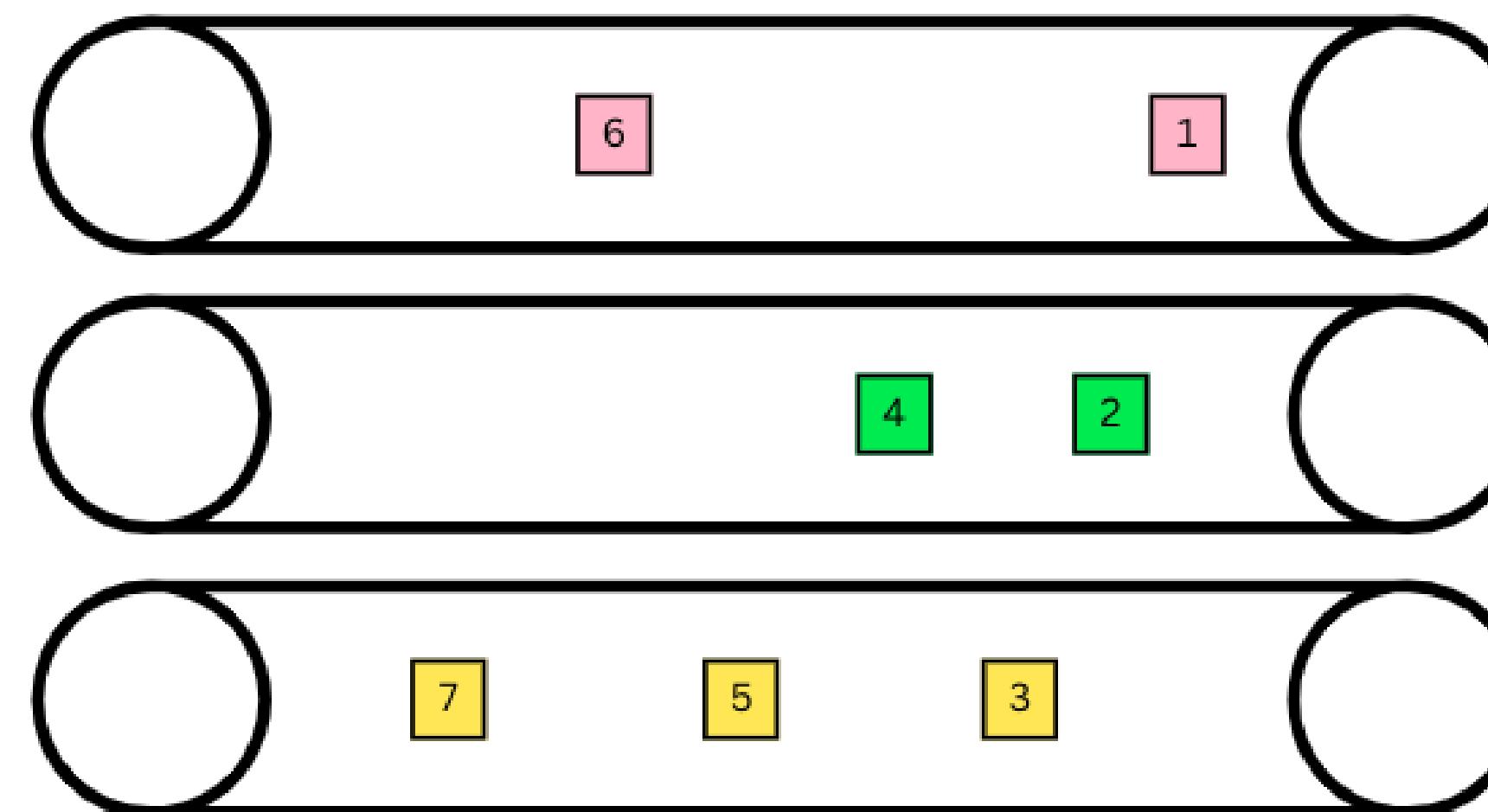
- HTML
- CSS
- JS



QUIC SOLUTION TO HOL

Independent streams over a connection

- █ HTML
- █ CSS
- █ JS

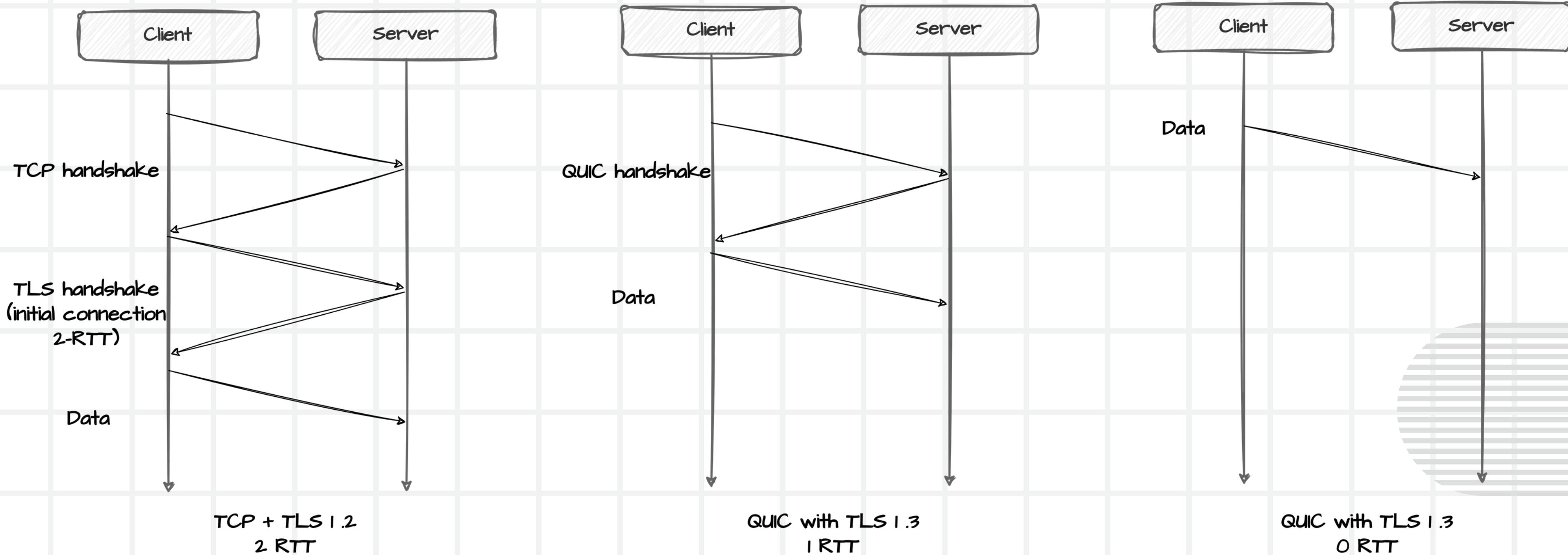


CONNECTION MIGRATION



QUIC uses connection ID (20 bytes) and UDP allows the client to change its source address without breaking the session while TCP needs to form new.

RTT COMPARISON



OTHER FEATURES

- TCP has been integrated into kernel-space since its early implementation in operating systems in the 1980s.
- Updating TCP in kernel space requires OS updates and kernel recompilation, making protocol evolution slow.
- QUIC is implemented in user-space which helps developers to push frequent updates with new features and optimizations without having to wait for kernel updates.
- Therefore, there exist several implementations of QUIC based on one's use case and needs.

AIOQUIC+PICOQUIC+MINQUIC TERMINAL OUTPUTS

```
examples$ python examples/http3_server.py --certificate tests/ssl_cert.pem --private-key tests/ssl_key.pem
2024-11-29 00:27:24,669 INFO quic [5c8549c3e18d0235] Negotiated protocol version 0x00000001 (VERSION_1)
2024-11-29 00:27:24,674 INFO quic [5c8549c3e18d0235] ALPN negotiated protocol hq-interop
2024-11-29 00:27:24,675 INFO quic [5c8549c3e18d0235] HTTP request GET /
2024-11-29 00:27:24,678 INFO quic [5c8549c3e18d0235] Connection close received (code 0x100, reason )
2024-11-29 00:27:33,778 INFO quic [0dfa2e5fb7fc4c7] Negotiated protocol version 0x00000001 (VERSION_1)
2024-11-29 00:27:33,783 INFO quic [0dfa2e5fb7fc4c7] ALPN negotiated protocol h3
2024-11-29 00:27:33,784 INFO quic [0dfa2e5fb7fc4c7] HTTP request GET /
2024-11-29 00:27:33,784 INFO quic [0dfa2e5fb7fc4c7] HTTP request GET /style.css
2024-11-29 00:27:33,787 INFO quic [0dfa2e5fb7fc4c7] Connection close received (code 0x100, reason )
examples
  - examples
    - htdocs
    - templates
  - README.rst
HTTP/3
HTTP/3 server
```

```
source aioquic-env/bin/activate
python examples/http3_client.py --ca-certs tests/pycacert.pem --legacy-http https://localhost:4433/
2024-11-29 00:27:24,672 INFO quic [5c8549c3e18d0235] Negotiated protocol version 0x00000001 (VERSION_1)
2024-11-29 00:27:24,674 INFO quic [5c8549c3e18d0235] ALPN negotiated protocol hq-interop
2024-11-29 00:27:24,674 INFO client New session ticket received
2024-11-29 00:27:24,678 INFO client Response received for GET / : 1106 bytes in 0.0 s (2.693 Mbps)
2024-11-29 00:27:24,678 INFO quic [5c8549c3e18d0235] Connection close sent (code 0x100, reason )
python examples/http3_client.py --ca-certs tests/pycacert.pem https://localhost:4433/
2024-11-29 00:27:33,781 INFO quic [0dfa2e5fb7fc4c7] Negotiated protocol version 0x00000001 (VERSION_1)
2024-11-29 00:27:33,782 INFO quic [0dfa2e5fb7fc4c7] ALPN negotiated protocol h3
2024-11-29 00:27:33,783 INFO client New session ticket received
2024-11-29 00:27:33,784 INFO client Response received for GET / : 1196 bytes in 0.0 s (8.251 Mbps)
2024-11-29 00:27:33,785 INFO client Push received for GET /style.css : 0 bytes
2024-11-29 00:27:33,785 INFO quic [0dfa2e5fb7fc4c7] Connection close sent (code 0x100, reason )
~/C/m/impl/aioquic main ?1 aioquic-env
```

```
picoquic:picoquicdemo
579f4aa3c5bedf5c: stream 8, offset 1076289, length 1407, fin = 0: 5a5a5a5a5a5a5a5a...
579f4aa3c5bedf5c: T= 0.039795, cwin: 94473, flight: 24480, nb_ret: 0, rtt_min: 61, rtt: 622, rtt_var: 979, ma
x_ack_delay: 0, state: 14
579f4aa3c5bedf5c: Sending 1440 bytes to [0:0:0:0:0:0:1]:49363 at T=0.039795 (113111b6e)
579f4aa3c5bedf5c: Sending packet type: 6 (1rtt protected), S0, Q0, quic_server_test_max_ivy
579f4aa3c5bedf5c: <6e09ac272a35a111>, Seq: 773 (773), Phi: 0, quic_client_test_stream_ivy
579f4aa3c5bedf5c: Prepared 1413 bytes
579f4aa3c5bedf5c: stream 8, offset 1077696, length 1407, fin = 0: 5a5a5a5a5a5a5a5a...
579f4aa3c5bedf5c: T= 0.039795, cwin: 94473, flight: 25920, nb_ret: 0, rtt_min: 61, rtt: 622, rtt_var: 979, ma
x_ack_delay: 0, state: 14
579f4aa3c5bedf5c: Sending 1440 bytes to [0:0:0:0:0:0:1]:49363 at T=0.039795 (113111b6e)
579f4aa3c5bedf5c: Sending packet type: 6 (1rtt protected), S0, Q0, picoquic
579f4aa3c5bedf5c: <6e09ac272a35a111>, Seq: 774 (774), Phi: 0,
579f4aa3c5bedf5c: Prepared 1413 bytes
~/Code/mtp/impl:go README MIT license MIT license
go run ming/bin/server/main.go
2024/11/29 11:05:48 New connection
2024/11/29 11:05:48 State changed to StateEstablished
2024/11/29 11:05:48 State changed to StateClosing
2024/11/29 11:05:54 State changed to StateClosed
WARNING
Minq is absolutely not suitable for any kind of production use and should only be used for testing purposes.
In particular, it explicitly doesn't validate certificates.
```

```
picoquic:zsh
source ~/ivy_env/bin/activate
./picoquicdemo localhost
Starting Picoquic (v1.1.28.0) connection to server = localhost, port = 4443
Testing scenario: <0:index.html;4:test.html;8:/1234567;12:main.jpg;16:war-and-peace.txt;20:en/latest;/2
4:/file-123K>
Max stream id bidir remote before start = 0 (0)
Starting client connection. Version = 1, I-CID: 579f4aa3c5bedf5c
Max stream id bidir remote after start = -4 (0)
Waiting for packets.
Client port (AF=10): 54208.
Negotiated ALPN: h3
Almost ready!

Connection established. Version = 1, I-CID: 579f4aa3c5bedf5c, verified: 1
Opening stream 0 to GET /index.html
Stream 0 ended after 386 bytes
~/Code/mtp/impl:zsh
go run ming/bin/client/main.go
2024/11/29 11:05:48 PID= 8670
2024/11/29 11:05:48 Client conn id=fba6142dd7
2024/11/29 11:05:48 State changed to StateWaitServerInitial
2024/11/29 11:05:48 State changed to StateWaitServerFirstFlight
2024/11/29 11:05:48 State changed to StateEstablished
2024/11/29 11:05:48 Connection established server CID = 8fd99c249d
2024/11/29 11:05:54 State changed to StateClosing
2024/11/29 11:05:54 Error Connection is closing
~/Code/mtp/impl 5s ivy_env
```

AIOQUIC

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	::1	::1	QUIC	1262	Initial, DCID=fe29c8ff1d89f179, SCID=ba067e86fadafcb, PKN: 0, CRYPTO
2	0.004952479	::1	::1	QUIC	1262	Handshake, DCID=ba067e86fadafcb, SCID=ade34b1c33930023
3	0.004961229	::1	::1	QUIC	1240	Handshake, DCID=ba067e86fadafcb, SCID=ade34b1c33930023
4	0.004964894	::1	::1	QUIC	215	Protected Payload (KP0), DCID=ba067e86fadafcb
5	0.005739182	::1	::1	QUIC	1262	Handshake, DCID=ade34b1c33930023, SCID=ba067e86fadafcb
6	0.007243768	::1	::1	QUIC	419	Protected Payload (KP0), DCID=ade34b1c33930023
7	0.007649271	::1	::1	QUIC	97	Protected Payload (KP0), DCID=ade34b1c33930023
8	0.007800708	::1	::1	QUIC	124	Protected Payload (KP0), DCID=ade34b1c33930023
9	0.007831301	::1	::1	QUIC	294	Protected Payload (KP0), DCID=ba067e86fadafcb
10	0.008420231	::1	::1	QUIC	144	Protected Payload (KP0), DCID=ba067e86fadafcb
11	0.008675042	::1	::1	QUIC	94	Protected Payload (KP0), DCID=ade34b1c33930023
12	0.010345661	::1	::1	QUIC	142	Protected Payload (KP0), DCID=ba067e86fadafcb
13	0.010438760	::1	::1	QUIC	1262	Protected Payload (KP0), DCID=ba067e86fadafcb
14	0.010442803	::1	::1	QUIC	127	Protected Payload (KP0), DCID=ba067e86fadafcb
15	0.010970886	::1	::1	QUIC	93	Protected Payload (KP0), DCID=ade34b1c33930023

> Frame 1: 1262 bytes on wire (10096 bits), 1262 bytes captured (10096 bits) on interface lo, id 0
> Ethernet II, Src: Xerox_00:00:00 (00:00:00:00:00:00), Dst: Xerox_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 6, Src: ::1, Dst: ::1
> User Datagram Protocol, Src Port: 49823, Dst Port: 4433
 `- QUIC IETF
 `- QUIC Connection information
 [Packet Length: 524]
 `- 1... = Header Form: Long Header (1)
 `- .1... = Fixed Bit: True
 `- ..00 = Packet Type: Initial (0)
 `- [.... 00.. = Reserved: 0]
 `- [.... ..01 = Packet Number Length: 2 bytes (1)]
 `- Version: 1 (0x00000001)
 `- Destination Connection ID Length: 8
 `- Destination Connection ID: fe29c8ff1d89f179
 `- Source Connection ID Length: 8
 `- Source Connection ID: ba067e86fadafcb
 `- Token Length: 0
 `- Length: 498
 `- [Packet Number: 0]
 `- Payload: ee9b39ff2247f4b578e0f7ef4963d2eeee84cd59472e84f7783bc4efbe486dd6ea0cbe75...
 `- CRYPTO
 `- QUIC IETF
 `- [Expert Info (Note/Protocol): (Random) padding data appended to the datagram]
 `- [(Random) padding data appended to the datagram]
 `- [Severity level: Note]

Frame (1262 bytes) Decrypted QUIC (480 bytes)

Loopback: lo: <live capture in progress> | Packets: 15 · Displayed: 15 (100.0%) | Profile: Default

MINQUIC

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	127.0.0.1	127.0.0.1	UDP	1243	40441 → 4433 Len=1201
2	0.003350172	127.0.0.1	127.0.0.1	UDP	213	4433 → 40441 Len=171
3	0.003595129	127.0.0.1	127.0.0.1	UDP	676	4433 → 40441 Len=634
4	0.003784181	127.0.0.1	127.0.0.1	UDP	85	40441 → 4433 Len=43
5	0.005575573	127.0.0.1	127.0.0.1	UDP	124	40441 → 4433 Len=82
6	0.005939226	127.0.0.1	127.0.0.1	UDP	84	4433 → 40441 Len=42
7	0.006007277	127.0.0.1	127.0.0.1	UDP	128	4433 → 40441 Len=86
8	0.106608895	127.0.0.1	127.0.0.1	UDP	73	40441 → 4433 Len=31

```
>- Frame 1: 1243 bytes on wire (9944 bits), 1243 bytes captured (9944 bits) on interface lo, id 0
>- Ethernet II, Src: Xerox_00:00:00 (00:00:00:00:00:00), Dst: Xerox_00:00:00 (00:00:00:00:00:00)
>- Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
└╼ User Datagram Protocol, Src Port: 40441, Dst Port: 4433
    └── Source Port: 40441
    └── Destination Port: 4433
    └── Length: 1209
    └── Checksum: 0x02cd [unverified]
        └── [Checksum Status: Unverified]
        └── [Stream index: 0]
    >-[Timestamps]
    └── UDP payload (1201 bytes)
    └╼ Data (1201 bytes)
        └── Data: ffff0000f5215850538195a39e4b1825d3a5100449b7aa44ff868f0c4c1ff1c612a8627...
            └── [Length: 1201]
```

0000	00	00	00	00	00	00	00	00	00	00	00	00	00	08	00	45	00
0010	04	cd	d5	e2	40	00	40	11	62	3b	7f	00	00	01	7f	00	..
0020	00	01	9d	f9	11	51	04	b9	02	cd	ff	ff	00	00	0f	52	..
0030	15	85	05	38	19	5a	39	e4	b1	82	5d	3a	51	00	44	9b	..
0040	7a	a4	4f	f8	68	f0	c4	c1	ff	1c	61	2a	86	27	2a	c5	z..
0050	f8	65	1d	67	2e	7e	70	8a	a6	09	8b	94	c3	df	05	cb	..e
0060	85	4a	f1	2e	aa	69	a8	c3	d9	70	78	6e	34	0d	2d	74	.J
0070	03	c5	4e	d9	ff	0d	cb	16	19	38	09	3d	bf	bb	7f	70	..M
0080	7c	77	02	4b	d6	65	9e	28	65	a5	87	2e	9c	0f	32	fa	w
0090	95	0a	54	d5	6d	e5	fd	3b	9d	6f	c7	c2	d3	9b	96	34	..
00a0	bd	0f	5e	b9	e6	1a	34	cc	ed	93	14	48	67	0a	93	61	..
00b0	e4	cf	23	0f	16	69	a3	a5	ee	ff	5f	a5	4a	52	e7	2a	..
00c0	c5	a8	8c	f8	47	ed	1a	fe	25	de	2d	71	dd	e4	31	e0	..
00d0	53	a1	24	0d	25	76	b1	2a	74	5a	87	4d	a2	5e	d0	92	S..S
00e0	3e	6f	36	f8	91	79	0f	53	ac	2e	7e	5c	32	4c	17	5e	>o..
00f0	55	dc	a1	77	a4	15	c4	89	09	a6	95	7f	a6	b3	fc	62	U..
0100	75	79	e7	d3	03	62	b3	4d	ed	79	3e	fc	b8	d6	7e	5d	uy
0110	d1	47	d2	e8	3f	9e	7a	64	ab	f0	14	7f	8d	24	0c	43	.G
0120	ae	6b	7b	ae	67	3c	51	1e	44	fa	2c	3f	85	7b	6a	54	.k..
0130	48	38	26	91	a3	98	a2	29	45	52	ec	95	6d	2e	3e	8e	H8..
0140	0c	63	ee	e4	4a	7d	ec	20	bd	04	5b	42	7a	40	b4	00	.c..
0150	37	b7	55	0b	9f	3d	9e	52	96	b5	51	4a	f9	5e	5c	23	7..U
0160	bt	43	86	37	d3	23	8c	16	94	aa	68	72	e1	47	cd	7a	.C..
0170	77	a3	d8	27	eb	e1	98	c6	23	37	99	8c	f5	ac	7d	60	W..
0180	16	d2	fb	10	e0	bb	66	66	5b	6b	2a	95	1b	a3	9c	16	..



INTEROPERABILITY TESTS



UNSUCCESSFUL HANDSHAKE TEST BET'N MSQUIC (IMPL BY MICROSOFT) & MVFST (IMPL BY META)

No.	Time	Source	Destination	Protocol	Length	Info
19	0.211094	193.167.0.2	193.167.0.100	TCP	54	57832 - 58948 [RST] Seq=1 Win=8388480 Len=0
20	0.218959	193.167.0.100	193.167.100.100	QUIC	1262	Initial, DCID=fb4dfa5ed7e70feb, PKN: 0, CRYPTO, PADDING
21	0.257113	193.167.100.100	193.167.0.100	QUIC	1274	Initial, SCID=400000d057b3a35a, PKN: 10456286, CRYPTO, ACK, PADDING
22	0.257742	193.167.100.100	193.167.0.100	QUIC	791	Handshake, SCID=400000d057b3a35a
23	0.257780	193.167.100.100	193.167.0.100	QUIC	122	Protected Payload (KP0)
24	0.258099	193.167.0.100	193.167.100.100	QUIC	126	Handshake, DCID=400000d057b3a35a
25	0.258128	193.167.0.100	193.167.100.100	QUIC	1294	Protected Payload (KP0), DCID=400000d057b3a35a
26	0.258209	193.167.0.100	193.167.100.100	QUIC	83	Protected Payload (KP0), DCID=400000d057b3a35a
27	0.258252	193.167.0.100	193.167.100.100	QUIC	92	Protected Payload (KP0), DCID=400000d057b3a35a
28	0.288772	193.167.100.100	193.167.0.100	QUIC	80	Handshake, SCID=400000d057b3a35a
29	0.288984	193.167.100.100	193.167.0.100	QUIC	314	Protected Payload (KP0)
30	0.309808	193.167.100.100	193.167.0.100	QUIC	90	Protected Payload (KP0)
31	0.309902	193.167.0.100	193.167.100.100	QUIC	1374	Protected Payload (KP0), DCID=400000d057b3a35a
32	0.315124	193.167.0.100	193.167.100.100	QUIC	79	Protected Payload (KP0), DCID=400000d057b3a35a
33	0.361895	193.167.100.100	193.167.0.100	QUIC	90	Protected Payload (KP0)
34	0.362015	193.167.0.100	193.167.100.100	QUIC	1454	Protected Payload (KP0), DCID=400000d057b3a35a
35	0.413864	193.167.100.100	193.167.0.100	QUIC	90	Protected Payload (KP0)
36	0.413974	193.167.0.100	193.167.100.100	QUIC	1514	Protected Payload (KP0), DCID=400000d057b3a35a
37	0.465813	193.167.100.100	193.167.0.100	QUIC	90	Protected Payload (KP0)
38	0.520023	fe80::b4c7:45ff:feb... ff02::16		ICMPv6	130	Multicast Listener Report Message v2
39	0.531943	fe80::b4c7:45ff:feb... ff02::16		ICMPv6	90	Multicast Listener Report Message v2
40	0.584043	fe80::42:c1ff:fea7... ff02::16		ICMPv6	110	Multicast Listener Report Message v2
41	0.584080	fe80::42:c1ff:fea7... ff02::2		ICMPv6	70	Router Solicitation from 02:42:c1:a7:00:64

>- Ethernet II, Src: 02:42:c1:a7:00:02 (02:42:c1:a7:00:02), Dst: 02:42:c1:a7:00:64 (02:42:c1:a7:00:64)
 >- Internet Protocol Version 4, Src: 193.167.100.100, Dst: 193.167.0.100
 >- User Datagram Protocol, Src Port: 443, Dst Port: 56999
 >- QUIC IETF
 > QUIC Connection information
 [Packet Length: 1232]
 1.... = Header Form: Long Header (1)
 .1.... = Fixed Bit: True
 ..00 = Packet Type: Initial (0)
 [.... 00.. = Reserved: 0]
 [.... .11 = Packet Number Length: 4 bytes (3)]
 Version: 1 (0x00000001)
 Destination Connection ID Length: 0
 Source Connection ID Length: 8
 Source Connection ID: 400000d057b3a35a
 Token Length: 0
 Length: 1214
 [Packet Number: 10456286]

0000 02 42 c1 a7 00 64 02 42 c1 a7 00 02 08 00 45 00 ·B
 0010 04 ec 61 5a 40 00 3e 11 ee 8f c1 a7 64 64 c1 a7 ···
 0020 00 64 01 bb de a7 04 d8 79 7b c8 00 00 00 01 00 ·d
 0030 08 40 00 00 d0 57 b3 a3 5a 00 44 be 8a ed 6e d4 ·@
 0040 67 c2 18 4f ee 19 10 57 b1 25 53 63 2a 8e 46 27 g
 0050 93 d9 eb 0c 50 1d d7 f0 26 e2 96 04 f7 9a 2e 78 ··
 0060 34 42 42 6a df 79 bf be 2b 98 8a c3 80 fc 1e 6e 4B
 0070 76 5c 88 5e 62 69 21 90 25 3c 40 56 65 84 1d db v\
 0080 55 02 0d a4 39 e8 4d 80 6c 37 97 1e 73 96 07 93 U
 0090 f9 90 13 f8 75 40 ea 87 c6 71 0b 55 9d e5 d1 88 ··
 00a0 6d d3 6a 14 f7 1a d9 fd 67 d3 f2 8b 93 b3 d6 94 m
 00b0 20 3c 65 03 01 0d ab 24 39 e7 50 1f 1c b6 <
 00c0 af d7 da 70 76 fd 49 23 6a c0 a6 5e ea 98 5b 85 ··
 00d0 13 be 61 e4 3f d8 51 32 d2 1c b5 7d f0 8c b1 fa ··
 00e0 c2 01 89 09 3d a8 57 06 40 ec 7c c5 e2 05 31 19 ··
 00f0 82 2a 7d 5d 07 73 86 73 e8 ee 1b 6c 93 fd 70 ba ··
 0100 7e 36 c7 97 f7 ca c7 a5 d7 73 ab cc 9f 3a a4 14 ~6
 0110 48 4f b4 79 04 6c fe 09 3b 16 80 45 ef e0 c1 a6 H0
 0120 8c ae 16 f7 27 4b 50 96 8b 47 e4 d7 7d 70 e7 d6 ··
 0130 a4 aa 68 da b7 19 f0 86 0c ee 1d 6f da 58 b6 68 ··
 0140 f1 b0 b3 29 e2 f7 f7 88 ee fe bd 1c 68 ec 6b ··
 0150 ae 61 df dd bc d4 77 65 51 51 ca c7 b3 41 3f 87 a
 0160 7a 1c 00 05 00 71 5c 10 00 71 1c 50 16 00 75 ··

Frame (1274 bytes) Decrypted QUIC (1194 bytes)

unsuccessful handshake.pcap

Packets: 56 · Displayed: 56 (100.0%)

Profile: Default

TEST ENVIRONMENT SETUP

SETUP 1

Arch Linux x86_64 with 45 GB root and 50 GB of /home. Use of python environments wherever necessary.

SETUP 2

Docker container with Ubuntu-18, runs inside setup 1. Takes up 16 GB.

RESULTS SETUP 1

```
> python test.py iters=2 server=picoquic test=quic_server_test_stream
output directory: temp/1
implementation directory: /home/huntrag/Code/mtp/new_impl/picoquic
implementation command: ./picoquicdemo -L -l -
./quic_server_test_stream (0) ...
implementation command: ['./picoquicdemo', '-L', '-l', '-']
server pid: 9325
timeout 100 ./build/quic_server_test_stream seed=0 the_cid=0 server_cid=1 client_port=4987 client_port_alt=4988
timeout: the monitored command dumped core
client return code: -4
FAIL
...
./quic_server_test_stream (1) ...
implementation command: ['./picoquicdemo', '-L', '-l', '-']
server pid: 9334
timeout 100 ./build/quic_server_test_stream seed=1 the_cid=2 server_cid=3 client_port=4989 client_port_alt=4990
timeout: the monitored command dumped core
client return code: -4
FAIL
error: 2 tests(s) failed
> python test.py iters=2 server=winquic test=quic_server_test_max
output directory: temp/3
implementation directory: ..
implementation command: true
./quic_server_test_max (0) ...
implementation command: ['true']
server pid: 10408
timeout 100 ./build/quic_server_test_max seed=0 the_cid=0 server_cid=1 client_port=4987 client_port_alt=4988
timeout: the monitored command dumped core
client return code: -4
FAIL
...
./quic_server_test_max (1) ...
implementation command: ['true']
server pid: 10415
timeout 100 ./build/quic_server_test_max seed=1 the_cid=2 server_cid=3 client_port=4989 client_port_alt=4990
timeout: the monitored command dumped core
client return code: -4
FAIL
error: 2 tests(s) failed
```

OUTPUT SETUP 1

The figure shows two windows of the ivy_ev_viewer tool, both titled "Sheet 0".

Left Window:

- Event: `tls_api.upper.create(0,0,[{quic_transport_parameters:{transport_parameters:[{initial_max_stream_data_bidi_local:{stream_pos_32:0x2000}}],{}}])`
- Event: `http_request_file.read`
- Event: `ivy_return_code(-4)`

Right Window:

- Event: `tls_api.upper.create(0,0,[{quic_transport_parameters:{transport_parameters:[{initial_max_stream_data_bidi_local:{stream_pos_32:0x2000}}],{}}])`

PICOQUIC SERVER TESTS ON SETUP 2

```
Running as user "root" and group "root". This could be dangerous.
Capturing on 'lo'
tshark: cap_set_proc() fail return: Operation not permitted
tshark: cap_set_proc() fail return: Operation not permitted
between random: 82942441
between random: 82942437
between random: 82942441
between random: 28081
"           require f.data = crypto_data(scid,e).segment(f.offset,f.offset+f.length); # [2]
"
/usr/local/lib/python2.7/dist-packages/ivy/include/1.7/quic_frame.ivy: line 803: error: assumption failed
output directory: temp/13
implementation directory: /quic/picoquic
implementation command: ./picoquicdemo -l -D -L -q /results/picoquic_qlog
./quic_server_test_crypto_limit_error (0) ...
implementation command: ['./picoquicdemo', '-l', '-D', '-L', '-q', '/results/picoquic_qlog']
quic_process pid: 18614
timeout 100 ./build/quic_server_test_crypto_limit_error seed=495 the_cid=0 server_cid=1 client_port=4987 client_port_alt=4988
client return code: 1
FAIL
error: 1 tests(s) failed
test_server.sh: line 94: [: 15: unary operator expected
\Iteration => 15
\Implementation => picoquic
\Test => quic_server_test_crypto_limit_error
```

GNOME Text Editor - Wikipedia

The program was officially announced by Hergert. The text editor is

Wikipedia

Ubuntu Text Editors - Verpex

Ubuntu 20.04 LTS — The default text editor in the system is Gedit. Gedit is a simple

Verpex

Ubuntu 22.10 Replaces Gedit

GTK4 app shipping as part of GNOME

OMG! Ubuntu

Show

CONCLUSION

SETUP ERRORS

Compatibility issue in setup 1 and, space and convenience issue in setup 2. Use virtual machines instead.

RFC 9000 & DRAFT-29

Differences between draft-18, draft-29 and RFC-9000 need to be listed down

ALTERNATIVES TO IVY

No commits regarding development for long time though both papers conclude Ivy is operational for testing. If not Dafny or TLA+ can be explored.

EXPECTED RESULTS

Test Case	Picoquic	Quant
quic_server_test_stream	614/1000	362/1000
quic_server_test_max	682/1000	306/1000
quic_server_test_connection_close	92/1000	78/1000
quic_client_test_max	133/1000	0/1000

These are results of 1000 iterations per test. These are the number of tests that passed.

Test Case	Error Code	#
quic_server_test_stream	require ~_generating & ~queued_non_ack(scid) → ack_credit(scid) & 0; [5]	242
	Ran out of values for type cid	121
	require ~path_challenge_pending(dcld,f.data);	24
	bind failed: Address already in use	2
	require conn_seen(dcld) → 1 hi_non_probing_endpoint(dcld,dst); [10]	1
Total		390/1000
quic_server_test_max	require stream_id_allowed(dcld,f.id); [4]	219
	Ran out of values for type cid	102
	require ~path_challenge_pending(dcld,f.data);	8
	require ~_generating & ~queued_non_ack(scid) → ack_credit(scid) & 0; [5]	12
	require conn_total_data(the_cid) & 0;	31
	require conn_seen(dcld) → 7 hi_non_probing_endpoint(dcld,dst); [10]	7
	bind failed: Address already in use	1
Total		380/1000

Error code distribution of the tests conducted in setup 1