Department of Informatics
Technical University of Munich

TECHNICAL UNIVERSITY OF MUNICH

DEPARTMENT OF INFORMATICS

BACHELOR'S THESIS IN INFORMATICS

The First Year of QUIC v1 Deployment

Dániel Hegedüs

Technical University of Munich

Department of Informatics

Bachelor's Thesis in Informatics

The First Year of QUIC v1 Deployment

Einsatz von QUIC v1 im Ersten Jahr

Author:	Dániel Hegedüs
Supervisor:	Prof. Dr.-Ing. Georg Carle
Advisor:	Johannes Zirngibl Patrick Sattler Benedikt Jaeger Juliane Aulbach
Date:	April 15, 2022

I confirm that this Bachelor's Thesis is my own work and I have documented all sources and material used.

Garching, April 15, 2022

Location, Date

Signature

Abstract

QUIC is a new transport protocol, originally developed by Google and proposed to the Internet Engineering Task Force (IETF) in 2015 for standardization. Since then, the first final version of QUIC was released in May 2021 after 34 draft versions.

Almost a full year has passed since the release, and the protocols' adaptation has evolved through increasing usage and support by larger companies and vendors of HTTP servers and browsers (Quicwg [1], and Deveria [2]). Because of general availability and ease of deployment, QUIC can now be used by anyone for various applications and use cases.

This thesis analyses discovered QUIC deployments for IPv4 and IPv6, and how they have evolved since the release of v1 to estimate the current state of QUIC. Measurements show that the number of addresses serving QUIC has not necessarily increased since May 2021 (IPv4: -18,96%, IPv6: +6,25%), however, the relative connection success rate has improved (IPv4: 6.9% to 15,9%, IPv6: 27,20% to 27,20%). Furthermore, the amount of unique hosts contactable via these addresses has increased significantly (IPv4: +270,51%, IPv6: +181,40%).

The number of distinct Autonomous Systems (ASes) has also increased for both address spaces, but the majority of the deployments remain as part of only a few large ASes, with the most prevalent examples being Cloudflare Net (AS13335), Google (AS15169), Akamai-ASN1 (AS20940), and Fastly (AS54113). One further observation is, that since release, the version distribution is shifting towards the usage of QUIC v1 more and more (IPv4: 8,81% to 19,58%, IPv6: 14,6% to 21,72%).

The thesis also contains an analysis of the distribution of responses from the QUIC deployments after attempted connection establishment. In the case of an error, the most common reason for the failure was observed to be a kind of crypto error. Lastly, an analysis of the used servers is performed for deployments that could be contacted via Hypertext Transport Protocol (HTTP).

Contents

List of Figures

List of Tables

Chapter 1

Introduction

QUIC (first as the acronym ”Quick UDP Internet Connection” but now just ”QUIC”) is a new general-purpose transport protocol based on the User Datagram Protocol (UDP), which could have a large impact on the Internet by acting as a replacement for many Transmission Control Protocol (TCP) + Transport Layer Security (TLS) deployments.

The protocol offers some advantages over TCP. One of the advantages is, that QUIC has built-in streams. In the case of TCP, Head-of-Line Blocking (HOL) could occur if a packet is lost in transition and the request contains multiple data parts. TCP is designed to hold back all succeeding packets of a single connection in that case, even if the application could use and process the data of succeeding packets. The application has to wait until the lost packet is retransmitted. QUIC is designed to counter HOL by utilizing streams inside one connection. Only data of that lost stream is held back, other packets are passed to the application immediately for further processing.

Furthermore, each connection is based on a separate Connection ID and not the IP address from the UDP connection. This way the possibility for multipath connections is preserved, and the connection can remain open and functional, even if the IP address changes. One of the use cases of multipath connections could be, that the client changes networks, e.g. from Wi-Fi to mobile data when moving out of the house. The connection will then seamlessly transition without the need to re-establish a new QUIC connection.

These improvements make QUIC optimal for use cases like the Hypertext Transport Protocol (HTTP) and thus making it the proposed basis for HTTP version 3 (Request for Comments (RFC) draft HTTP/3 [3]).

The protocol has been in development by Google since 2012 and was proposed as a standard to the Internet Engineering Task Force (IETF) in 2015. Since then the protocol has received 32 RFC drafts until the proposal was put into last call in October 2020. After two more revisions, version one was released in May 2021, making the finished protocol almost exactly one year old.

1.1 Motivation

Already previous to the release of v1 many larger companies started using QUIC as early adopters. Google and Facebook provided insights on the benefits that they gained by switching large shares of their traffic to be served via QUIC. Google released a paper about their usage of QUIC (Langley *et al.* [4]) in 2017 where they described, that they have already switched ”over 30%” of their traffic to QUIC. Facebook on the other hand reported, that they switched ”more than 75% of traffic” to QUIC in 2020 (Joras *et al.* [5]). Part of the thesis is looking at the changes in the spread of ASes to see if only the larger companies remained part of the QUIC deployments or if many new users have appeared since release.

Because QUIC is implemented in the user layer and is not restricted to updates via the kernel, it is easily adoptable for different needs. Furthermore, it is possible to update it with new features at any time. Because of this advantage, many companies develop their own QUIC implementations to further optimize the protocol for their specific traffic, use case and needed features. As an example, mvfst (Facebookincubator [6]), the implementation maintained and used by Facebook, is developed primarily with large scale deployments in mind, whereas MsQuic (Microsoft [7]), a QUIC implementation by Microsoft, focuses on maximal throughput and minimal latency. The currently most used versions and implementations of QUIC will be evaluated, and if the deployments have updated or even completely changed their offered QUIC versions over time. If the former is not the case or the latter is true, then possible reasons will be explored.

Since the release of the first version of QUIC, many browsers, e.g. Chrome, Edge, Opera, Firefox, etc. (Deveria [2]), and HTTP servers like Nginx, Node.js, LiteSpeed, etc. have released stable versions of their software with a QUIC implementations included (Quicwg [1]). This makes it more feasible for smaller companies and individuals to use QUIC for their own purposes. By looking at the different HTTP servers and the ASes that they were served by, it can be evaluated if larger ASes start to move from their own servers to more established ones or vice versa smaller ASes tend to use the custom software of the larger firms.

Overall, the changes in the amount of QUIC deployments since version one will be analyzed to get a picture of the adoption rate of the Internet to the new protocol. These scans are then put into relation to each other to see the evolution. Additionally, the amount of successful or failed connections is evaluated to see if the deployments are actually serving content via QUIC for the public.

1.2 Outline

The thesis starts with the background in Chapter 2, where the handshake of the protocol itself is explained on a more technical level. Furthermore, the tools used for collecting data from the deployments are introduced and the type of scan methods are explained.

Chapter 3 offers an overview of related work that has already evaluated data about QUIC deployments before the release of v1. Related work about the protocol itself is also mentioned to offer a broader overview of QUIC, and its possible advantages and use cases. Furthermore, research about HTTP/3 is mentioned as well.

Continuing with the approach (Chapter 4) the number of scans and their different types are highlighted. Additionally, the process of how the raw initial datasets are extended and put into relation with each other to evaluate the data is explained.

The main part of the thesis consists of Chapter 5, where the actual relational data is shown, analyzed and the results evaluated and as far as possible explained. Section 5.1 contains the changes of QUIC deployments regarding the amount distinct addresses. Additionally, in Section 5.2 the changes of the deployments regarding the unique ASes are evaluated. Continuing with Section 5.3 the ASes are analyzed on how their spread has changed over time and how large the share of each AS is. Furthermore, the QUIC versions used by the deployments are evaluated in Section 5.5 regarding their distribution in groups and each on their own. It is also explored if a major shift towards the IETF v1 has taken place since its release.

Previously, the number of discoverable deployments was analyzed via unique addresses, however, in the case of SNI scans the number of distinct hostnames and their ASes are also evaluated in Section 5.4. Furthermore, regarding stateless scans, many deployments do not answer with a successful response despite connection establishment with an announced supported version. The amount of successful responses, or the type of error messages if the connection fails, is analyzed in Section 5.6. Lastly, deployments that do respond to requests via HTTP can be analyzed on their response headers. In Section 5.7 the different kinds of used HTTP servers are evaluated.

In the final chapter (Chapter 6), the evaluated data is summarized, and the key takeaways highlighted in Section 6.1. As the very last part of the thesis future work is mentioned in Section 6.2.

Appendix A contains information regarding acronyms and the full names for each mentioned AS number. Furthermore, some tables and figures containing additional data were added here for completeness purposes.

Chapter 2

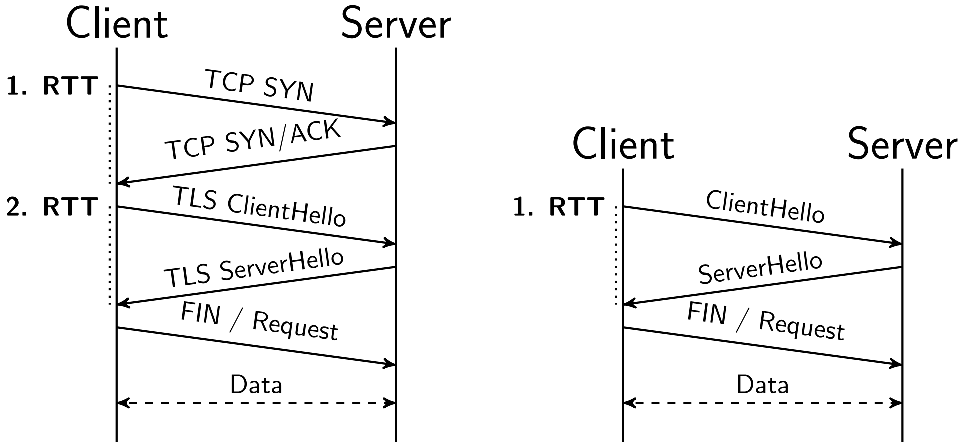
Background

QUIC is designed to cut down on overhead and reduce latency. By using two different header types, (long headers before connection establishment and short headers after) the packet size is minimized for each state of the connection.

One further optimization of QUIC is the combination of the cryptographic and transport handshake into one. Because of this design choice, the connection time can be greatly reduced in comparison to TCP + TLS. After the initial TCP handshake, another TLS handshake needs to be performed for a successful, encrypted connection. Older TLS versions might even need more Round-Trip-Time (RTT)s for successful connection establishment.

QUIC merged the TLS v1.3 key exchange into the initial handshake by performing the cryptographic handshake inside the same `Initial` packet used for connection establishment to be able to omit the extra handshake completely. If beforehand a connection was already successfully established, there is even the possibility for 0-RTT connection establishment by reusing the previously negotiated parameters. In that case, the first packet sent by the client can already contain requests, which can be answered by the server instantaneously without the need for any RTTs.

The QUIC connection starts with the handshake (Figure 2.1). First, the two endpoints, the server, and the client try to negotiate a common version via which the two endpoints can communicate. The `initial` packet which is sent to the receiving endpoint contains a 32bit `version` field with its preferred QUIC version for communication. In the case, that the selected version is supported by the server, a response is sent which confirms if the communication via that version can commence and a shared secret using the inbuilt TLS protocol is established. In the case that the requested version is not supported by



(a) TCP + TLS v1.3

(b) QUIC v1

Figure 2.1: Difference in the handshake and the amount of RTTs needed for TCP + TLS v1.3 and QUIC connection establishment

the server, a `version negotiation` packet is sent as a response. This packet contains a list of all supported versions by the server. The client can then pick a version from the supported versions of the server and retry to establish the connection with the new version.

Some `version` field values are reserved for special functionality. For example `0x00000000` is reserved to represent `version negotiation` packets. The current QUIC v1 version is identified by `0x00000001`. Section 5.5 is about the most common version patterns and their spread. Versions that follow the pattern `0x?a?a?a?a` are reserved to force version negotiation packets from the server (RFC [8] Section 15: Versions).

Because the transport and cryptographic handshake are merged, new problems can occur when one of the two fails. For that reason, specific crypto error codes are returned as QUIC transport errors which contain the TLS error. 256 values (from `0x100` to `0x1ff`) are reserved for carrying these TLS specific codes. The TLS error code is added to the initial value (`0x100`) to receive the new value, which represents the `CRYPTO ERROR`. The most common errors can be seen in Table 2.1.

The scans are split into two different kinds, stateless and stateful. Stateless scans are simpler because they only consist of one request, and the response is not needed for later use. The initial response is the desired data. Stateful scans on the other hand are more complex because they need to evaluate the response and handle according to the received data. In our case, the connection has to be established if the response is a valid response to the `initial` packet.

Table 2.1: Most common CRYPTO ERROR codes and their corresponding TLS code and textual representation

QUIC Error Code	TLS Error Code	Text
0x128	40	generic code / handshake_failure
0x131	49	access_denied
0x146	70	protocol_version
0x150	80	internal_error
0x16d	109	missing_extension
0x178	120	no_application_protocol

ZMap is the stateless network scanner used for checking if an IP address does serve content via QUIC. The QUIC module for ZMap was developed by Rüth *et al.* [9] and extended by Zirngibl *et al.* [10].

The module checks if a client is a QUIC deployment by sending an initial packet to the client with the version field set to a version with the pattern 0x?a?a?a?a. These reserved versions should trigger a version negotiation packet by the server as described above. If the response is a valid QUIC version negotiation packet, then the endpoint is considered a QUIC deployment. The received packet contains useful information on all supported versions.

From 1st January 2022 on, till the 14th January 2022, the packet sent to trigger the response from the QUIC deployments has been changed with the version field set to the IETF version (0x00000001). This has been done to test for better coverage because some QUIC implementations could be programmed to discard packets with invalid version field values on initial connection, as the 0x?a?a?a?a pattern is declared as reserved. Because the responses after this change do not guarantee a version negotiation packet as the response, evaluation of QUIC versions is not possible for this timeframe. The effect of this change will be analyzed in Chapter 5.

QScanner is the stateful pendant to the ZMap module, based on quic-go (Lucas-Clemente [11]) and adopted for the discovery of QUIC deployments by Zirngibl *et al.* [10].

If IPs from the stateless scan or through HTTPS Domain Name System (DNS) Record Ranges (RR) and HTTP Alternative Services (ALT-SVC) headers are discovered to be QUIC deployments, connection establishment is initiated with QScanner. QScanner exposes information about the handshake, which is then useful for analysis. The main point of interest for this thesis is the success rate of handshakes and the error message that occurred if the handshake fails. Furthermore, the HTTP headers of deployments that were responding to HTTP requests are also extracted by QScanner.

Because IP addresses are scarce, multiple hostnames can be served via the same IP address. Therefore, (multiple) QUIC deployments could be unnoticed by the stateless scanner if the default request to an address leads to a non-QUIC serving deployment. In that case, SNI, a TLS extension, is used to request different hosts from the same IP address by requesting a specific certificate via an additional hostname in the TLS `ClientHello` frame (QUIC manageability draft-16 [12]).

Chapter 3

Related Work

QUIC has been part of a lot of research in the last few years with the pace picking up since the release of version one.

Many papers have proven, that QUIC offers substantial benefits over TCP + TLS in the right use case. One of the major benefits of QUIC, discovered by Shreedhar *et al.* [13] is, that the performance or video streaming far exceeds TCP + TLS, because QUICs connection establishment is 90% faster, reducing buffer times and improving content delivery. This was also confirmed by Joras *et al.* [5] and their real-world analysis on Facebook's services in 2020, where a 22% improvement between video rebufferings was observed. The error count for video requests was reduced by 8% and the video stall rate by 20%. Furthermore, Cook *et al.* [14] discovered, that QUIC provides better performance on unstable, lossy networks. When comparing the draft versions of HTTP/3 vs HTTP/2, Saif *et al.* [15] also concluded, that HTTP/3 offers a far better Quality of experience (QoE) on lossy networks, and a higher average throughput (1.24MBps vs 1.03MBps), but otherwise performs slightly worse than HTTP/2. Wolsing *et al.* [16] experienced similar results when testing QUIC with HTTP/2. However, they also discovered, that choosing the right congestion control protocol is almost more important to improve performance than the transport protocol itself, however, QUIC is far more flexible and better for continuous evolution than TCP + TLS, and thus makes QUIC the ”preferred protocol for the future Web”.

Because of this, the research for QUIC is not only limited to the current state but also future extensions that improve upon further long-standing problems of TCP + TLS. The paper of Kosek *et al.* [17] explores some of these possibilities, like `MASQUE` and `WebTransport`.

As the main topic of the thesis remains the development of QUIC deployments over the internet, many papers with a focus on the protocol itself or the implementation are not directly relevant. Two main papers have researched the state of QUIC deployments:

Rüth *et al.* [9] evaluated IPv4 addresses and 46% of the DNS space for QUIC capable hosts. They discovered, that over the months from August 2016 to October 2017 that they monitored the web, the number of QUIC deployments tripled to around 617.59k unique deployments. The increase was mainly driven by Google and Akamai with 53.53% and respectively 40.71% share. Rüth *et al.* estimates, that QUIC is responsible for 2.6% to 9.1% of the traffic on the internet.

The second publication is by Zirngibl *et al.* [10]. With consideration for IPv4 and IPv6 addresses and further discovery over HTTPS DNS RR and HTTP ALT-SVC headers over 26 million QUIC targets could be contacted from more than 4.7k ASes. Zirngibl *et al.* also discovered, that mainly large corporations were serving content via QUIC, however, Cloudflare was the largest contrary to the discovery of Rüth *et al.* [9] with Google, Akamai, and Mozilla are still highly present.

Furthermore, there is one paper focusing on HTTP/3 deployments by Trevisan *et al.* [18]. They checked the adoption rate of HTTP/3 by leading companies such as Google, Facebook and Cloudflare. The conclusion was, that Cloudflare is by far the number one (12455 of 14725 deployments, or 84,58%), with Google in the second place for HTTP/3 usage (1094 deployments).

Contrary to the related works about QUIC deployments, this thesis focuses on the time since the release of QUIC v1 to paint a picture of the evolution after a stable version to see if the previously mentioned discoveries have remained or changed.

Chapter 4

Approach

First, the data from ZMap and QScanner is processed by converting it into a database format. For a better overview and easier grouping, the AS number of each scanned IP is sourced using pyasn[1] in combination with routeviews[2] historic data for each of the scans. Furthermore, the name of the owner of the AS is collected and assigned to the AS numbers via a list from the CIDR report[3].

The created data frames are then used for the evaluation of each point in time (a snapshot). By comparing the analysis of each snapshot, the evolution of QUIC since the release can be evaluated. In order to get a grasp of the absolute change since the release of version one, the difference between the first and very last scan is analyzed for each evaluation aspect. Even if large changes took place between the first and last snapshot, only the final scan represents the current state of QUIC deployments, after one year of the QUIC v1 release. However, if suddenly large changes appear and e.g. the IP count fluctuates a lot, emphasis is given to that scan and the possible reason is explored. Most of the time, one AS is responsible, which is pointed out in the analysis.

The ZMap scans are used to collect the amount of distinct IPs. These are dissected into four different groups based on their status from the previous scan, which can be seen in Table 4.2. Estimations about the share of QUIC over the address spaces can be

[1] `https://github.com/hadiasghari/pyasn`

[2] `http://archive.routeviews.org/`

[3] `https://www.cidr-report.org/as2.0/autnums.html`

Table 4.1: List of scans and their different configurations. The scans are scheduled approximately weekly. Some scans are missing because of hardware failure or some had to be discarded after changes in configuration corrupted the results.

Scan Type	Version	Form	To	SNI	Scan Count
stateless	IPv4	2021-05-31	2022-03-01	no	39
	IPv6	2021-06-03	2022-03-04	no	32
stateful	IPv4	2021-06-02	2022-03-03	no	39
				yes	37
	IPv6	2021-06-03	2022-03-04	no	30
				yes	34

done by looking at the number of IPs that respond. Specifically, the number of unique addresses that have acted as a QUIC deployment until now can be seen.

By applying the same schema as described in Table 4.2 and grouping the IPs to their AS, the change in the distinct count of ASes can be evaluated. Furthermore, the spread is estimated by checking how often each AS appears in relation to the others. This way, the large users of QUIC are visible, and it can be seen if smaller companies are starting to use QUIC and occupying significant shares of the network over time, or if the deployment space is still dominated by a selected few ASes.

When looking at the stateful SNI scans, there is also the possibility to look at the count of deployments by filtering for distinct hostnames and not only the address. In that case, the ASes share is analyzed, and it will be evaluated if the share in the network remains similar compared to the distinct addresses. Analysis on the errors and HTTP headers is not performed additionally, because almost all targets respond the same way for the same address.

One further aspect of evaluation will be the implementations and versions used by the different deployments. Each deployment of the stateless scans responded with a version negotiation packet until the request packet's version field was set to `0x?a?a?a?a`. The response contains a list of all QUIC versions supported by the server. Many deployments are expected to respond with the same group of versions. Especially deployments part of larger ASes. The spread of these groups and their ASes will be put into relation. Additionally, the groups of versions are split into every single version and the overall share in comparison to all other versions is evaluated to get an overview of the most used versions across all deployments. Over time the change in the share of QUIC v1 is evaluated to estimate if the share of the final IETF version is increasing over time.

Table 4.2: Description of IP types after analysis

name	**IPs ...**
defunct	...were serving QUIC on the previous scan but stopped
persistent	...remain serving QUIC since the previous scan
reoccuring new	...have served via QUIC, went defunct and reappear again
unique new	...were never observed before this scan

The stateful QScanner scans also contain an error message, that is either empty if the connection establishment of the scan was successful or a string from quic-go (Lucas-Clemente [11]) with a reason for the failed connection establishment. By evaluating these scans, the amount of responsive QUIC deployments is estimated in comparison to all stateful QUIC deployments. Furthermore, the biggest reasons for unsuccessful connections will be evaluated. Particularly how the QUIC deployments react to the different set version fields in the `initial` packet is part of the evaluation.

Connections that were able to contact the QUIC deployment via HTTP and got a valid response back, can be analyzed by each header. One of these is the "Server" type header, which informs the client via which HTTP server the QUIC connection served its content. Because many HTTP servers only added QUIC support after the release of version one, the distribution of these servers is evaluated to see if changes are visible after stable releases of the server software were released.

Chapter 5

Evaluation

This chapter contains several sections, each focusing on one specific aspect of the current state of QUIC. Most of the time, each scan type contains different results for the different aspects. Therefore, many sections contain paragraphs separately for stateless and stateful scans, respective SNI as well as no SNI scans.

5.1 Changes in the Number of IPs Serving via QUIC

Table 5.1: Absolute change of distinct addresses since the release of QUIC v1 till the corresponding last scan from Table 4.1. No SNI scans are based on the ZMap addresses, so the ZMap IP count equals the no SNI IP count.

Version	SNI	First	Last	% change
IPv4	no	2.149.285	1.741.793	- 18.96
	yes	260.904	473.680	+ 81,55
IPv6	no	210.156	223.297	+ 6,25
	yes	132.024	656.038	+ 396,91

Regarding IPv4 no SNI, the overall number of QUIC deployments has declined to this date. This can be seen in Figure 5.1 and Table 5.1. Shortly after the release, around 2,149 million unique addresses were discovered. This number steadily increased until the 16th August 2021, when a sudden drop occurred with around 350k total addresses going defunct over the next three scans until the 1st September 2021. For the first two scans mainly IPs from Fastly (AS54113) go defunct, however on the third date Fastly (AS54113) regains almost the full amount of defunct IPs with a difference of just 3520 IPs less. On the same date, Google (AS15169) responds with around 355k

addresses less. From this point on, the previous trend continues and a slow, but steady increase in IPs can be seen.
After switching to the new `version` field on the 4th January 2022, a lot of unique new IPs are answering to the request. On the other hand, many other deployments stopped answering to the scan, leading to many defunct addresses as well. However, the total number of IPs stayed approximately the same as on the scans before.
The last scan on the 1st March 2022 consists of around 1,74 million unique addresses, which is an absolute decrease of approximately 23,39% compared to the 2,15 million addresses shortly after release. This is rather contrary to the expectation of increasing adoption of QUIC since the release of v1 of the protocol, especially for the IPv4 address space.

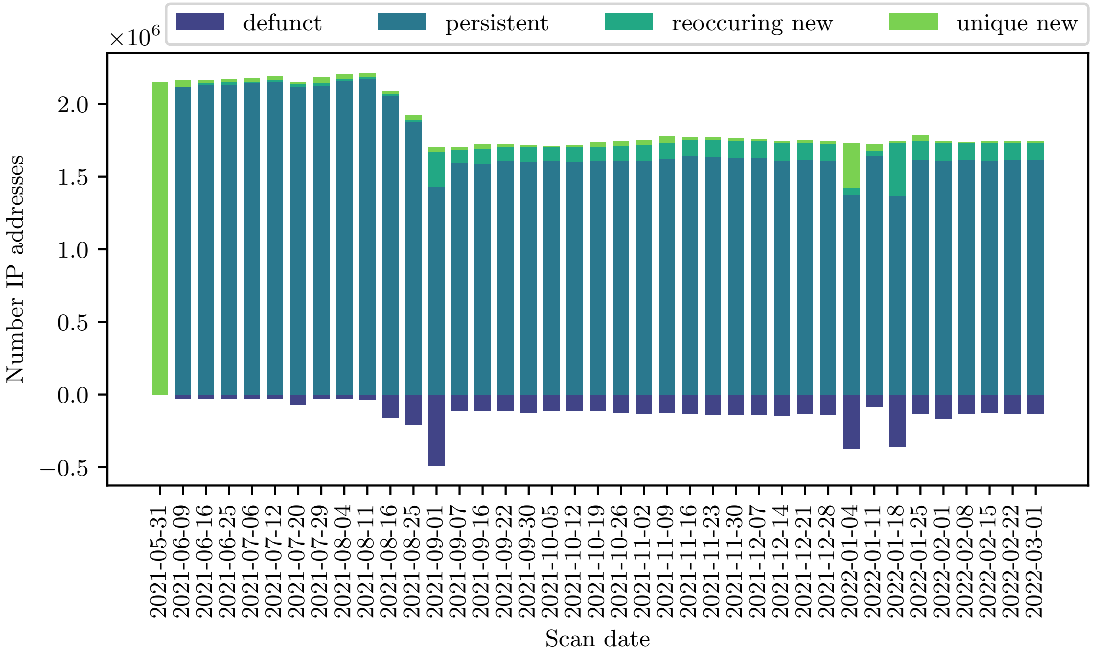


Figure 5.1: IPv4 no SNI addresses serving QUIC deployments (legend as described in Chapter 4)

As can be seen in Table 5.1, the number of QUIC deployments for IPv4 SNI has massively increased. The first few scans until the 15th July 2021 consistently remained between 260 and 282k deployments with a sudden jump to 473k. After the 3rd September 2021 a new loss occurs by about 67k deployments. From there on the number of deployments steadily increased to 388k with one spike on the 2nd December 2021 to 412k, but instant drop on the next scan to 362k where the number of deployments remained until the 27th January 2022. After that scan, the number suddenly rises to 428k with a steady growth until the last scan to the final count of 474k unique addresses.

The absolute number of unique IPv6 no SNI addresses has increased from 210 to 223k signifying an increase of 6,25%. Contrary to the IPv4 counterpart, the IPv6 deployments are fluctuating a lot from the 5th November 2021 onwards, with ranges from 210k addresses to a max of 524k addresses. This can be seen in Figure 5.2. These rapidly changing IPs are all part of Amazons' AS. According to self-published IP ranges[1], almost all IPs are part of its `AMAZON` service, `GLOBAL` region, and `GLOBAL` network border group. These fluctuations disappear after the 24th December 2021 and roughly 233k distinct addresses remain.

The two scans with the `version` field set to IETF QUIC v1 received a lot of new responses with around 130k unique new addresses (330k total) on the 7th January 2022, and a further 135k unique new (354k total) on the 14th January 2022. Interestingly the number of defunct addresses for the second date was also very high with around (158k addresses), leading to only a small jump in the count. Google (AS15169) suffered the largest loss in deployments with around 24k fewer addresses for that scan and Amazon-02 (AS16509) and As-Hostinger (AS47583) the largest gain with 61 and 48k new addresses.

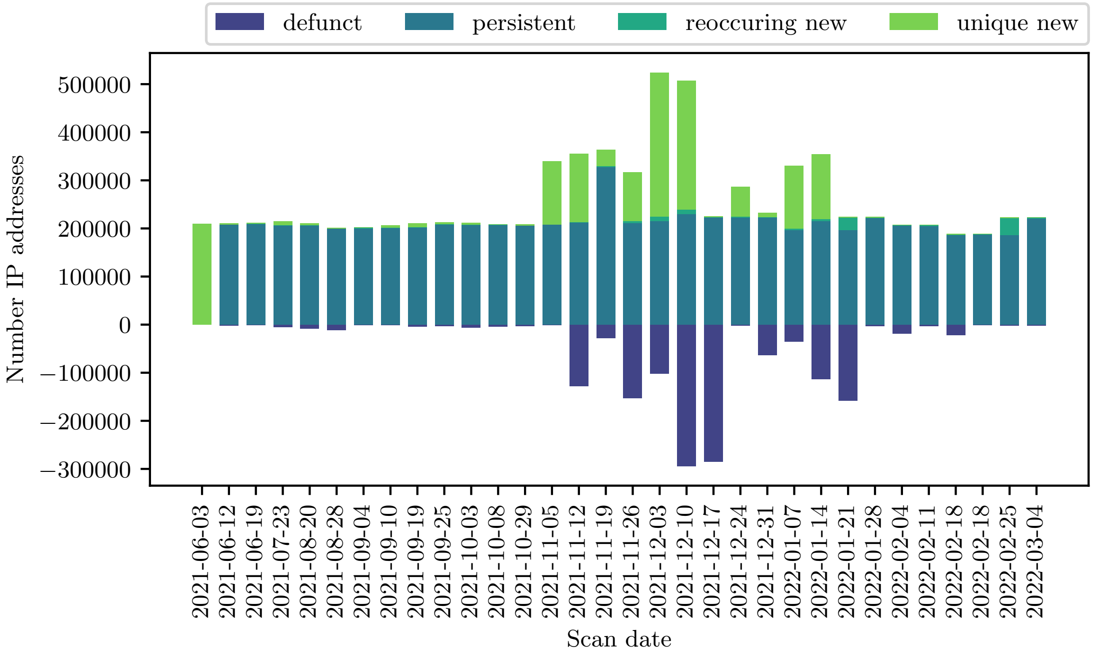


Figure 5.2: IPv6 addresses serving QUIC discovered by stateless scan (Legend as described in Chapter 4)

[1] `https://ip-ranges.amazonaws.com/ip-ranges.json`

The absolute change in discovered IPv6 SNI deployments is even more extreme than the IPv4 pendant (Table 5.1). The amount almost quadrupled since the first scan from 132k to 656k. For the four first scans, the number only decreased slowly with a larger drop on the 9th July 2021. After that, the number of deployments increases at once to 269k addresses, almost only with IPs from Cloudflare Net (AS13335) and stays around that mark until the 12th November 2021, where another jump of about 66k additional deployments occurs. On the succeeding three scans the amount further increases drastically but drops by 123k on the 26th November 2021. From there on the number of deployments only increases until the 14th January 2022, when another 6k increase in unique IPs occurs. However, the newly gained errors are all dropped on the next scan. No larger new changes occur from thereon, and the last scan reaches the final count that can be seen in Table 5.1.

5.2 Changes in the Number of ASes Serving via QUIC

Table 5.2: Absolute change of distinct ASes since release of QUIC v1 for corresponding data from Table 4.1

Version	SNI	First Scan	Last Scan	% change
IPv4	no	4792	5370	+ 12,06
	yes	1140	2221	+ 94,82
IPv6	no	1713	1928	+ 12,55
	yes	515	703	+ 36,50

Despite the fluctuation in distinct IPs, the amount of distinct ASes almost only increased on each new scan for stateless scans. For IPv4 no SNI, 4792 distinct ASes were discovered on the first scan, but 5370 on the scan on the 4th January 2022 (see Table 5.2). This increase is equivalent to 12,06% more ASes at once. Only one larger jump was noticeable, that occurred after the switch to the IETF v1 `version` field, where many unique new IPs were discovered as well. The AS count jumped from 5255 to 8180 on the next scan after the 28th December 2021. After the `version` field was reset to the previous state, the number of ASes went down again to 5289. Since then, the amount only increased slowly until the last scan.

The SNI scan for IPv4 is more irregular than the stateless scans. After the first two scans there is a sudden drop to just 194 distinct ASes compared to 1170 on the 12th June 2021. The amount recovers to 826 unique ASes on the 15th July 2021, and after the succeeding scan, the count further increases to 1788 where the amount stabilizes until the 9th December 2021. From there on, the unique count drops to just 1287 where it slowly increases to 1356 on the 20th January 2022 and after that jumps back to 2316 on the next scan from where it only increases till the last scan, with 2221 unique ASes.

IPv6 no SNI behaves almost the same as IPv4 no SNI. The first scan contains 1713 distinct ASes. After that, a steady growth can be seen until the scan before the `version` field change, where 1921 unique ASes are observed. With the IETF v1 version set, 2067 unique ASes are discovered on the 7th January 2022 and 2060 on the 14th January 2022. After that, the amount slowly decreases to 1677 on the 18th February 2022 but quickly regains 259 reoccurring ASes on the 25th February 2022 for a total of 1922 with seven unique new ASes. The last scan then only increases slightly to 1928 total distinct ones.

In the case of IPv6 SNI, the same pattern as for IPv4 SNI can be observed in the beginning. The first two scans contain 515 distinct ASes, with a sudden drop to just 50 on the 19th June 2021. After that, the succeeding scan contains even less distinct ASes, with just eight total ASes. On the 15th July 2021 the count starts to rise again to 112 different ones, and on the 23rd July 2021 a sudden spike to 805 unique ASes occurs. However, in the next few scans, the amount drops to the same level as before and stabilizes between a count of 127 and 133, to then race to 700 on the 20th August 2021. From there on, the amount only grows to around 925, with a small dip to around 661 to 729 on the four scans between 5th November 2021 and 26th November 2021. After that, the amount stabilizes around 925 distinct ASes and reaches its peak on the 4th February 2022 with 1034 ASes. However, just after the peak, another larger drop occurs and only 686 distinct ones are observed. The last scan finishes with a total of 703 distinct ASes.

5.3 Spread of QUIC Deployments

The distribution of larger ASes (Figure 5.3) for IPv4 no SNI only changed a little in comparison to each succeeding scan, except for Google (AS15169) and Fastly (AS54113), which lost a lot of IPs between 16th August 2021 and 1st September 2021, but almost regained all of it, as described in Section 5.1. After 1st September 2021, Amazon-02 (AS16509) started to appear with a substantial share as well. The first scan after the `version` field change shows, that the distribution has shifted somewhat. Fastly (AS54113) and Google (AS15169) respond to a lot fewer requests. Fastly (AS54113) decreased from 233k deployments to only 68k, whereas Google (AS15169) even misses the 2% threshold. However, smaller ASes with a share of less than 2% of all discovered addresses answer 43,23% more. Furthermore, As-Hostinger (AS47583) appears as an AS with a larger share of around 51k deployments. After the switch of the `version` field back to the previous state, the smaller ASes decrease again, As-Hostinger (AS47583)

Table 5.3: Absolute change in AS spread of QUIC deployments for the different scan types since release up until the last scan. "$\leq$ 2.0%" is the sum of all ASes that do not exceed a 2% share for that specific scan.

	no SNI				SNI			
	IPv4		IPv6		IPv4		IPv6	
AS	**First**	**Last**	**First**	**Last**	**First**	**Last**	**First**	**Last**
209242	-	-	-	-	2,11%	-	2,67%	-
54113	9,36%	13,64%	-	-	-	-	-	-
47583	-	-	-	-	-	-	-	72,63%
20940	15,13%	10,87%	11,90%	7,69%	-	5,38%	-	-
16276	-	-	-	-	-	-	-	-
15169	23,75%	9,63%	12,39%	14,70%	36,05%	-	-	-
14061	-	-	-	-	-	3,31%	-	-
13335	31,69%	39,73%	58,03%	57,93%	54,36%	12,91%	91,28%	19,92%
12824	-	-	-	-	-	2,14%	-	-
4134	-	2,16%	-	-	-	33,77%	-	-
$\leq$ 2.0%	20,07%	23,97%	17,68%	19,69%	7,48%	42,49%	6,05%	7,45%

disappeared again but Google (AS15169) reappeared again. On the 18th January 2022 Amazon-02 (AS16509) disappears again but ChinaNet Assess (AS4134) appears with 37k addresses. From Table 5.3 the absolute change can be seen. The only two larger ASes which gained more addresses are Cloudflare Net (AS13335) and Fastly (AS54113). All others decreased in number. Additionally, the smaller ASes with a share of less than 2% of all discovered addresses gained more.

Compared to the no SNI scans, the SNI scans are fairly unstable and contain a lot of changes in the number of addresses, as can be seen in Figure 5.4. IPv4 SNI scans start with only three ASes with significant shares. The two larger ones are Cloudflare Net (AS13335) and Google (AS15169) with 141,8k and 94k deployments respectively. Furthermore, Cloudflare Spectrum (AS209242) is represented with a smaller share of 5,5k deployments. These ASes gain around 500 new deployments each until the 8th July 2021. However, smaller ASes with a share less than 2% gain 18k new deployments. On the 15th July 2021 the AS distribution experiences a shift. Whereas Cloudflare Net (AS13335) and Google (AS15169) only gain around 1-2k new deployments, the deployments from Cloudflare Spectrum (AS209242) drop below the 2% threshold. The ASes under the threshold increase to 167,9k deployments and two new ASes appear: OVH (AS16276) (15k deployments) and DigitalOcean (AS14061) (8653 deployments). From there on, the AS distribution remains stable until the 3rd September 2021, when Google (AS15169) suddenly decreases to 26,9k deployments. A2 Hosting Inc (AS55293)

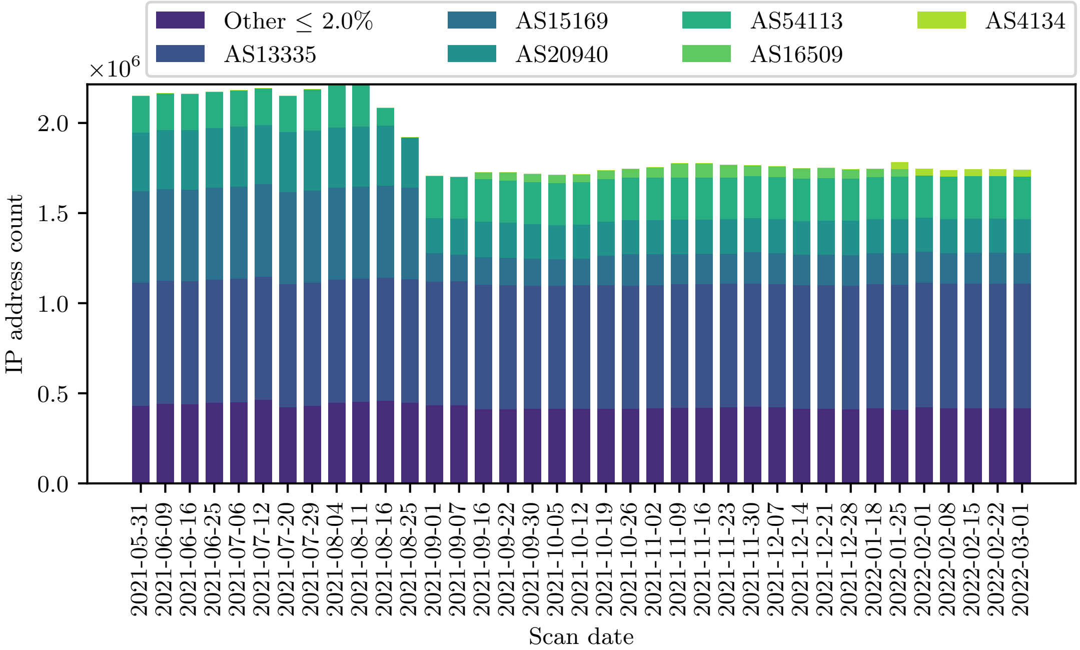


Figure 5.3: IPv4 AS distribution for no SNI

and GTS Telecom SRL (AS5606) emerge from the ASes with ≤ 2% share, with each around 8,2k deployments. The amount of deployments stabilizes again and a slight increase until the 14th October 2021 is noticeable. On that date, As-Hostinger (AS47583) increases to 11,1k deployments and is elevated above the threshold. No larger shifts are apparent until the 2nd December 2021, only with 1-2k changes for most ASes, except for As-Hostinger (AS47583) which has gained 13k addresses over the last few scans and Cloudflare Net (AS13335) suddenly jumps by 17k to 154k overall addresses. The successive scan drops from 412k total addresses to 362k. Cloudflare Net (AS13335) decreases by 20k addresses and DigitalOcean (AS14061) drops to below the threshold. However, the ASes with ≤ 2% also further decreased by 12k and Google (AS15169) by 6k addresses. Furthermore, all other ASes also decrease by 6 to 8%. The ASes do not change significantly on the consecutive scans until the 20th January 2022, only with DigitalOcean (AS14061) moving above the threshold again between the 6th January 2022 and 13th January 2022, and Google (AS15169) decreasing to 11k addresses and then increasing again up to 47,5k. On the 27th January 2022 another 10k addresses are added to Google (AS15169), however A2 Hosting Inc (AS55293), GTS Telecom SRL (AS5606), and As-Hostinger (AS47583) also move below the threshold of 2%, so the smaller ASes jump to 196,7k addresses. Furthermore, Cloudflare Net (AS13335) jumps to 160,7k addresses from 134k. The total number of addresses is around 428k addresses. With the next scan, the amount further increases to 454,6k. DigitalOcean (AS14061) and As-Hostinger (AS47583) both regain addresses and reappear with 10 and 9,1k addresses. OVH (AS16276) also gains further 17k addresses. On the last few scans no ASes move below or above average, however all gain further addresses. Only As-Hostinger (AS47583) experiences a significant increase to 25,5k addresses. The last scan contains the all-time high for the number of addresses with 473,7k distinct ones.

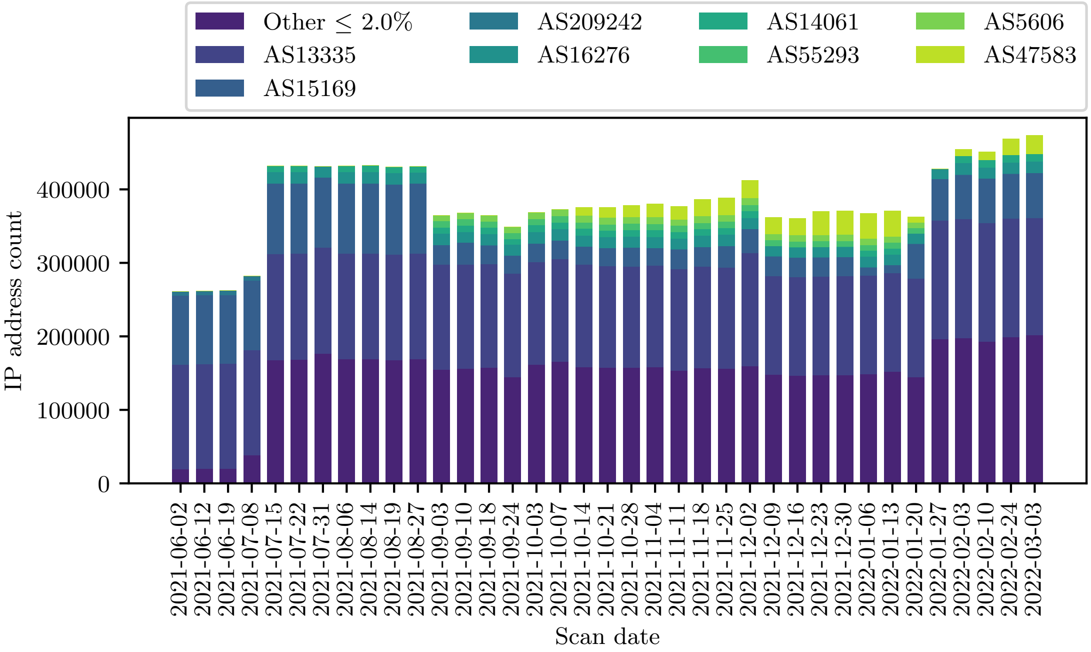


Figure 5.4: IPv4 AS distribution for SNI

Regarding IPv6 no SNI, Cloudflare Net (AS13335), Google (AS15169), and Akamai-ASN1 (AS20940) have the largest share of QUIC deployments. From the 5th November 2021 onwards, Amazon-02 (AS16509) has the majority in shares. However, as previously described in Section 5.1 the IPs from Amazon-02 (AS16509) fluctuate a lot and disappear again. Since the `version` field changes, after 7th January 2022, larger new ASes do appear with the most prominent being As-Hostinger (AS47583) (61k new addresses) and Cloudflare Spectrum (AS209242) (48k addresses). Additionally, Akamai-ASN1 (AS20940) decreased drastically with around 24k addresses. As can be seen in Table 5.3, the absolute change is not very large. No significant new ASes appeared. The largest shift is by Akamai-ASN1 (AS20940), with a decrease from 11,90% to 7,69%. Otherwise, all ASes did not change by more than 2%.

The SNI scans (Figure A.1d) contain only five different ASes with a larger share than $\leq 2\%$ at any point in time. However, on the first scan only Cloudflare Net (AS13335) appears with 120,5k, and Cloudflare Spectrum (AS209242) with 3521 distinct addresses. The number of deployments under the threshold is also small with just 7993 unique addresses, making Cloudflare Net (AS13335) by far the majority with 91,2% of all addresses. This state remains for the next two scans. On the 9th July 2021 deployments $\leq 2\%$ drop to 1035 addresses. Cloudflare Spectrum (AS209242) completely disappears and Cloudflare Net (AS13335) decreases to 70,9k addresses. However, on the next scan, many new unique addresses are discovered. Privatesystems (AS63410) appears with 5785 addresses in addition to 174k addresses of As-Hostinger (AS47583). Also, Cloudflare Net (AS13335) increases by 5k addresses and $\leq 2\%$ ASes gain 13k addresses. The successive scan contains a spike to 336,6k total addresses, mainly consisting of a jump of Cloudflare Net (AS13335) to 122k addresses. Privatesystems (AS63410) drops under the threshold and $\leq 2\%$ increases to 36k deployments. However, on the next scan, the previous state is restored and stays the same for the three scans. On the 14th August 2021 a new spike is observed, which is very similar to the previous one. Cloudflare Net (AS13335) reaches 122k addresses and $\leq 2\%$ increases to 31,1k. From that date on, the AS distribution is stable again until the 5th November 2021, when a new AS, Amazon-02 (AS16509) appears with 37,5k addresses and As-Hostinger (AS47583) increases from 151k to 191k. For the next scan, the same two ASes increase by 83,8 and 122,9k addresses respectively. One more jump in unique addresses is observed on the 19th November 2021 for the ASes Amazon-02 (AS16509) (to 155,5k) and As-Hostinger (AS47583) (to 382,2k). However, all addresses from Amazon-02 (AS16509) disappear on the 26th November 2021. ASes $\leq 2\%$ increase by 9k addresses to 40,9k and As-Hostinger (AS47583) gains another 20k addresses. These two ASes keep increasing until the last scan. Smaller ASes with $\leq 2\%$ reach a max of 54,5k addresses on the 3rd December 2021 but remain at around 48,8k unique addresses on the last scan. Furthermore, As-Hostinger (AS47583) increases to 476,5k addresses until the last scan with an all-time high of 486k addresses on the 14th January 2022. On the same date, Amazon-02 (AS16509) reappeared for one scan with 90,5k addresses. Cloudflare Net (AS13335) remained at around 130k addresses since the 3rd December 2021 and has only fluctuated by around 1k.

5.4 Count of QUIC Hosts and their ASes

When filtering the SNI scans based on distinct hostnames and not IPs, the number of deployments change drastically and are multiple times larger than the amount non SNI scans (see Table 5.4). SNI scans regarding the hostnames are very much dominated by only a few ASes, with the largest one being Cloudflare by far (share never drops below 64% for IPv4 and never below 90% for IPv6), as can be seen in Table 5.5.

Table 5.4: Absolute change in distinct host count of QUIC deployments

Version	First	Last	% change
IPv4	5.485.035	20.322.859	+ 270,51
IPv6	5.060.372	14.239.893	+ 181,40

Table 5.5: Absolute change in AS spread of QUIC deployments for hosts. ”≤ 2.0%” as explained in Table 5.3

	IPv4		IPv6	
AS	**First Scan**	**Last Scan**	**First Scan**	**Last Scan**
47583	-	-	-	4,95%
16276	-	2,40%	-	-
15169	3,78%	-	-	-
13335	93,95%	64,67%	99,25%	90,52%
≤ 2.0%	2,27%	32,93%	0,75%	4,54%

Regarding IPv4 (Figure 5.5), 5,485 million unique hostnames are discovered on the first scan. This amount stays the same for the following two scans but jumps to 12,788 million on the 8th July 2021. On the 15th July 2021 the number of unique hostnames further increases to 19,7 million, almost reaching the amount of the last scan. However, from there on the number of unique hostnames fluctuates between 19,4 million (16th December 2021) and 21,568 million (6th January 2022) until the last scan. The maximum of above 21 million is only reached for two dates, the 6th January 2022 and 13th January 2022.

Except for the first four scans (5,15 to 5,17 million unique hosts for the first three scans and 12,348 million on the 8th July 2021), Cloudflare Net (AS13335) serves between 13,1 and 14,1 million unique hosts. The other major part of all scans are the ASes with ≤ 2% share. From the 15th July 2021 on, around 5,15 to 6,9 million hosts are part of these smaller ASes.

There are also 5,06 million IPv6 hosts discovered on the first scan. The amount does not change a lot for the first three scans. On the 9th July 2021 a significant drop to just 3,377 million addresses is observed. However, on the next scan, over 12,646 million unique hosts are discovered. This number steadily increases until the 14th January 2022. From where a small decline to just 15,149 million hosts until the 4th February 2022 occurred.

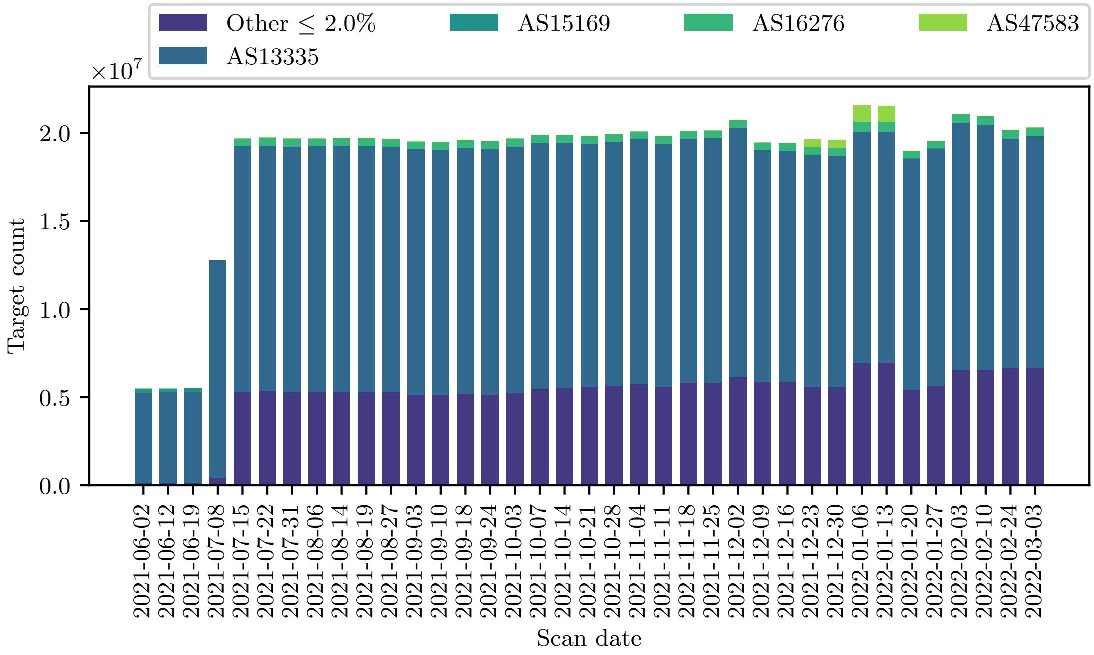


Figure 5.5: IPv4 AS distribution of SNI IPv4 scans

A further drop by 1 million addresses happens on the next scan, but on the last scan, a slight increase can be noticed again to finally reach around 14,24 million addresses.

The AS distribution for IPv6 is even more extreme than for IPv4 regarding hosts. On all scans, the share of Cloudflare Net (AS13335) is above 90%. From the 15th July 2021 on, the ASes with a share of $\leq$ 2% are only barely represented with a share between 2,74% and 4,08%. Since 12th November 2021 one other AS besides Cloudflare Net (AS13335) has a significant share with more than 2%: As-Hostinger (AS47583). However, the maximal share reached by AS47583 is only at around 5,01% and thus, very little.

5.5 Version Distribution of QUIC Deployments

QUIC's versions are distributed by the owners of different implementations. Each owner is assigned a version prefix that they can increment to differentiate their own versions of QUIC. A list of all the owners and their respective prefixes can be found at Quicwg [19]. For the sake of this thesis, the hex code is translated into human-readable version names. Table A.1 lists the owners and their version alias schema that is used in this thesis.

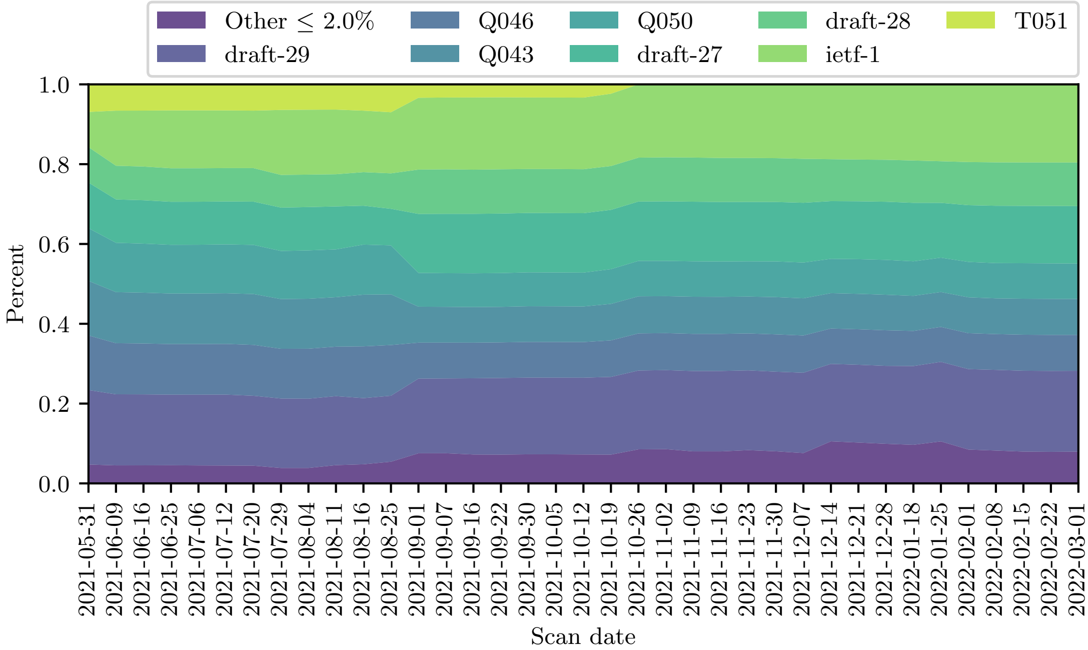


Figure 5.6: Relative QUIC version distribution for IPv4 addresses with the dates 3rd January 2022 and 14th January 2022 missing because of the changed `version` field as mentioned in Chapter 2

The relative version distribution of the IPv4 address space did not change a lot over time, as can be seen in Figure 5.6. Since the release of QUIC v1 the dominant versions seem to be ones by the IETF and Google. The biggest change since release occurred on the 1st September 2021, when the addresses of Google (AS15169) disappeared as described in Section 5.1. Because this was an AS controlled by Google, mostly versions from Google were announced by those IPs. Therefore, mainly Q043, Q046 (both 12,7% to 9,01%), Q050 (12,27% to 8,46%) and T051 (6,99% to 3,36%) decreased. Interestingly the Google TLS version further kept decreasing until the 26th October 2021, where the number of IPs serving Google TLS fell below the 2% threshold.

As anticipated, the relative share of the IETF versions did grow over time with the `ietf-1` version having the largest growth since release. On the last scan, the relative share has reached 19,58% (vs. 8,81% on the first). However, `draft-29` with 20,26% was still the most represented version. draft-27 remained the oldest IETF version with a significant (14,41%) share. Despite, `draft-27` being released on 24th August 2020 and quickly updated with version 28 just three months later on the 21st November 2020, the share remained far larger then the one of `draft-28`.

On the first scan, IETF versions (ietf-1, draft-29, draft-28, draft-27) were supported by 47,78% of all QUIC deployments. Google accounted for 47,49% (with versions T051, Q050, Q046, and Q043). The last scan shows that the share of the IETF versions has increased to 65,17% and Googles versions decreased to 26,88%.

In the case of IPv6, the version distribution is similar to the one of IPv4, however, the IETF v1 version is much closer to draft-29. ietf-1 is supported by 21.72% (vs. 14,6% on the first) of all IPv6 deployment on the last scan, but draft-29 exceeds this with 21.79%. Otherwise, there is a sudden spike in support for draft-29 between 29th October 2021 and 10th December 2021 because of the many deployments by Amazon-02 (AS16509). Furthermore, on the 24th December 2021 a spike in additional supported versions can be recognized with draft-30 to draft-34 having a significant share of around 4,4% each.

IPv6 started with a larger IETF version share compared to IPv4. 65,64% of all deployments supported one of ietf-1, draft-29, draft-28, draft-27. Whereas Google's versions were only supported by 30.65% of all deployments. On the last scan over 72,37% of all deployments announced support for one of IETF's versions. The share of Google declined to just 23,65%.

Table 5.6: Relative version group distribution of QUIC for IPv4

Versions	**First Scan**	**Last Scan**
ietf-1 draft-29 draft-28 draft-27	33,23%	42,33%
draft-29 T051 Q050 Q046 Q043	27,21%	2,59%
Q050 Q046 Q043	22,72%	18,70%
draft-29 draft-27	9,33%	-
mvfst-2 mvfst-1 mvfst-14 draft-29 draft-27	2,05%	-
ietf-1 draft-29 draft-27	-	13,66%
ietf-1 draft-29 Q050 Q046 Q043	-	12,12%
ietf-1 draft-29 draft-30 draft-31 draft-32	-	4,43%
mvfst-2 mvfst-14 mvfst-16 ietf-1 draft-29	-	2,90%
Other $\leq$ 2.0%	5,46%	3,28%

Looking at the version group distribution for IPv4 (Table 5.6), more versions of QUIC appear, which did not have a significant share when looking at each versions on its own. Namely, Facebook's mvfst is represented a lot with its versions ranging from 2 to 16. Also, the reason why the IETF versions have the largest share can be seen. Almost all common version groups contain at least one IETF version. However, ietf-1 is only announced in eight of the 16 groups (the groups can be seen in Figure A.1b) with a larger share than 2% at one point in time. Additionally, all groups that contain ietf-1 also contain draft-29. Furthermore, 14 of the 16 groups contain draft-29, making it obvious why draft-29 has a larger share on its own than ietf-1.

5.6 Responses on Connection Establishment

The responses on connection establishment can be of different kinds. In the best case, the connection is successful, and no error message is returned. However, if an error occurred and the connection establishment failed, than a reason is returned to the client. In most cases, the error is classified as a crypto error. Error messages arising from cryptographic problems are hard to differentiate because a generic code (0x128) (as defined in RFC [20]) may be returned as a security measure. However, there is a code included with each crypto error that corresponds to the hex value of a TLS error. The ones that have occurred for a significant amount are listed in Table 2.1.

As already mentioned in Section 5.1, the amount of IPv4 no SNI addresses that were discovered via ZMap have decreased since the release of version one. This is rather contrary to the expectation of growing adoption due to the improvements of QUIC in comparison to TCP + TLS. However, the relative successful connection rate has increased from 6.95% (first scan) to 15,92% (last scan) for no SNI scans, with an all-time high of 18.48% on the 27th August 2021. Crypto errors with the code 0x128 stayed steadily around the same share, but from 18th September 2021 on, the code 0x131 started to appear persistently. Rare errors with less than 2% relative share decreased slowly from 35,70% to 25,48% until the last scan.

The errors differ quite a bit after the version field change. Most of the unsuccessful connections occurred because of cryptographic errors for both methods, with the major one being the generic / handshake error (0x128). However, all scans with the version field set differently suffered rare occurring errors. The first big difference seems to be in the timeout error. The scans with the version field set to the version negotiation value (0x?a?a?a?a) experiences over three times more timeouts. Furthermore, many deployments contacted with the new packet, answer with a 0x131 crypto error, which corresponds to the access_denied (Table 2.1) TLS error. And lastly, the new packet also seems to trigger no compatible QUIC versions found errors, which did not appear with a significant share for the previous packet.

Compared to the no SNI scans, a lot more connections were successful for the SNI scans. Over the timespan of all scans, the rate improved from 35,72% to 54,88%. Protocol violation consistently stayed at around 4% to 5% with a spike between the 19th June 2021 and 27th August 2021 with ranges between 20,69% to 34,44%. no compatible QUIC version and timeout errors only appeared after the 8th July 2021,

Table 5.7: Relative average error message distribution of IPv4, for both `version` fields as well as for no SNI and SNI scans.

	no SNI		**SNI**
error type	**0x?a?a?a?a**	**0x00000001**	
crypto error (0x128)	45,21%	41,21%	17,12%
other ≤ 2.0% share per scan	26,20%	23,87%	4,60%
successful	15,55%	12,31%	44,07%
timeout	10,73%	3,38%	19,20%
crypto error (0x131)	1,43%	2,73%	-
crypto error (0x150)	-	12,88%	-
no compatible QUIC version	-	2,58%	6,36%
protocol violation	0,5%	1,04%	8,52%

with the former stabilizing between 19% to 24%. The latter appeared with a rate of 12,25% but continuously decreased to 4,91% until the last scan. Furthermore, in the beginning, rare errors with less than 2% relative share occurred with a major stake of around 34,22%, but dropped to approximately 2% to 4% from the 19th June 2021 on.

IPv6 no SNI (Figure A.1a) evolved similarly to IPv4. In the beginning, the relative connection success rate was at 27,20% with an all-time high of 31,59% on the 22nd January 2022. Over time a decrease to 31,50% until the last scan was observed. However, a strong decrease was noticeable to around 14% with the `version` field set to the IETF v1 code. Previous to that change, the rate fluctuated between 12% to 31%, because of the unresponsive IPs by Amazon-02 (AS16509) as described in Section 5.1. Almost all IPs from this AS responded with `crypto error (0x131)` or `access_denied` TLS errors (see Table 2.1). Otherwise, `crypto error (0x128)` has consistently the largest stake with about 120 to 130k deployments responding with this error on each scan. The `transport parameter` error solely appeared on the 19th June 2021 with a share of 4,46%. Additionally, one further large change with the new version field set was that many `crypto error (0x150)` errors occurred. With 15,56%, respective 15,29%, the error had a larger share than all successful connections for those two specific scans on the 7th January 2022 and 14th January 2022. Lastly, `no compatible QUIC version` errors also appeared with a share of 2,07% on the scan on the 7th January 2022, whereas they were not significant on the previous scans.

Many similarities to Table 5.7 can be seen regarding the IPv6 SNI scan in Table 5.8. `crypto error (0x128)` and the successful connections both changed in the same way, compared to their respective no SNI scans. Successful connections increased and the 0x128 crypto error decreased significantly. The rare errors with less than 2% relative

Table 5.8: Relative average error message distribution of IPv6, for both version fields as well as for no SNI and SNI scans.

	no SNI		**SNI**
error type	**0x?a?a?a?a**	**0x00000001**	
crypto error (0x128)	50,31%	38,03%	12,15%
successful	25,45%	13,66%	65,48%
crypto error (0x131)	13,29%	23,07%	1,83%
other ≤ 2.0% share per scan	10,46%	8,78%	0,76%
crypto error (0x150)	-	15,42%	-
no compatible QUIC version	-	1,04%	1,28%
timeout	-	-	18,08%

share also significantly decreased compared to the SNI scans. The success rate started at 58,18% with a drop to 27,83% on the 15th July 2021, from where the rate alternates between 25,40% and 30,62% till the 4th September 2021. From there on, the success rate almost increased on every new scan up to 88,61% on the last scan. This is an especially impressive result because the unique IP count increased from 132 to 656k. The `crypto error (0x128)` error started off with a large share of 38,94% and dropped over time to just 8,48% on the last scan. On the dates 15th July 2021 and from 1st August 2021 to 14th August 2021 the error did not significantly appear at all. However, including this time range, more specifically from 15th July 2021 to 8th October 2021 the `timeout` error started to completely overshadow all other errors with a max of 66,33% on the 15th July 2021 and then slowly decreasing to 3,02% on the 29th October 2021. Nearly all of these errors occurred by contacting IPs from Cloudflare Net (AS13335). The `crypto error (0x131)` only significantly appeared on the three scans 5th November 2021 to 19th November 2021 with a share of 9,80%, 20,64%, and 22,53%. Similarly, the `no compatible QUIC version` error only significantly appeared between the 15th July 2021 to the 20th August 2021 and once on the 29th October 2021 with an average of 2,5% for these seven scans.

5.7 HTTP Server Spread from Headers

QScanner (Chapter 2) connections that were able to contact the QUIC deployment via HTTP and got a valid response back, can be analyzed by each HTTP header. One of these headers is the `Server` type header, which informs the client via which HTTP server the QUIC connection supplies its content.

Only a max of around 269k unique addresses responded to a request via HTTP for the stateless IPv4 no SNI addresses. Ten different HTTP servers with a relative share of over 2% were found, as can be seen in Figure 5.7. Whereas for the first two scans only six major servers were found from around 102k addresses, the number quickly rose on the 18th June 2021 to 136k addresses with three new HTTP servers, but `proxygen-bolt` completely stopped serving. Consecutive scans did not change a lot, but another stark jump in addresses occurred on the 22nd July 2021 when the number of unique addresses increased to 187k. Almost all of these additional addresses were reappearing `proxygen-bolt` addresses.

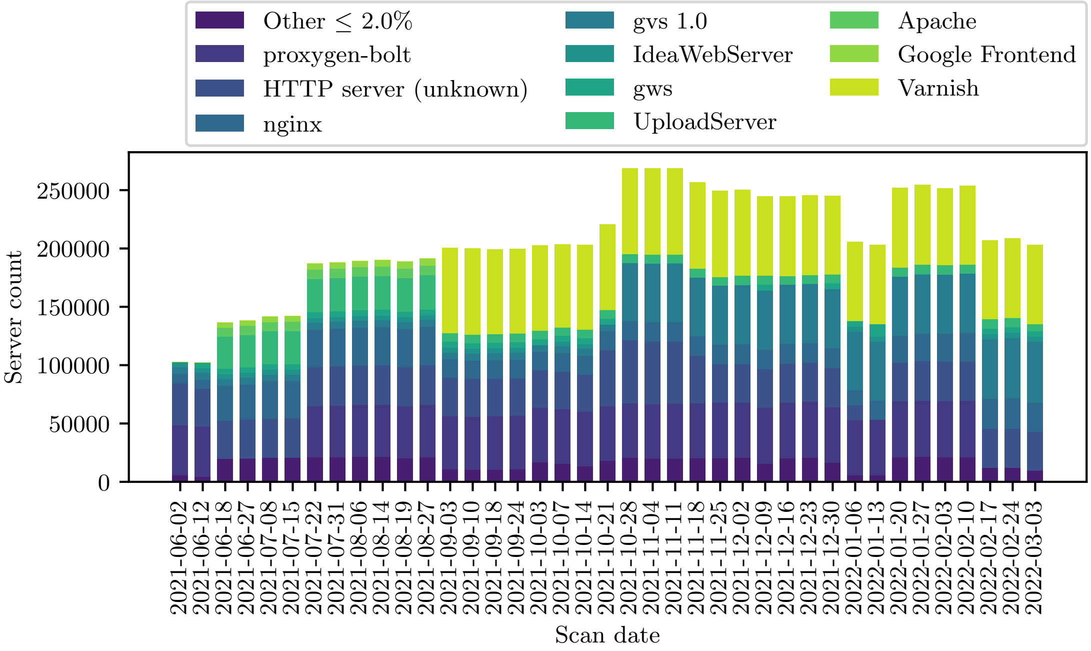


Figure 5.7: Distribution of IPv4 no SNI HTTP servers for each distinct address as ”sever count”

The addresses stabilized again and not a lot of changes appeared until the 3rd September 2021, when `Apache` and `Google Frontend` disappeared from the significant server list. Additionally, `UploadServer` and `nginx` each lost 21k and 17k addresses at once. The less significant servers with less than 2% relative share also lost more than 10k addresses. However, the dropped number of addresses all were replaced by a new server: `Varnish`, which appeared with around 73k unique addresses. Nearly all of these new IPs were in the range of FASTLY's (AS54113) IP ranges[1]. Varnish[2] is a caching and a load balance HTTP proxy, which can be installed in front of any HTTP server to

[1] `https://api.fastly.com/public-ip-list`

[2] `https://varnish-cache.org/`

improve content delivery. Furthermore, on the 28th October 2021 another big increase in IPs occurred, where `gvs 1.0` jumped from just under six thousand deployments to around 50k.

After a slight decline, the number of addresses stabilized. With the new `version` field set for ZMap scans on the 6th January 2022 and 13th January 2022, the number of unique addresses decreased again. Furthermore, the amount of rarer ($\leq$ 2% share) HTTP servers decreased by ten thousand IPs. Additionally, responses with `HTTP server (unknown)` appeared with 20k addresses less. When looking at the ASes of these IPs, these addresses belong to Google (AS15169) and suffered a loss of about 25k. After the change back to the old `version` field, almost the same state as before is observed, however, after the 17th February 2022 deployments previously announcing `proxygen-bolt` as their server stopped to set the `server` header field, and do not appear anymore.

IPv4 SNI is dominated by two HTTP servers as can be seen in Figure A.1c: `cloudflare`, and `LiteSpeed` with `proxygen-bolt` and `IdeaWebServer` also appearing with significant shares. On the first scan, `IdeaWebServer` appears with around three thousand deployments but sinks below the 2% relative share threshold on the 7th October 2021. At the same time `proxygen-bolt` also has a larger share than 2% until the 4th November 2021 with around five to seven thousand deployments. Over the whole time, `cloudflare` bounces between 94k to 100k deployments. `LiteSpeed` starts appearing from the 15th July 2021 onwards with around 20k deployments and the amount only increased steadily on each consecutive scan until the end, when `LiteSpeed` reached 90k deployments. The usage of QUIC was turned on by default for LiteSpeed on the 7th June 2021 (”Enable HTTP/3 v1 by default”[1]), which might explain the steady increase on each scan. After the 20th January 2022 new HTTP servers appear: `nginx` and `UploadServer` both, with around 6 to 6,5k addresses, furthermore, smaller servers with $\leq$ 2% share also increase by 2k addresses. On the succeeding scan `proxygen-bolt` reappears with around 6k addresses and `gvs 1.0` appears for the first time with 14,9k addresses. The amount for the new servers increases with each consecutive scan slightly, however, `proxygen-bolt` completely disappears after the 24th February 2022 again.

IPv6 no SNI has a smaller amount of HTTP servers serving via QUIC than IPv4. With only four being significant with a share larger than 2% at any point over the year and all of them are already observeable on the first scan: `proxygen-bolt` (8,7k), `nginx`, (3,8k) `gvs 1.0` (2,9k) and `UploadServer` (516). The amount of deployments only increases slightly until the 29th October 2021 where `gvs 1.0` gains around 22k addresses at once.

[1] `https://www.litespeedtech.com/products/litespeed-web-server/release-log`

After the 25th February 2022, the same way as for IPv4, the deployments of `proxygen-bolt` stopped setting the `server` header field and disappeared. Otherwise, the amount only changes slightly until the end.

IPv6 SNI is very similar to Section 5.7 as in there are the same two very dominant HTTP servers that cover almost 97% of the deployments on the last scan. The other changes are also very similar. `cloudflare` is present again with an almost constant growth and fluctuations between 69 and 89k addresses.

Just like mentioned in Section 5.7 `LiteSpeed` starts to appear on the 1st August 2021 with just six thousand deployments and then adding more deployments after each consecutive scan, until at the last scan just under 487k deployments are reached.

Chapter 6

Conclusion

One year after the release of v1 still seems to be a very small portion of the overall lifetime of an internet protocol like QUIC. Many things have changed since the release, and are changing still. The larger companies seem to have great expectations for QUIC and can already offer examples of some real-world benefits compared to TCP + TLS, thus making the protocol more and more attractive with continuous development and improvements.

6.1 Summary of Results

Analysis shows, that the number of distinct IPs detected by ZMap for IPv4 has encountered a decline. On the other hand, the IPv6 counterpart almost stayed the same all the time, with just one large AS (Amazon-02 (AS16509)) showing atypically fast changes with a lot of unresponsive deployments. This AS also disappeared after a few scans almost completely.

Despite the fluctuation in the number of unique addresses, both address spaces steadily increased in the number of unique ASes that they were served by. The ASes controlled by larger companies still make up the vast majority of all deployments and thus, the largest changes were detected for these ASes. However, many new smaller ASes appeared since release, and they keep increasing in the amount as well as in their share compared to the larger ones.

When looking at the version distribution of the deployments, a clear move towards the newer IETF versions was observed. Since the release of QUIC v1, many deployments using versions by Google switched, as can be seen in Section 5.5. However, the number of other implementations also grew somewhat, with versions by Facebook increasing the most besides the IETF versions. One further interesting aspect is, that almost no deployment exists without support for at least one of the IETF versions, guaranteeing good compatibility and interoperability.

In the case of deployments discovered via SNI the relative increase was faster than for no SNI, especially regarding unique hostnames. Both addresses spaces resulted in a significant increase with IPv6 even evolving to a multitude of deployments compared to the first scan. With the distinct hostnames as the separating factor, the results get very one-sided because Cloudflare and LiteSpeed make up 98,55% percent of all deployments.

Furthermore, the analysis also shows, that the amount of IPs is not all that matters because discovered stateless IPs can be unresponsive on a stateful connection establishment. Overall, the success rate for connection establishment has improved concerning the number of IPs for IPv4 but decreased for the IPv6 addresses. The average relative success rate for no SNI scans is very similar for both address spaces. SNI scans on the other hand exceed the no SNI rate and result in about 2,5 times more successful connections.

Unresponsive IPs act very similarly in both cases, IPv4 and IPv6. The most significant reasons for unresponsive IPs are `crypto error` type errors for all scan types. In the case of relative error rate, the only significant difference for SNI scans is, that the `timeout` error is somewhat more common.

After the change of the `version` field to `0x00000001` instead of the reserved `0x?a?a?a?a` pattern to trigger a `version negotiation` packet the success rate decreased slightly on average for both, IPv4 and IPv6. However, more `no compatible QUIC version` and `protocol violation` errors started to appear, which is expected as the deployments act according to the RFC. But also far more `crypto error (0x150)` errors started to appear.

When looking at the distribution of the HTTP servers discovered by no SNI IPs, Google has one of the largest combined shares and is almost always using its in-house server software. Otherwise, the well-known, sophisticated HTTP servers are the most prevalent, like `nginx`, `Apache`, or `Varnish`. For SNI scans, the amount of Google's software almost drops to zero. Furthermore, Cloudflare and LiteSpeed completely dominate the deployments discovered by SNI with their self-made HTTP servers.

6.2 Future Work

With the amount of changes, continuous observation of the deployments is a must to see the impact of the protocol on the Internet and if it is able to replace TCP + TLS in some areas.

Furthermore, there are multiple RFCs that are still in the works, that could majorly influence the future evolution of the protocol. When HTTP/3 will be released, further increase in the usage of QUIC is expected, leading to more discoverable deployments. Additionally, to the new HTTP version, the second IETF version of QUIC (Duke [21]) is also already in development. When all the early problems of QUIC are solved with the second version, even more deployments could switch to using QUIC. With new RFCs, the scans should be updated to reflect the new versions. Also, a comparison of v1 and v2 adoption rate would be important to evaluate maturity of the protocol.

This thesis evaluated IPv4, IPv6 addresses and domains separately on their own, however if it would be possible to estimate if different addresses from the different address spaces are part of the same full stack deployment, a more accurate number for the amount of QUIC deployments could be obtained.

Also, the `version` field set differently for the ZMap scans (described in Chapter 4) shows very different results. According to RFC 9000 ([8]), the first method should be accepted by all QUIC implementations. This does not seem to be the case. On more in-depth analysis the QUIC implementations and their versions that are not accepting the RFC specific trigger of Version Negotiation packets could be filtered out and analyzed. Furthermore, the implementations that only answer to the first method are also of interest and could show that there is already ossification happening between the deployments.

Chapter A

Appendix

A.1 List of Acronyms

ALT-SVC	Alternative Services
IETF	Internet Engineering Task Force
HTTP	Hypertext Transport Protocol
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
RFC	Request for Comments
SNI	Server Name Indication
DNS	Domain Name System
HOL	Head-of-Line Blocking
QoE	Quality of experience
RTT	Round-Trip-Time
AS	Autonomous System
RR	Record Ranges

A.2 List of ASes

AS209242	Cloudflare Spectrum
AS63410	Privatesystems
AS55293	A2 Hosting Inc
AS54113	Fastly
AS47583	As-Hostinger

AS20940	Akamai-ASN1
AS16509	Amazon-02
AS16276	OVH
AS14061	DigitalOcean
AS15169	Google
AS13335	Cloudflare Net
AS5606	GTS Telecom SRL
AS4134	ChinaNet Assess

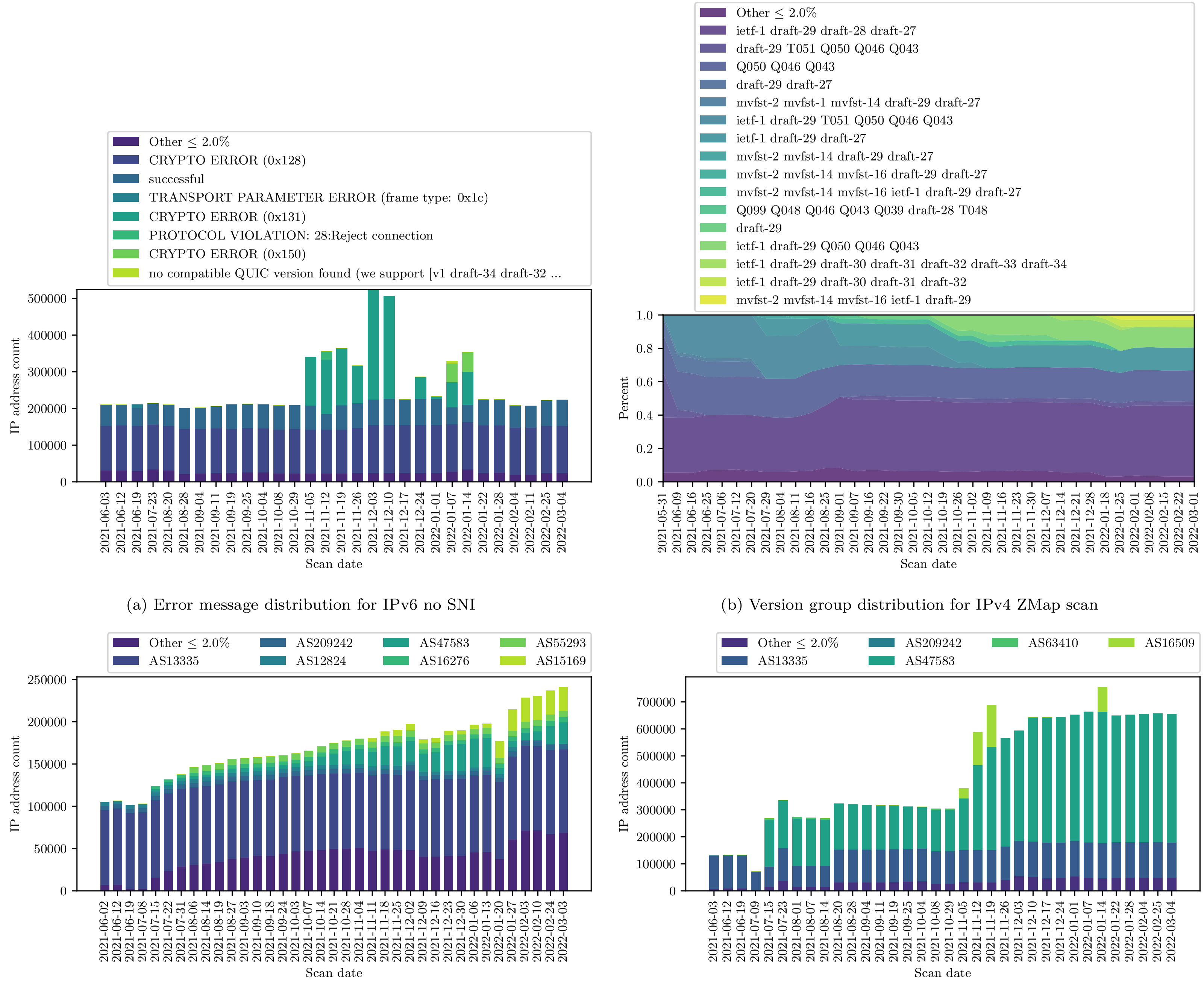
A.3 Additional Tables and Graphs

Table A.1: QUIC implementations naming schema with x being the version number.

Owner	**Naming Schema**
IETF drafts	draft-x
IETF	ietf-x
NetApp	quant-x
Private Octopus	picoquic-x
Google	G0xx
Google TLS	T0xx
Google proxy	prox
quic-go	quicgo-x
quicly	quicly -x
Microsoft	msq-x
Mozilla	mozq-x
Facebook	mvfst-x
ETH Zürich	ethzue-x
Telecom Italia	tcit-x
quinn-noise	quinn-x

Table A.2: HTTP servers and their developers

HTTP server	**developed by**
proxygen-bolt	Facebook
nginx	Nginx, Inc
IdeaWebServer	home.pl (Apache fork)
gvs 1.0, gws, UploadServer, Google Frontend	Google
Apache	Apache Software Foundation
Varnish	Varnish Software
LiteSpeed	LiteSpeed Technologies
cloudflare	Cloudflare



(a) Error message distribution for IPv6 no SNI

(b) Version group distribution for IPv4 ZMap scan

(c) AS distribution for IPv4 SNI addresses responding to connections via HTTP

(d) AS distribution for IPv6 SNI

Figure A.1: Additional figures

Bibliography

[1] Quicwg, *Implementations · quicwg/base-drafts Wiki*, Accessed: 2021-12-09. [Online]. Available: https://github.com/quicwg/base-drafts/wiki/Implementations.

[2] A. Deveria, *HTTP/3 protocol: Can I use... Support tables for HTML5, CSS3, etc*, Accessed: 2021-12-09. [Online]. Available: https://caniuse.com/http3.

[3] M. Bishop, "Hypertext Transfer Protocol Version 3 (HTTP/3)", Internet Engineering Task Force, Internet-Draft draft-ietf-quic-http-34, Feb. 2021, Work in Progress, 75 pp. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-quic-http-34.

[4] A. Langley, A. Riddoch, A. Wilk, A. Vicente, C. B. Krasic, C. Shi, D. Zhang, F. Yang, F. Kouranov, I. Swett, J. Iyengar, J. Bailey, J. C. Dorfman, J. Roskind, J. Kulik, P. G. Westin, R. Tenneti, R. Shade, R. Hamilton, V. Vasiliev, and W.-T. Chang, "The QUIC Transport Protocol: Design and Internet-Scale Deployment", 2017.

[5] M. Joras and Y. Chi, *How Facebook is bringing QUIC to billions*, Accessed: 2022-04-13, 2020. [Online]. Available: https://engineering.fb.com/2020/10/21/networking-traffic/how-facebook-is-bringing-quic-to-billions/.

[6] Facebookincubator, *Facebookincubator/MVFST: An implementation of the Quic Transport Protocol*, Accessed: 2022-03-11. [Online]. Available: https://github.com/facebookincubator/mvfst.

[7] Microsoft, *Microsoft/msquic: Cross-platform, C implementation of the IETF QUIC protocol*, Accessed: 2022-03-11. [Online]. Available: https://github.com/microsoft/msquic.

[8] J. Iyengar and M. Thomson, *QUIC: A UDP-Based Multiplexed and Secure Transport*, RFC 9000, May 2021. DOI: 10.17487/RFC9000. [Online]. Available: https://rfc-editor.org/rfc/rfc9000.txt.

[9] J. Rüth, I. Poese, C. Dietzel, and O. Hohlfeld, "A First Look at QUIC in the Wild", *CoRR*, vol. abs/1801.05168, 2018. arXiv: 1801.05168. [Online]. Available: http://arxiv.org/abs/1801.05168.

[10] J. Zirngibl, P. Buschmann, P. Sattler, B. Jaeger, J. Aulbach, and G. Carle, “It’s over 9000: Analyzing early QUIC Deployments with the Standardization on the Horizon”, in *Proceedings of the 2021 Internet Measurement Conference*, Virtual Event, USA: ACM, 2021. doi: `10.1145/3487552.3487826`.

[11] Lucas-Clemente, *Lucas-Clemente/quic-go: A quic implementation in pure go*, Accessed: 2022-03-11. [Online]. Available: `https://github.com/lucas-clemente/quic-go`.

[12] M. Kühlewind and B. Trammell, “Manageability of the QUIC Transport Protocol”, Internet Engineering Task Force, Internet-Draft draft-ietf-quic-manageability-16, Apr. 2022, Work in Progress, 35 pp. [Online]. Available: `https://datatracker.ietf.org/doc/html/draft-ietf-quic-manageability-16`.

[13] T. Shreedhar, R. Panda, S. Podanev, and V. Bajpai, “Evaluating QUIC Performance over Web, Cloud Storage and Video Workloads”, *IEEE Transactions on Network and Service Management*, pp. 1–1, 2021. doi: `10.1109/TNSM.2021.3134562`.

[14] S. Cook, B. Mathieu, P. Truong, and I. Hamchaoui, “QUIC: Better for what and for whom?”, in *2017 IEEE International Conference on Communications (ICC)*, 2017, pp. 1–6. doi: `10.1109/ICC.2017.7997281`.

[15] D. Saif, C.-H. Lung, and A. Matrawy, “An Early Benchmark of Quality of Experience Between HTTP/2 and HTTP/3 using Lighthouse”, in *ICC 2021 - IEEE International Conference on Communications*, 2021, pp. 1–6. doi: `10.1109/ICC42927.2021.9500258`.

[16] K. Wolsing, J. Rüth, K. Wehrle, and O. Hohlfeld, “A performance perspective on web optimized protocol stacks”, in *Proceedings of the Applied Networking Research Workshop*, ACM, 2019. doi: `10.1145/3340301.3341123`. [Online]. Available: `https://doi.org/10.1145%2F3340301.3341123`.

[17] M. Kosek, T. Shreedhar, and V. Bajpai, “Beyond QUIC v1: A First Look at Recent Transport Layer IETF Standardization Efforts”, *IEEE Communications Magazine*, vol. 59, no. 4, pp. 24–29, 2021. doi: `10.1109/MCOM.001.2000877`.

[18] M. Trevisan, D. Giordano, I. Drago, and A. S. Khatouni, “Measuring HTTP/3: Adoption and Performance”, in *2021 19th Mediterranean Communication and Computer Networking Conference (MedComNet)*, 2021, pp. 1–8. doi: `10.1109/MedComNet52149.2021.9501274`.

[19] Quicwg, *QUIC Versions · quicwg/base-drafts Wiki*, Accessed: 2021-12-09. [Online]. Available: `https://github.com/quicwg/base-drafts/wiki/QUIC-Versions`.

[20] M. Thomson and S. Turner, *Using TLS to Secure QUIC*, RFC 9001, May 2021. DOI: 10.17487/RFC9001. [Online]. Available: https://www.rfc-editor.org/info/rfc9001.

[21] M. Duke, “QUIC Version 2”, Internet Engineering Task Force, Internet-Draft draft-ietf-quic-v2-01, Jan. 2022, Work in Progress, 15 pp. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-quic-v2-01.