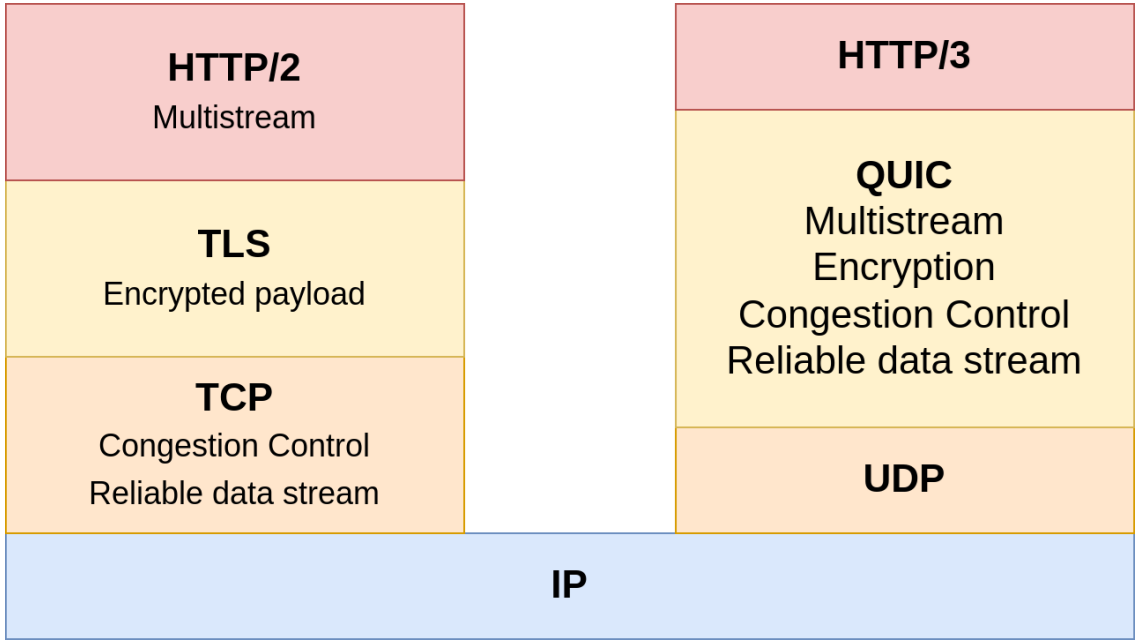
Jonas Mücke, Marcin Nawrocki, Raphael Hiesgen, Patrick Sattler, Johannes Zirngibl,
Georg Carle, Jan Luxemburk, Thomas C. Schmidt, Matthias Wählisch

Waiting for QUIC: Passive Measurements to Understand QUIC Deployments

ACM CoNEXT, Hong Kong // December 1-4, 2025

What is QUIC?

- A transport protocol standardized in May 2021 providing built-in encryption
- UDP based but implements reliability and congestion control
- QUIC connection can be maintained even when the source address changes because packets are linked to connections using connection IDs (CIDs)
- **Hides metadata from on-path observers**

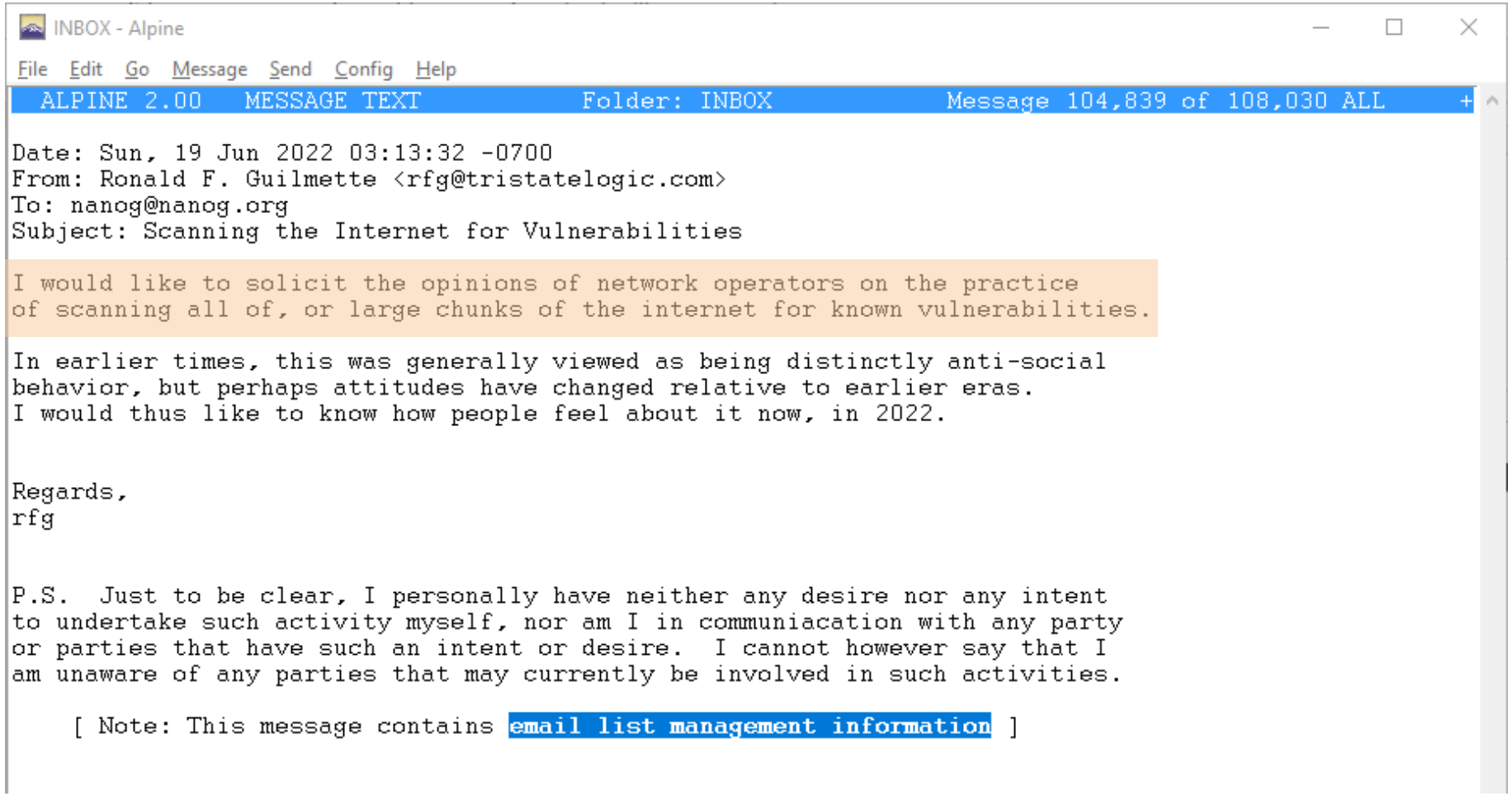


Given metadata-hiding and encryption

Are passive measurements still a viable method?

What can we learn about deployments?

Operators have strong feelings about active scanning



Operators have strong feelings about active scanning

INBOX - Alpine

File Edit Go Message Send Config Help

ALPINE 2.00 MESSAGE TEXT Folder: INBOX Message

Date: Sun, 19 Jun 2022 03:13:32 -0700
From: Ronald F. Guilmette <rfg@tristatelogic.com>
To: nanog@nanog.org
Subject: Scanning the Internet for Vulnerabilities

I would like to solicit the opinions of network operators on the practic
of scanning all of, or large chunks of the internet for known vulnerabil

In earlier times, this was generally viewed as being distinctly anti-soc
behavior, but perhaps attitudes have changed relative to earlier eras.
I would thus like to know how people feel about it now, in 2022.

Regards,
rfg

P.S. Just to be clear, I personally have neither any desire nor any int
to undertake such activity myself, nor am I in communiacation with any p
or parties that have such an intent or desire. I cannot however say tha
am unaware of any parties that may currently be involved in such activit

[Note: This message contains **email list management information**]

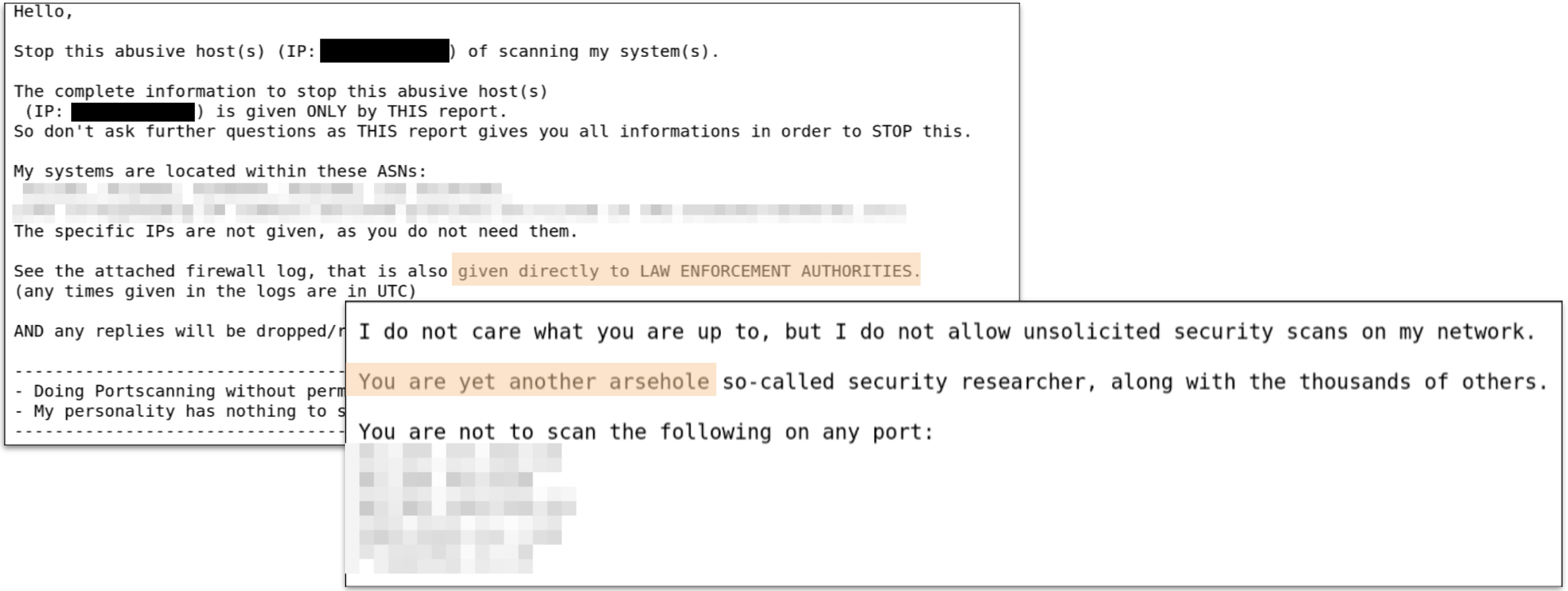
BIN - Alpine

File Edit Go Message Send Config Help

ALPINE 2.00 ZOOMED MESSAGE INDEX <mail@fu> BIN Msg 33,303 of 43,703 NEW +

```
X N 33303 Jun 19 Jorge Amodio          (11K) Re: Scanning the Internet for Vulnerabilities
X N 33304 Jun 19 Dovid Bender          (11K) Re: Scanning the Internet for Vulnerabilities
X N 33305 Jun 19 Ronald F. Guilmette   (8035) Re: Scanning the Internet for Vulnerabilities
X N 33306 Jun 19 Dovid Bender          (11K) Re: Scanning the Internet for Vulnerabilities
X N 33307 Jun 19 David Guo via NANOG   (24K) RE: Scanning the Internet for Vulnerabilities
X   33320 Jun 19 Forrest Christian (List (11K) Re: Scanning the Internet for Vulnerabilities
X N 33321 Jun 19 Forrest Christian (List (12K) Re: Scanning the Internet for Vulnerabilities
X N 33322 Jun 19 Randy Bush            (8092) Re: Scanning the Internet for Vulnerabilities
X N 33323 Jun 19 Mark Seiden           (16K) Re: Scanning the Internet for Vulnerabilities
X N 33325 Jun 19 Mark Seiden           (17K) Re: Scanning the Internet for Vulnerabilities
X N 33327 Jun 19 Amreesh Phokeer       (10K) Re: Scanning the Internet for Vulnerabilities
X N 33344 Jun 19 J. Hellenthal via NANOG (11K) Re: Scanning the Internet for Vulnerabilities
X N 33348 Jun 20 Mel Beckman           (22K) Re: Scanning the Internet for Vulnerabilities
X   33354 Jun 19 Ronald F. Guilmette   (8574) Re: Scanning the Internet for Vulnerabilities
X N 33355 Jun 19 Ronald F. Guilmette   (7872) Re: Scanning the Internet for Vulnerabilities
X N 33357 Jun 19 goemon--- via NANOG   (8205) Re: Scanning the Internet for Vulnerabilities
X N 33373 Jun 19 Owen DeLong via NANOG (9587) Re: Scanning the Internet for Vulnerabilities
X N 33374 Jun 19 Owen DeLong via NANOG (12K) Re: Scanning the Internet for Vulnerabilities
X N 33411 Jun 20 J. Hellenthal via NANOG (12K) Re: Scanning the Internet for Vulnerabilities
X N 33415 Jun 20 J. Hellenthal via NANOG (12K) Re: Scanning the Internet for Vulnerabilities
X N 33417 Jun 20 Carsten Bormann      (8786) Re: Scanning the Internet for Vulnerabilities
X N 33421 Jun 20 J. Hellenthal via NANOG (9609) Re: Scanning the Internet for Vulnerabilities
X N 33426 Jun 20 Carsten Bormann       (8537) Re: Scanning the Internet for Vulnerabilities
X   33429 Jun 20 John Kristoff        (8821) Re: Scanning the Internet for Vulnerabilities
X N 33430 Jun 20 Mel Beckman           (18K) Re: Scanning the Internet for Vulnerabilities
X N 33438 Jun 20 J. Hellenthal via NANOG (11K) Re: Scanning the Internet for Vulnerabilities
X N 33446 Jun 20 Michael Butler via NANOG (11K) Re: Scanning the Internet for Vulnerabilities
X N 33448 Jun 20 J. Hellenthal via NANOG (11K) Re: Scanning the Internet for Vulnerabilities
X   33462 Jun 20 goemon--- via NANOG   (8777) Re: Scanning the Internet for Vulnerabilities
X   33475 Jun 20 Randy Bush            (7962) Re: Scanning the Internet for Vulnerabilities
X   33477 Jun 20 Matthew Craig          (22K) Re: Scanning the Internet for Vulnerabilities
X N 33479 Jun 20 Mel Beckman           (17K) Re: Scanning the Internet for Vulnerabilities
X N 33480 Jun 20 nanog08@mulligan.org  (9462) Re: Scanning the Internet for Vulnerabilities
X N 33482 Jun 20 Carsten Bormann       (9720) Re: Scanning the Internet for Vulnerabilities
X N 33484 Jun 20 Mel Beckman           (20K) Re: Scanning the Internet for Vulnerabilities
X   33486 Jun 20 Carsten Bormann       (11K) Re: Scanning the Internet for Vulnerabilities
X   33488 Jun 20 bzs@theworld.com      (8801) Re: Scanning the Internet for Vulnerabilities
X N 33490 Jun 20 Robert L Mathews      (9954) Re: Scanning the Internet for Vulnerabilities
X   33493 Jun 20 J. Hellenthal via NANOG (9933) Re: Scanning the Internet for Vulnerabilities
X N 33496 Jun 21 Matt Palmer           (8461) Re: Scanning the Internet for Vulnerabilities
X N 33498 Jun 20 Joe Maimon            (8404) Re: Scanning the Internet for Vulnerabilities
X   33500 Jun 20 Randy Bush            (7885) Re: Scanning the Internet for Vulnerabilities
X   33501 Jun 20 Randy Bush            (7771) Re: Scanning the Internet for Vulnerabilities
X N 33532 Jun 21 Fernando Gont         (9446) Re: Scanning the Internet for Vulnerabilities
X   33538 Jun 20 Ronald F. Guilmette   (8179) Re: Scanning the Internet for Vulnerabilities
X N 33548 Jun 21 Fernando Gont         (10K) Re: Scanning the Internet for Vulnerabilities
X N 33552 Jun 21 Ronald F. Guilmette   (8348) Re: Scanning the Internet for Vulnerabilities
X N 33587 Jun 21 Daniel Seagraves      (8618) Re: Scanning the Internet for Vulnerabilities
X N 33685 Jun 21 bzs@theworld.com      (9725) Re: Scanning the Internet for Vulnerabilities
X N 33686 Jun 22 bzs@theworld.com      (9419) Re: Scanning the Internet for Vulnerabilities
X N 33755 Jun 22 John Curran           (20K) Re: Scanning the Internet for Vulnerabilities
X   33812 Jun 22 Fernando Gont         (11K) Re: Scanning the Internet for Vulnerabilities
X N 33813 Jun 22 bzs@theworld.com      (14K) Re: Scanning the Internet for Vulnerabilities
X N 33816 Jun 22 John Curran           (31K) Re: Scanning the Internet for Vulnerabilities
X N 38134 Jul 23 Abraham Y. Chen       (14K) Re: Scanning the Internet for Vulnerabilities Re:
X   38167 Jul 24 John Curran           (34K) Re: Scanning the Internet for Vulnerabilities Re:
                                  [First Index Page]
? Help      < FldrList   P PrevMsg   - PrevPage   D Delete   R Reply
O OTHER CMDS > [ViewMsg] N NextMsg  Spc NextPage  U Undelete F Forward
```

… and may send love letters when scanned



```
Hello,

Stop this abusive host(s) (IP: [redacted]) of scanning my system(s).

The complete information to stop this abusive host(s)
 (IP: [redacted]) is given ONLY by THIS report.
So don't ask further questions as THIS report gives you all informations in order to STOP this.

My systems are located within these ASNs:
[redacted]

The specific IPs are not given, as you do not need them.

See the attached firewall log, that is also given directly to LAW ENFORCEMENT AUTHORITIES.
(any times given in the logs are in UTC)

AND any replies will be dropped/r

---------------------------------
- Doing Portscanning without perm
- My personality has nothing to s
---------------------------------
```

```
I do not care what you are up to, but I do not allow unsolicited security scans on my network.

You are yet another arsehole so-called security researcher, along with the thousands of others.

You are not to scan the following on any port:
[redacted]
```

Our approach

Analyze QUIC traffic at a network telescope

Our approach

Analyze QUIC traffic at a network telescope

Why QUIC?
Broad adoption.
(2025, 89% of Meta egress traffic is QUIC.)

Exposes additional information
(compared to UDP and TCP).

Our approach

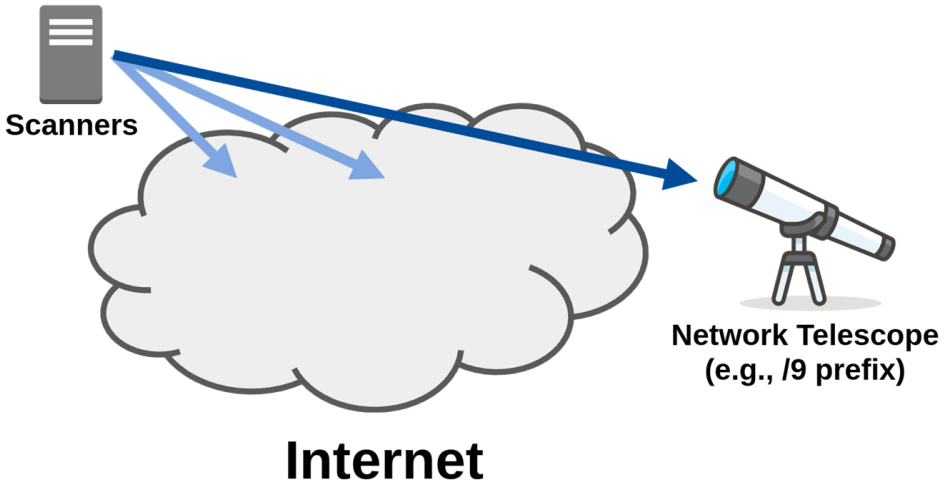
Why network telescope traffic?
Passive, non-intrusive.
Relatively easy to capture.

Analyze QUIC traffic at a network telescope

Why QUIC?
Broad adoption.
(2025, 89% of Meta egress traffic is QUIC).

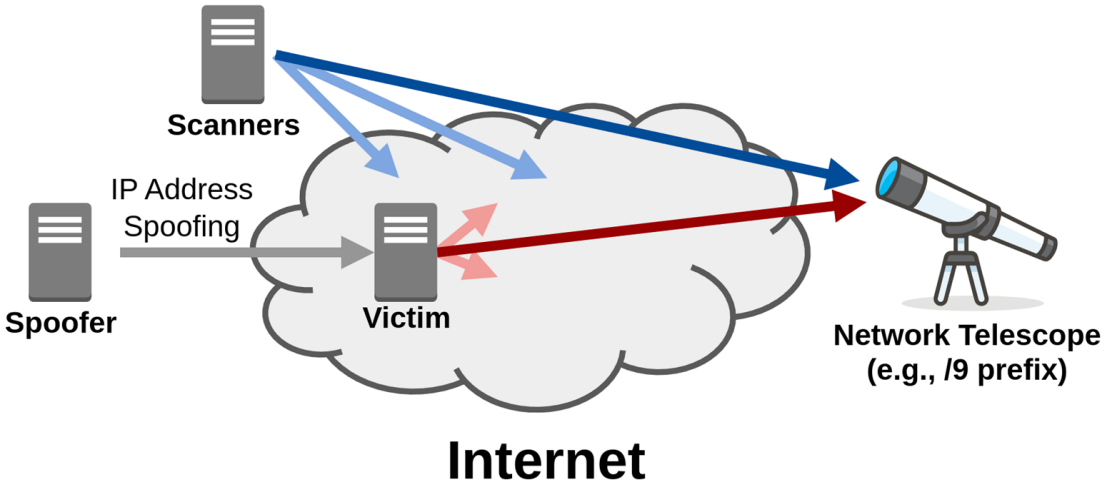
Exposes additional information
(compared to UDP and TCP).

Network telescopes capture scanner traffic



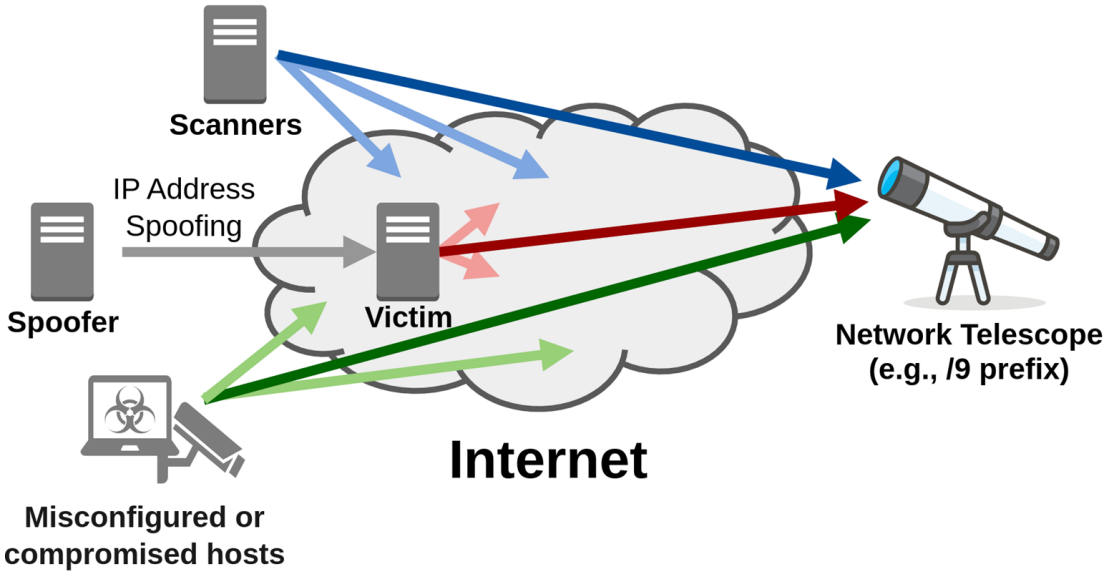
Network telescopes capture unsolicited traffic to a silent prefix.

Network telescopes capture backscatter to spoofed Initials



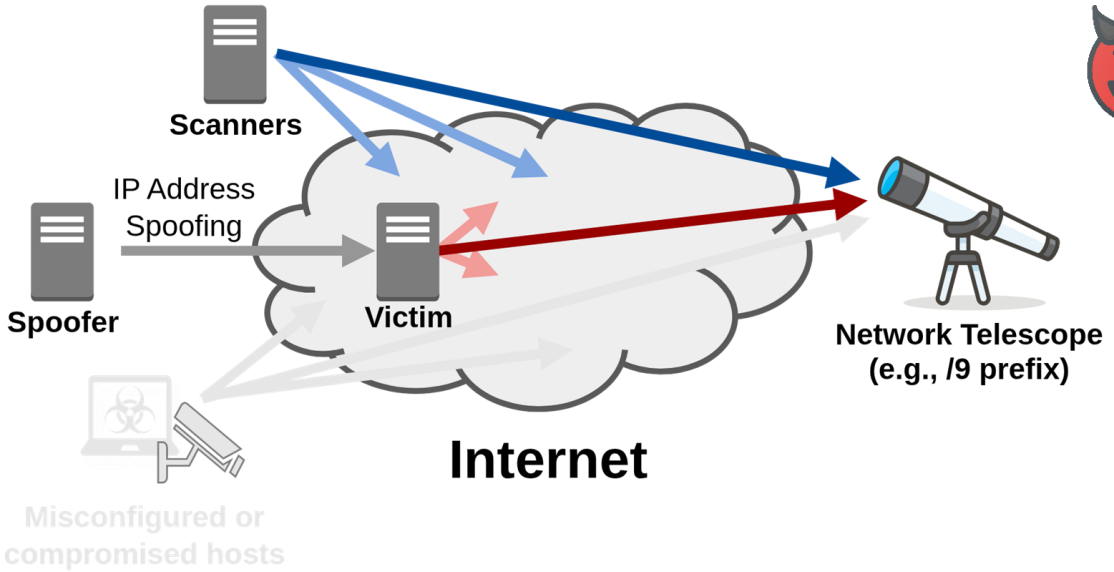
Network telescopes capture unsolicited traffic to a silent prefix.

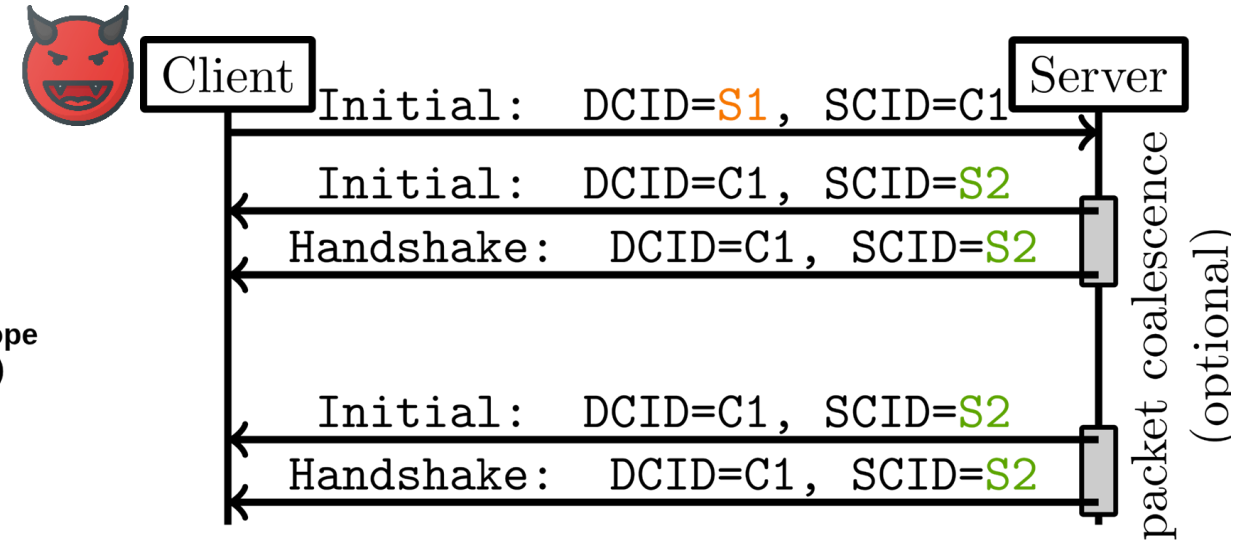
Network telescopes capture traffic from misconfigured hosts



Network telescopes capture unsolicited traffic to a silent prefix.

Network telescopes capture backscatter to spoofed Initials



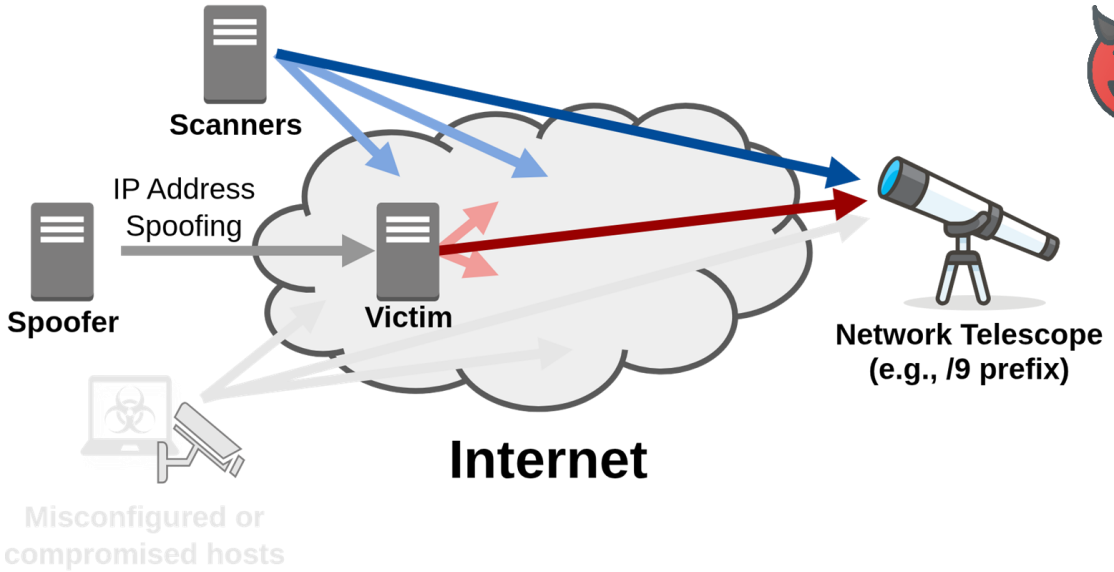


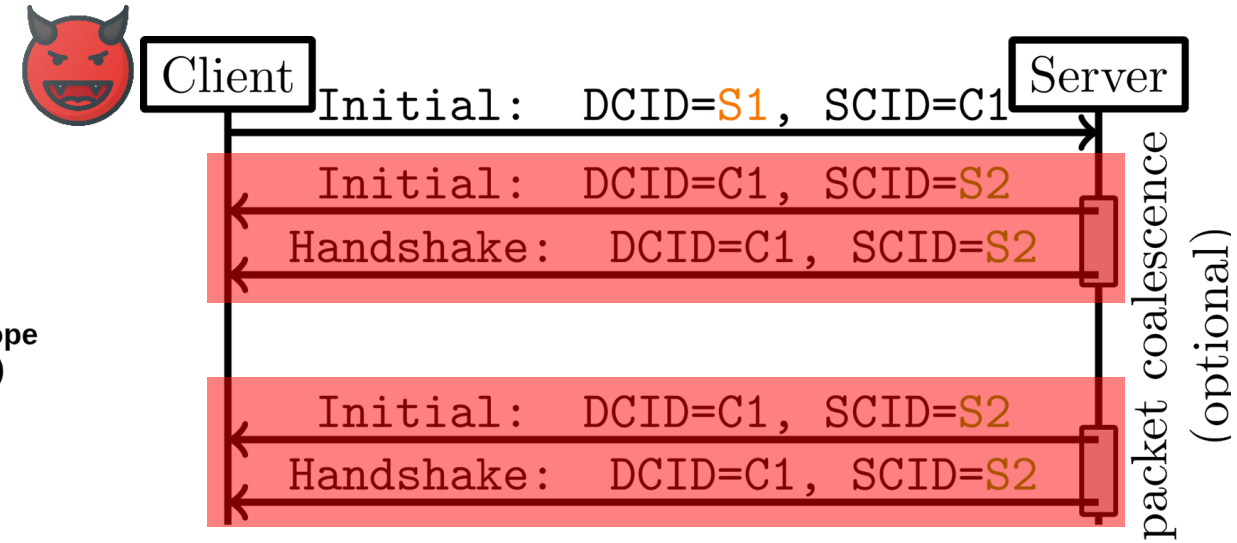
Network telescopes capture unsolicited traffic to a silent prefix.

QUIC backscatter consists of Initial, Handshake and 1-RTT packets.

Whenever servers retransmit those messages, we gain timing information.

Network telescopes capture backscatter to spoofed Initials





Network telescopes capture unsolicited traffic to a silent prefix.

QUIC backscatter consists of Initial, Handshake and 1-RTT packets.

Whenever servers retransmit those messages, we gain timing information.

Measurement method and setup

Primary datasource

/9 + /10 UCSD
Network Telescope

We identify ...

... servers of large content providers

... configuration of QUIC servers

... off-net servers

... L7 loadbalancers/frontend clusters

1 month per year 2021-2025

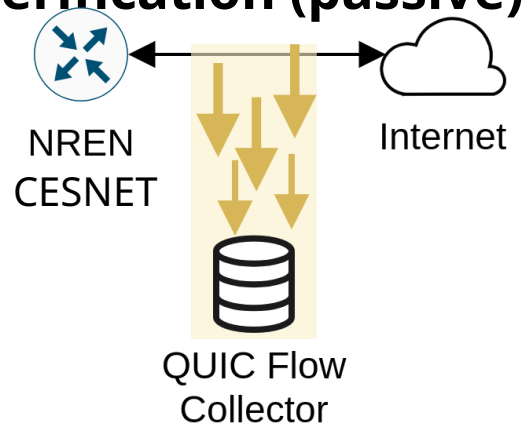
1.7B QUIC packets

Measurement method and setup

Primary datasource

/9 + /10 UCSD
Network Telescope

Verification (passive)



- ➔ **QUIC version**
- ➔ **Initial RTO**
- ➔ **# Retransmissions**
- ➔ **Structured CIDs**
- ➔ **L7 loadbalancers**

- ➔ **Verification of telescope observations**

1 month per year 2021-2025	1 month per year 2024-2025
1.7B QUIC packets	**24M QUIC Flows**

Measurement method and setup

Primary datasource

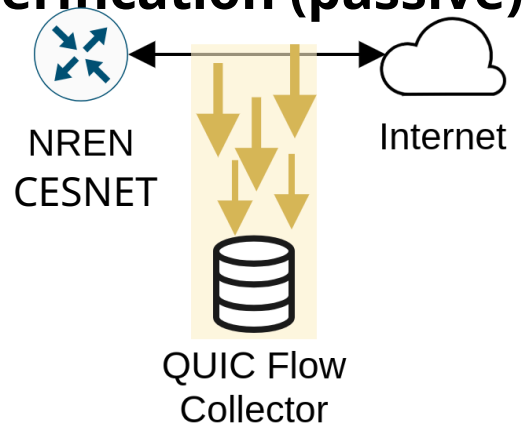
/9 + /10 UCSD
Network Telescope

- → **QUIC version**
- → **Initial RTO**
- → **# Retransmissions**
- → **Structured CIDs**
- → **L7 loadbalancers**

1 month per year 2021-2025

1.7B QUIC packets

Verification (passive)

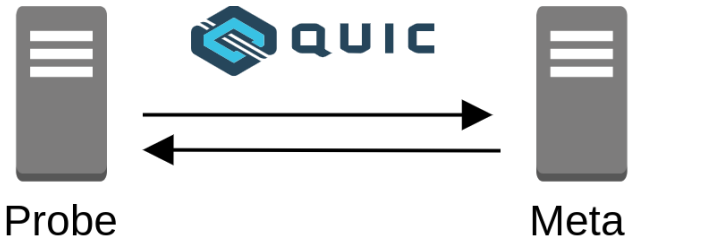


- → **Verification of telescope observations**

1 month per year 2024-2025

24M QUIC Flows

Verification (active)



- → **Verification of telescope observations**
- → **Extension of sparse data from the network telescope**

2022-2025

20,000 connections/VIP

Measurement method and setup

Primary datasource

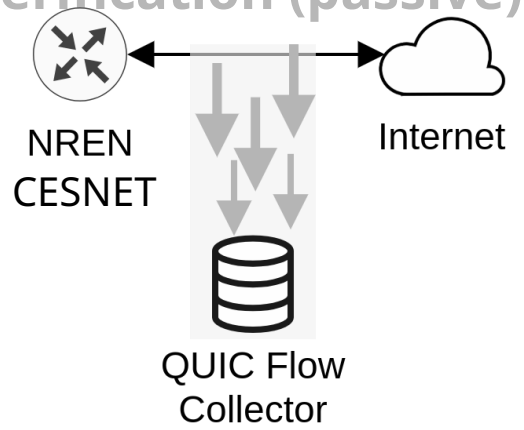
/9 + /10 UCSD
Network Telescope

- ➔ **QUIC version**
- ➔ **Initial RTO**
- ➔ **# Retransmissions**
- ➔ **Structured CIDs**
- ➔ **L7 loadbalancers**

1 month per year 2021-2025

1.7B QUIC packets

Verification (passive)

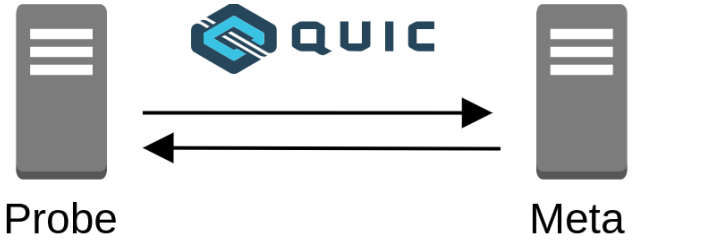


- ➔ **Verification of telescope observations**

1 month per year 2024-2025

24M QUIC Flows

Verification (active)

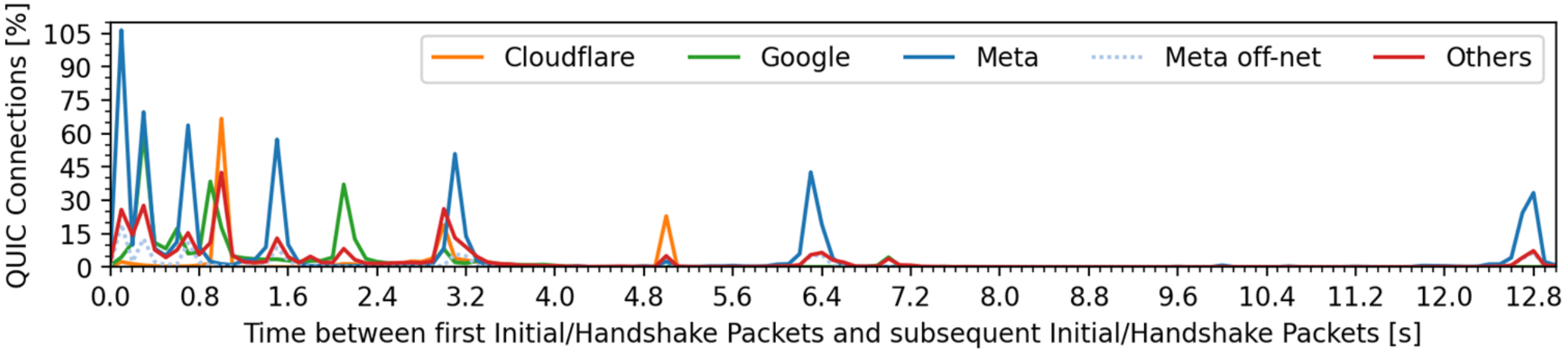


- ➔ **Verification of telescope observations**
- ➔ **Extension of sparse data from the network telescope**

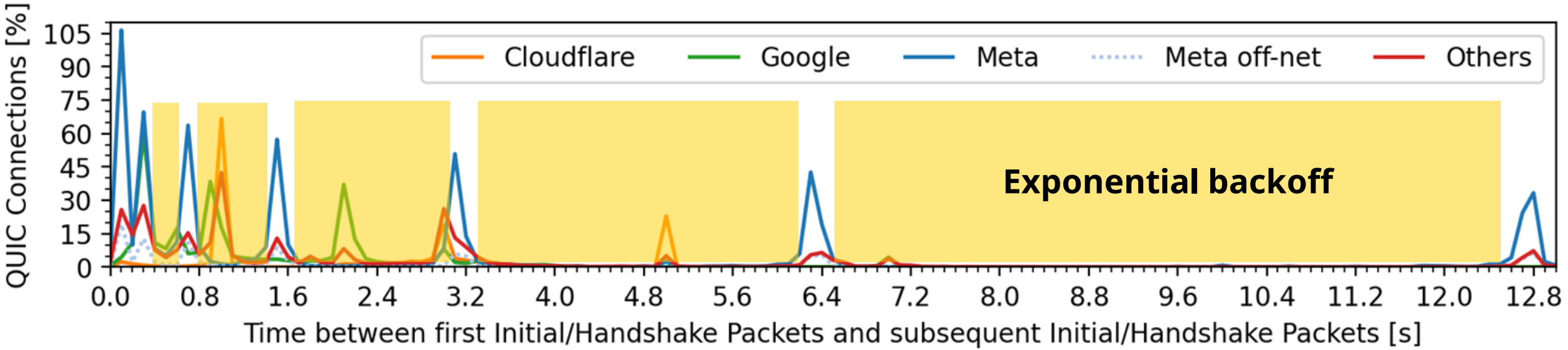
2022-2025

20,000 connections/VIP

Retransmission configurations of QUIC servers

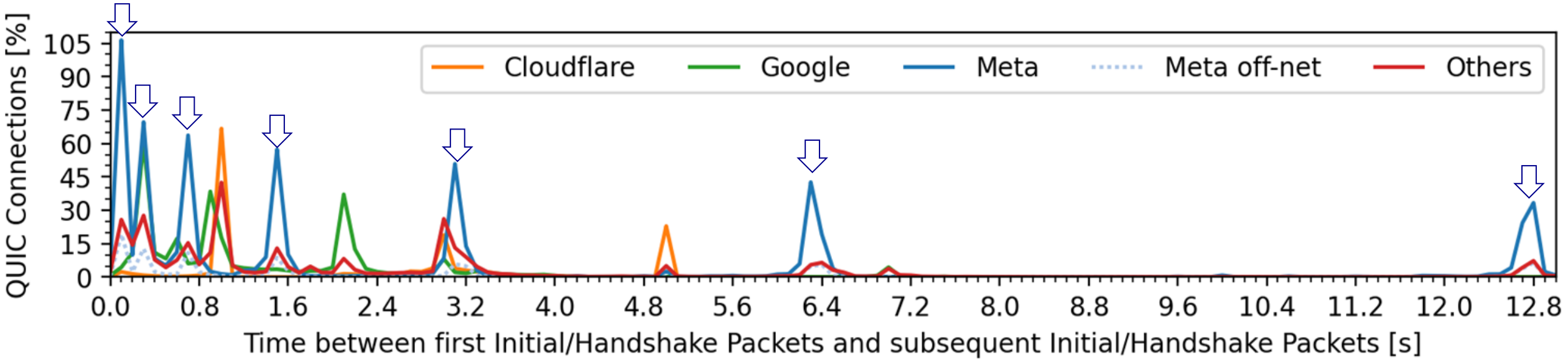


Retransmission configurations of QUIC servers



➔ **Large content providers use exponential backoff**

Retransmission configurations of QUIC servers



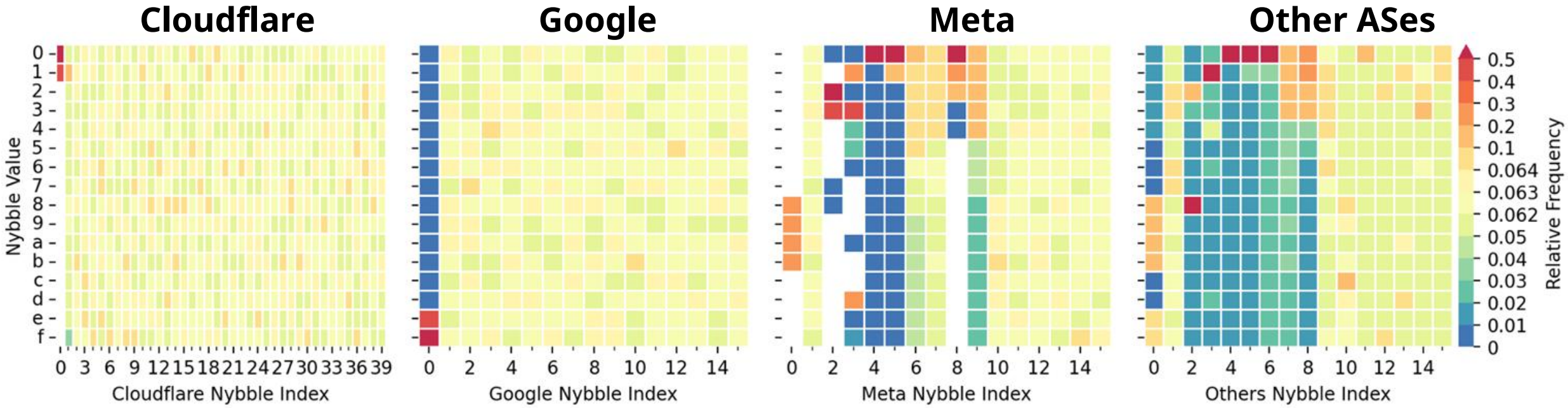
- ➔ **Large content providers use exponential backoff**
- ➔ **Initial RTOs between 0.1s and 1s.**
- ➔ **# Retransmissions between 2-8**
- ➔ **Details depend on the content provider**

QUIC Connection IDs (CIDs)

(half Byte, Nybble)

max. length 20 bytes

Structure of Server Connection IDs



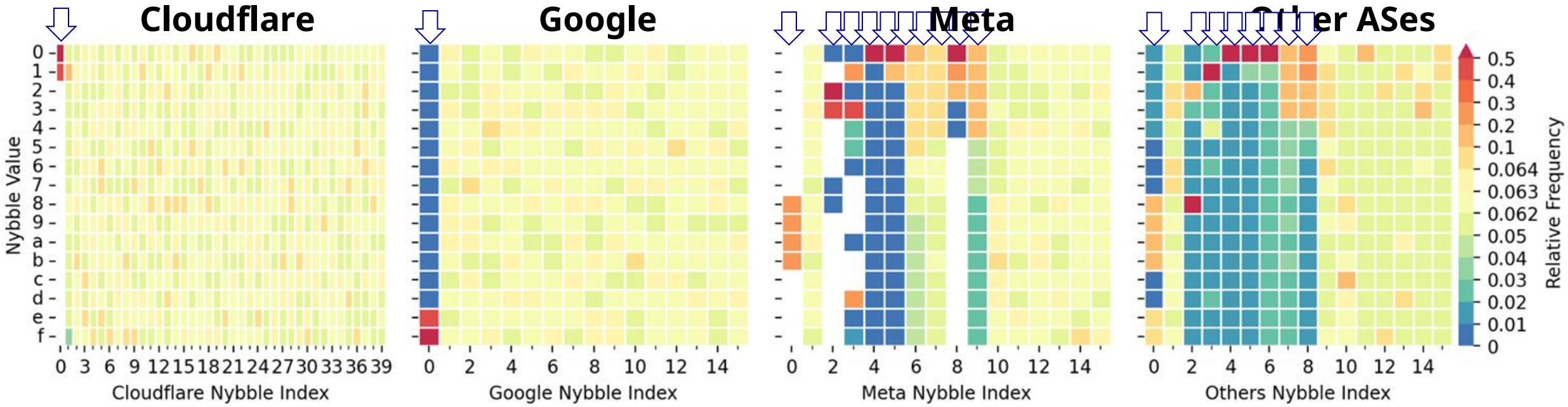
(half Byte, Nybble)

0
⋮
f

XXXXXX…XXXXXX

max. length 20 bytes

Structure of Server Connection IDs



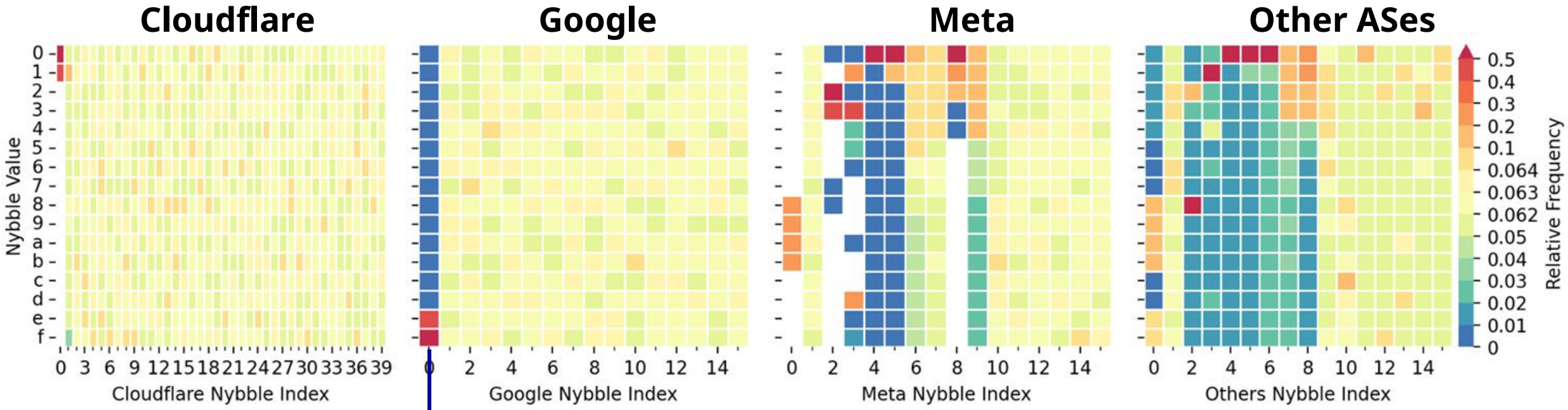
(half Byte, Nybble)

0
⋮
f

XXXXXX…XXXXXX

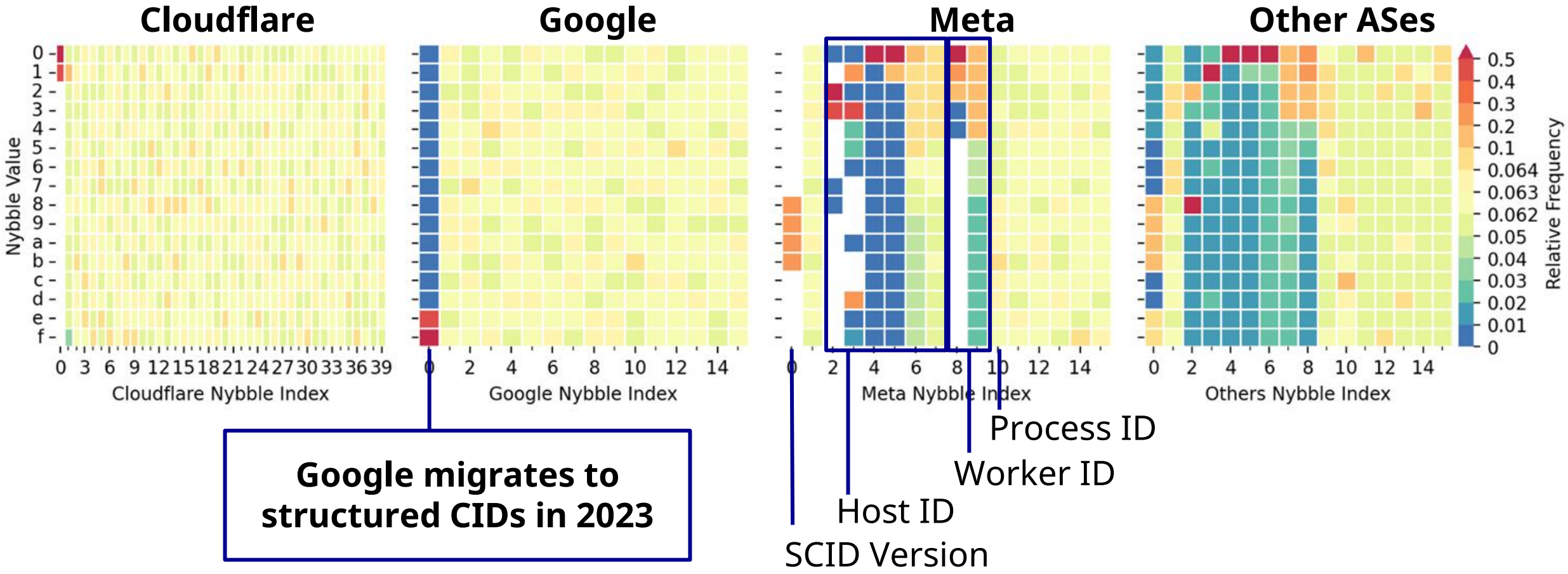
max. length 20 bytes

Structure of Server Connection IDs

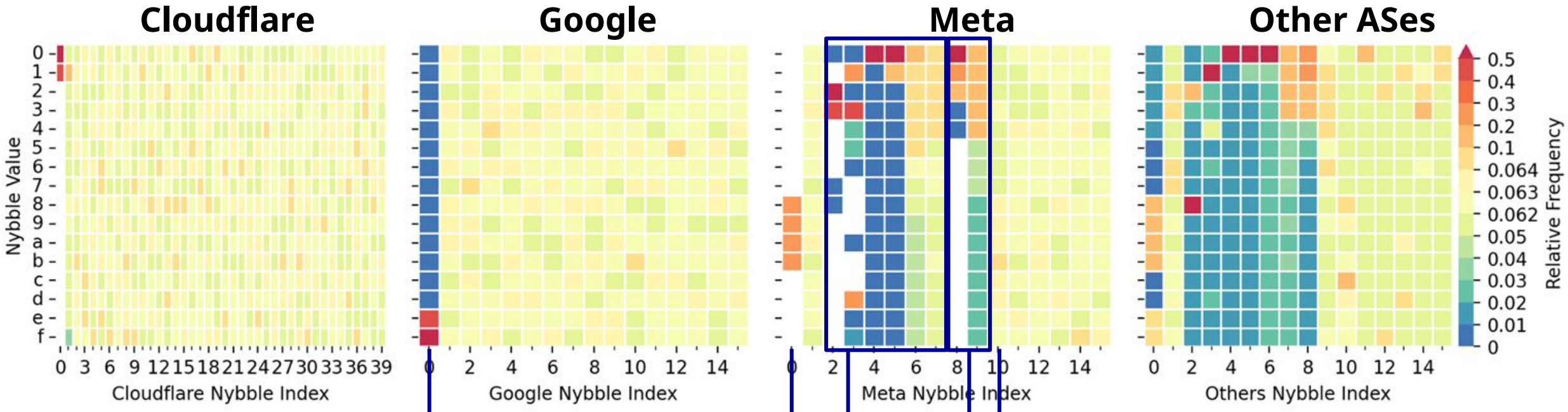


Google migrates to structured CIDs in 2023

Structure of Server Connection IDs



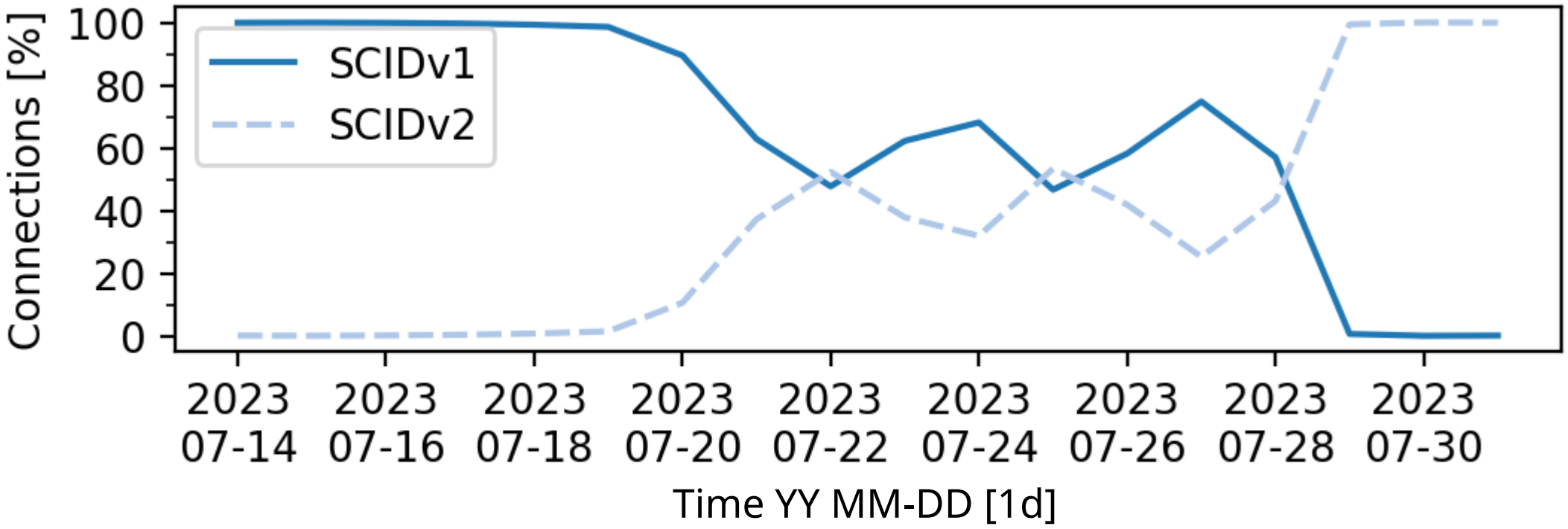
Structure of Server Connection IDs



Google migrates to structured CIDs in 2023

Documented in Meta's QUIC Implementation: SCIDv1, SCIDv2, SCIDv3

Migration to a new load balancer configuration



→ **We observe the migration process of Meta from SCIDv1 to SCIDv2 entirely passively**

Detecting off-net servers

Fingerprint on-net deployments:

- Typical packet lengths
- Packet coalescence
- Retransmission intervals
- SCID structure

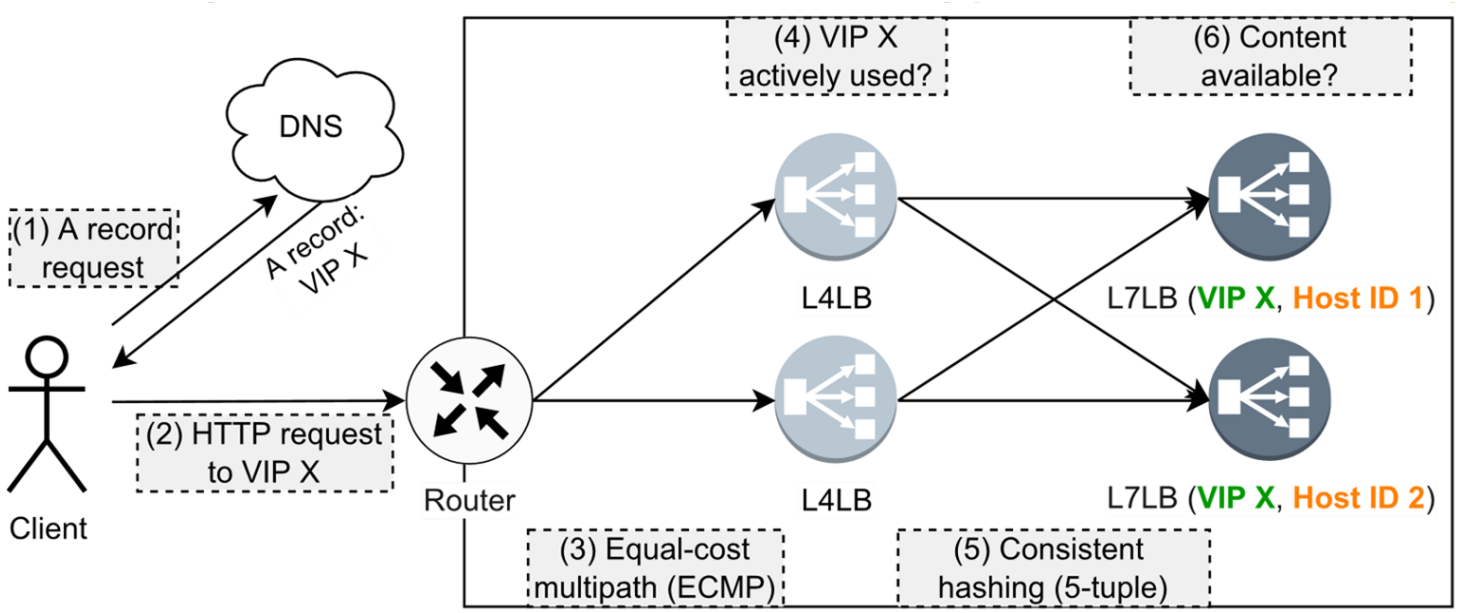
SCID structure has the best F_1 score to detect off-net deployments.

Other properties also have high TPR, but an increased FPR.

Classifier	F_1-score 2022	2023	2024	2025
Meta Off-net SCIDv1	0.98	0.98	-	-
Meta Off-net SCIDv2	-	-	0.98	0.99
Google SCIDv1	0.17	0.89	0.79	0.77
Google SCIDv2	0.12	0.38	0.8	0.78

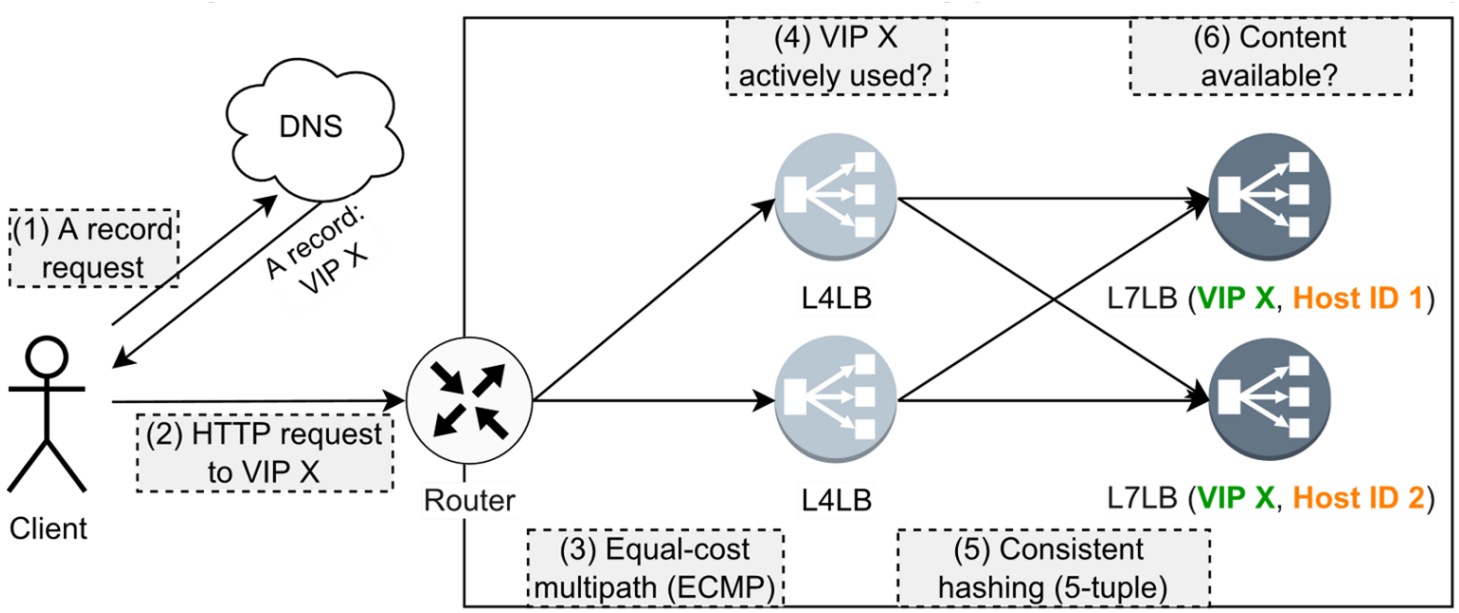
Verified by SANs in TLS certificates

Hypergiant frontend cluster deployment

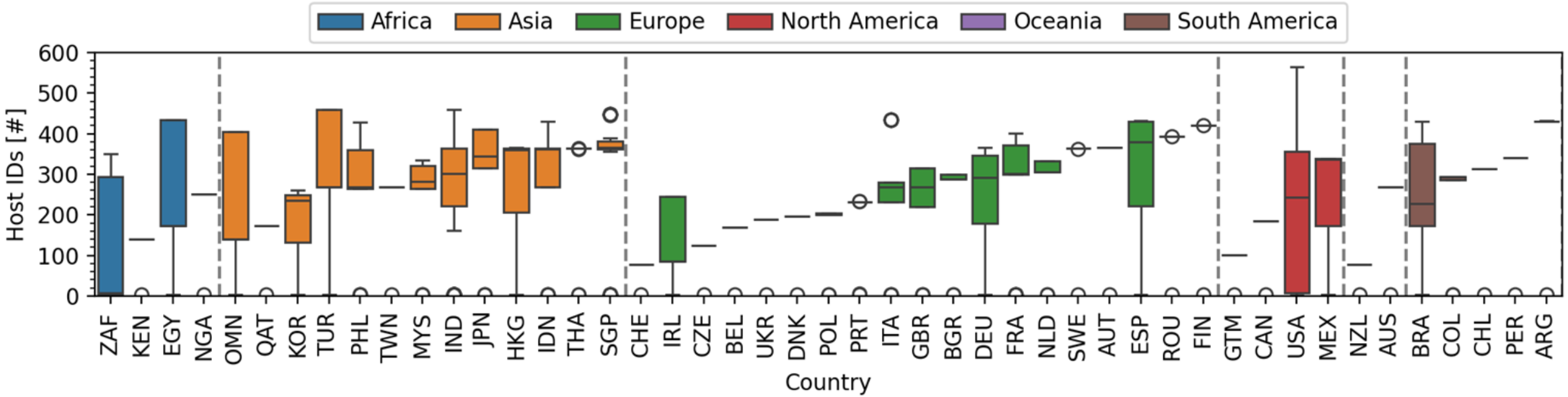


How to collect all unique host IDs of a VIP

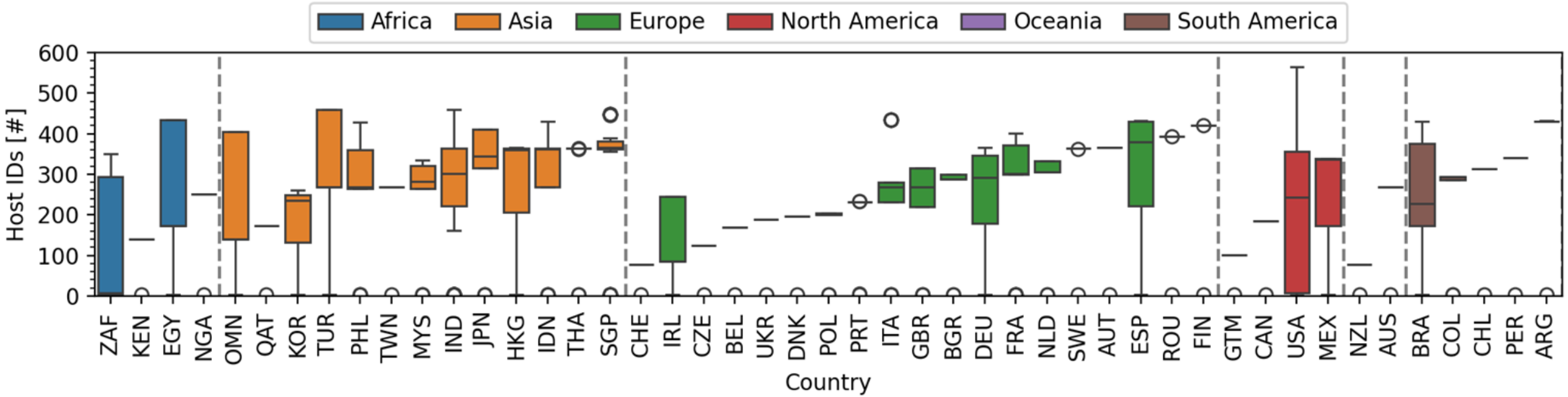
- ➔ We probe Meta servers to determine the number of Host IDs (#L7LBs).
- ➔ We connect 20,000 times to each Meta IPv4 address.
- ➔ We group the host IDs into frontend clusters.



Meta cluster sizes per country

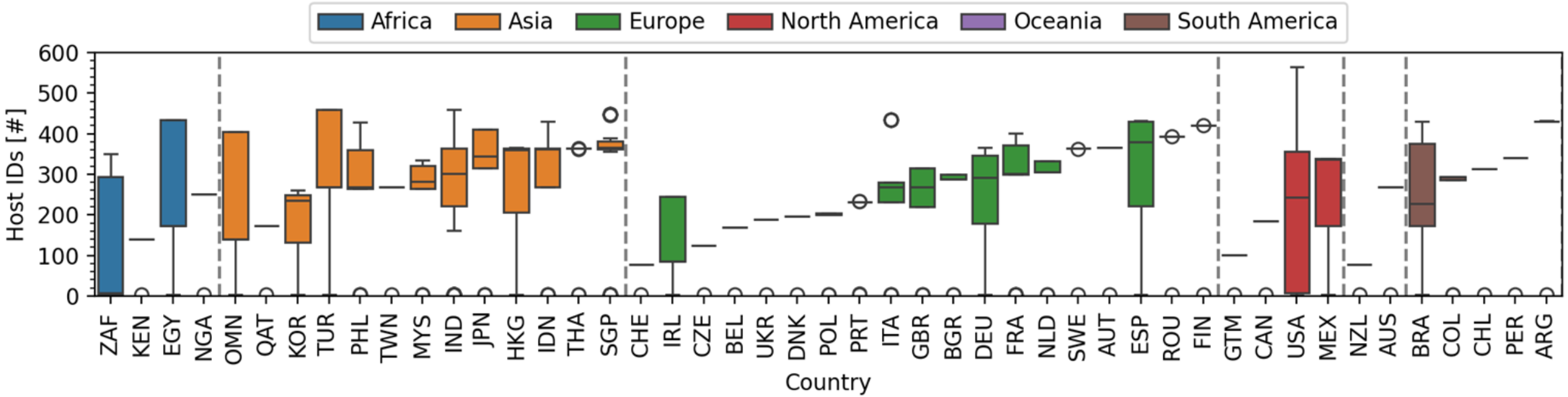


Meta cluster sizes per country



→ **Median cluster size in Asia is larger than on any other continent**

Meta cluster sizes per country



➔ Median cluster size in Asia is larger than on any other continent

➔ 29% of all host IDs in 2023 are contained in the telescope backscatter

Conclusion

Network telescopes can provide details of large content provider deployments, even facing metadata-hiding protocols such as QUIC.

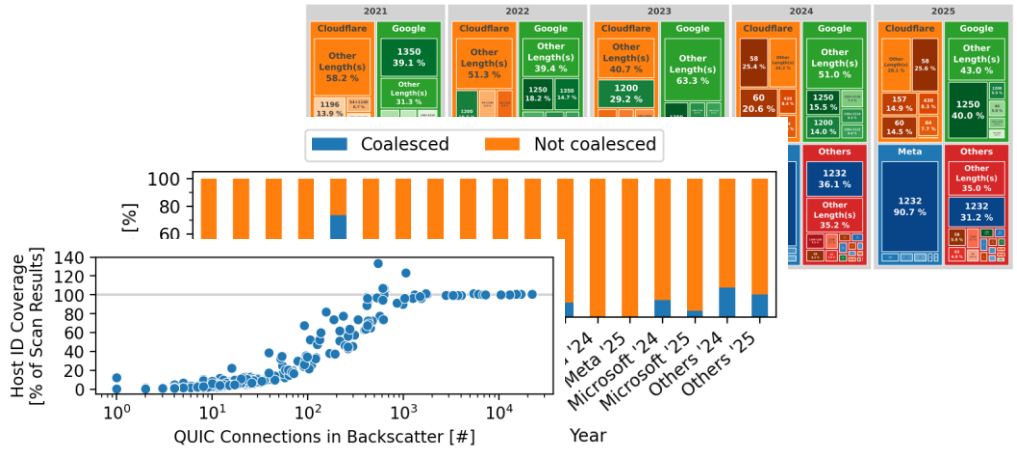
Fingerprinting on-net deployments allows inference of off-net deployments at high accuracy

		Hypergiant							
		Akamai	Amazon	Apple	Cloudflare	Fastly	Google	Meta	Microsoft
First backscatter visible		2023	2022	2022	2021	2023	2021	2021	2022
Features	Coalescence	✓	✓	✓	✓	✓	✓	✘	✓
	Structured SCIDs	✓	✓	✓	✓	✓	✓	✓	✓
	Retry observed	✘	✘	✘	✓	✘	✘	✘	✓
	L7 load balancers	n/a	n/a	n/a	n/a	n/a	n/a	✓	n/a
	SCID length	20 B	20 B	20 B	20 B	17 B	8 B	8 B	14/20 B
	Initial RTO	1 s	0.3 s	1 s	1 s	0.2 s	0.3 s	0.1 s	1 s
	Mean # retransmissions	2.1	4.0	2.7	1.5	6.0	3.4	7.5	1.3

More results in our paper,
e.g., denial of service mitigations

Waiting for QUIC: Passive Measurements to Understand QUIC Deployments

JONAS MÜCKE, TU Dresden, Germany
MARCIN NAWROCKI, NETSCOUT, USA
RAPHAEL HIESGEN, HAW Hamburg, Germany
PATRICK SATTLER, Technical University of Munich, Germany
JOHANNES ZIRNGIBL, Max Planck Institute for Informatics, Germany
GEORG CARLE, Technical University of Munich, Germany
JAN LUXEMBURK, FIT CTU & CESNET, Czech Republic
THOMAS C. SCHMIDT, HAW Hamburg, Germany
MATTHIAS WÄHLISCH, TU Dresden, Germany



Conclusion

Network telescopes can provide details of large content provider deployments, even facing metadata-hiding protocols such as QUIC.

Fingerprinting on-net deployments allows inference of off-net deployments at high accuracy

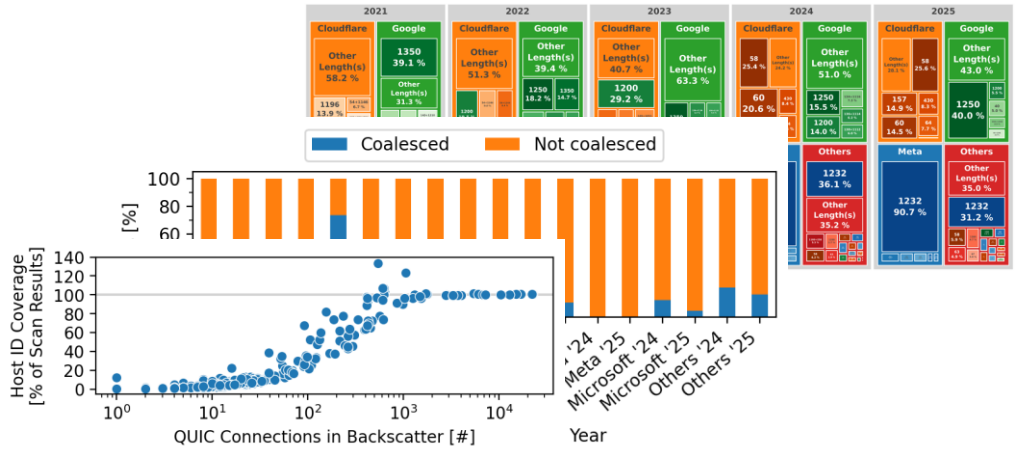
		Hypergiant							
		Akamai	Amazon	Apple	Cloudflare	Fastly	Google	Meta	Microsoft
First backscatter visible		2023	2022	2022	2021	2023	2021	2021	2022
Features	Coalescence	✓	✓	✓	✓	✓	✓	✘	✓
	Structured SCIDs	✓	✓	✓	✓	✓	✓	✓	✓
	Retry observed	✘	✘	✘	✓	✘	✘	✘	✓
	L7 load balancers	n/a	n/a	n/a	n/a	n/a	n/a	✓	n/a
	SCID length	20 B	20 B	20 B	20 B	17 B	8 B	8 B	14/20 B
	Initial RTO	1 s	0.3 s	1 s	1 s	0.2 s	0.3 s	0.1 s	1 s
	Mean # retransmissions	2.1	4.0	2.7	1.5	6.0	3.4	7.5	1.3

zenodo **1 year of detailed QUIC flow data**
doi.org/10.5281/zenodo.17249078

More results in our paper,
e.g., denial of service mitigations

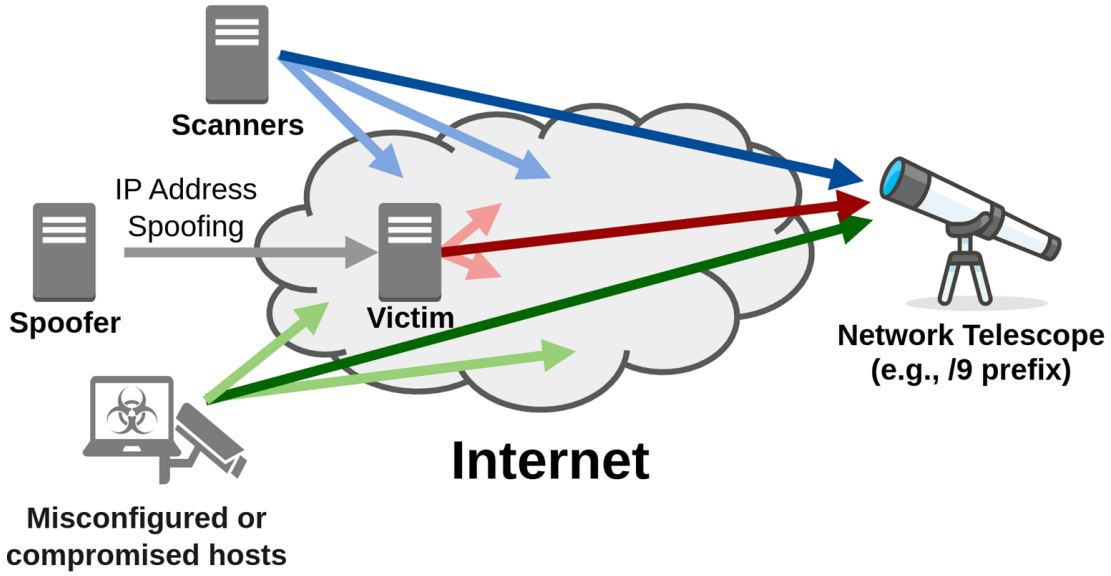
Waiting for QUIC: Passive Measurements to Understand QUIC Deployments

JONAS MÜCKE, TU Dresden, Germany
MARCIN NAWROCKI, NETSCOUT, USA
RAPHAEL HIESGEN, HAW Hamburg, Germany
PATRICK SATTLER, Technical University of Munich, Germany
JOHANNES ZIRNGIBL, Max Planck Institute for Informatics, Germany
GEORG CARLE, Technical University of Munich, Germany
JAN LUXEMBURK, FIT CTU & CESNET, Czech Republic
THOMAS C. SCHMIDT, HAW Hamburg, Germany
MATTHIAS WÄHLISCH, TU Dresden, Germany



Backup

Limitations



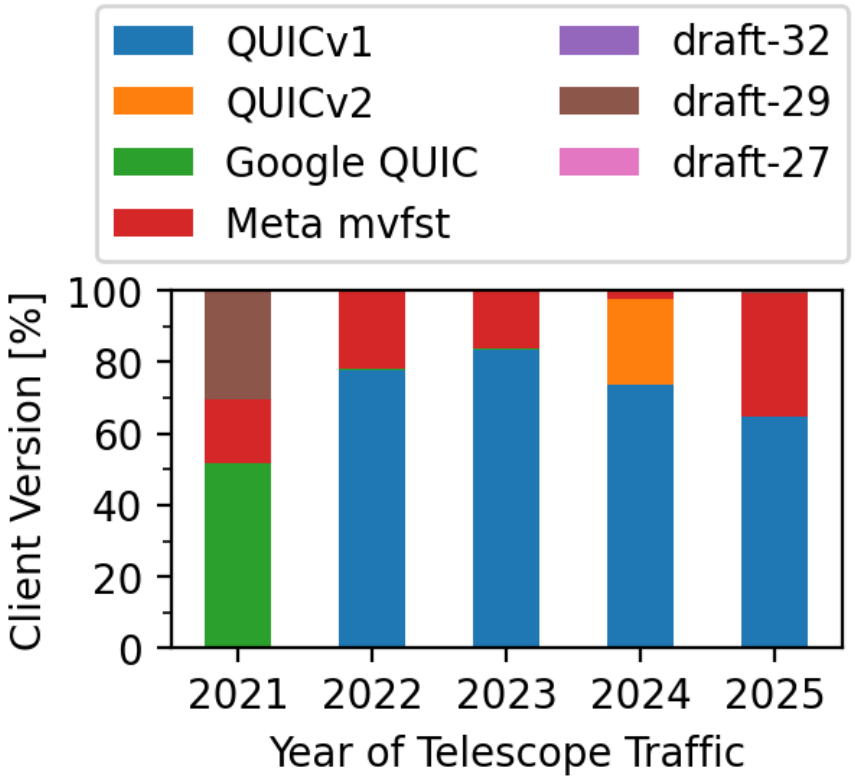
- ➔ **Our method depends on QUIC traffic from scanners and attackers.** TCP backscatter is visible for more than 25 years. We expect similar behavior.
- ➔ **Backscatter depends on attack target behavior**, e.g., attack mitigations, filters, ...
- ➔ **We analyze flow records from the past 2 years** due to recent implementation.
- ➔ **Only information from QUIC packets at the beginning of a connection can be decoded**, later packets are encrypted.

VIPs from source network in backscatter

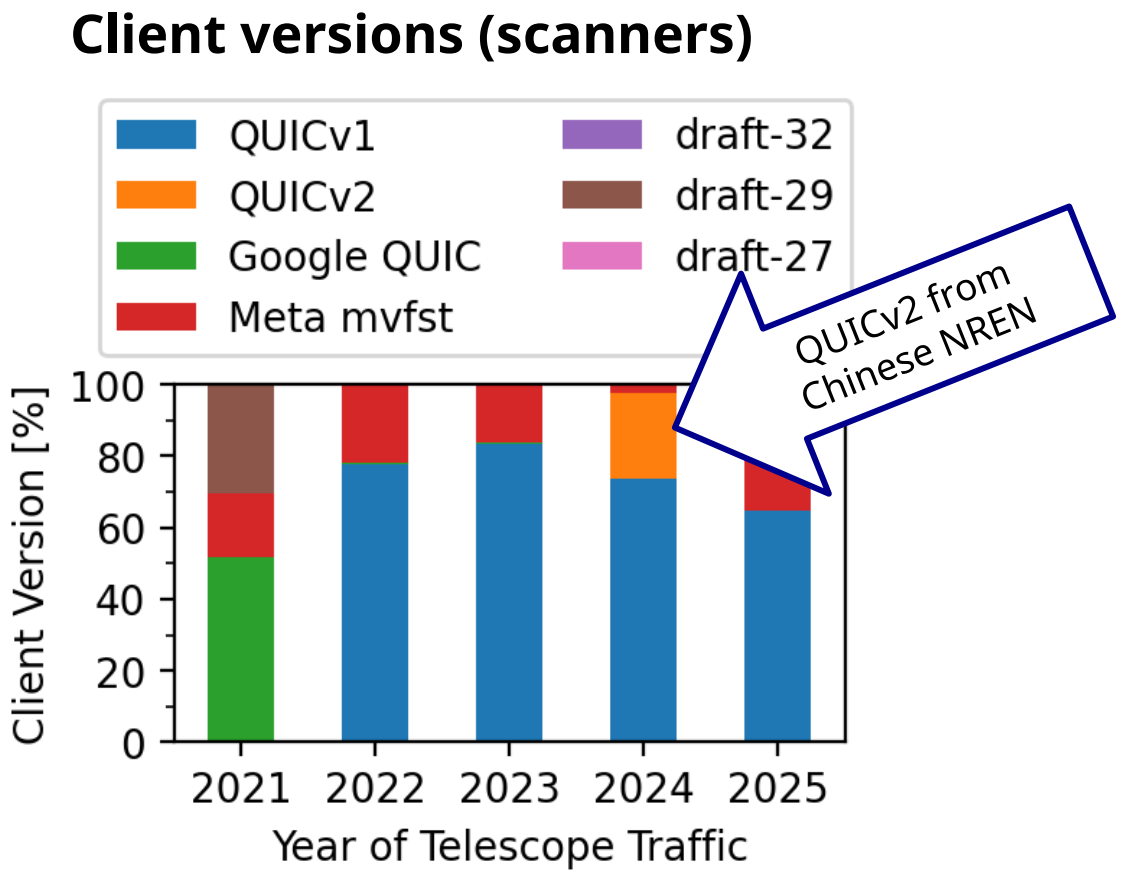
	Most Backscatter Observations				Subsequently subsumed as *Others*					
	VIPs from Source Network [#]			L7LBs [#]	VIPs from Source Network [#]					
Year	Cloudflare	Google	Meta	Meta	Akamai	Amazon	Apple	Fastly	Microsoft	Others
2021	33	1,790	167	4,273	-	1	-	-	-	604
2022	78	1,655	246	7,145	11	2	2	-	14	677
2023	359	2,769	350	12,048	258	115	33	19	51	1,623
2024	151	1,681	514	20,744	431	40	335	20	41	1,112
2025	250	2,042	637	22,527	396	124	331	51	61	1,290

Clients migrate to QUICv1 in 2022

Client versions (scanners)

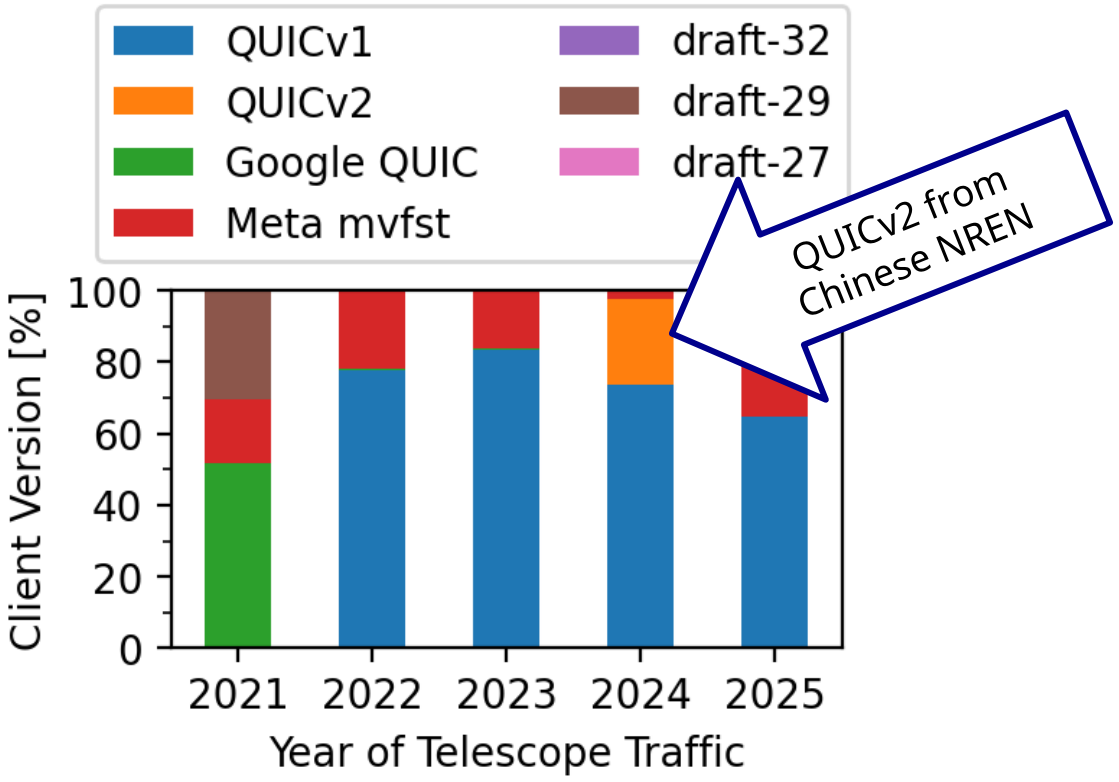


Clients migrate to QUICv1 in 2022

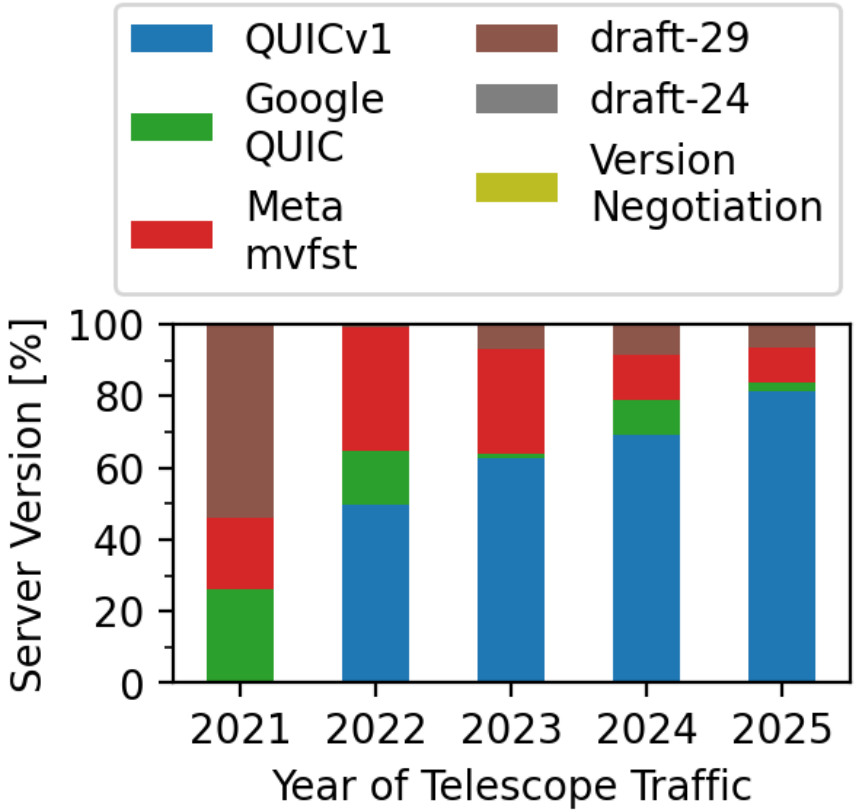


Clients and servers migrate to QUICv1 in 2022

Client versions (scanners)

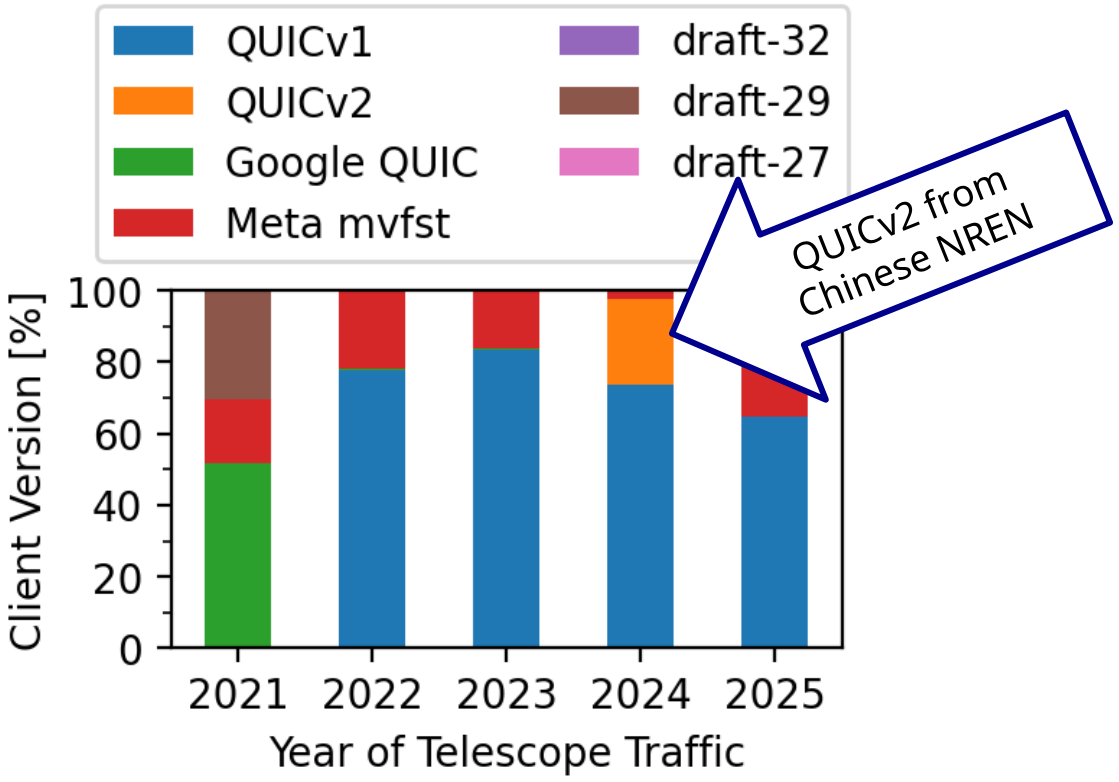


Server versions (Backscatter)

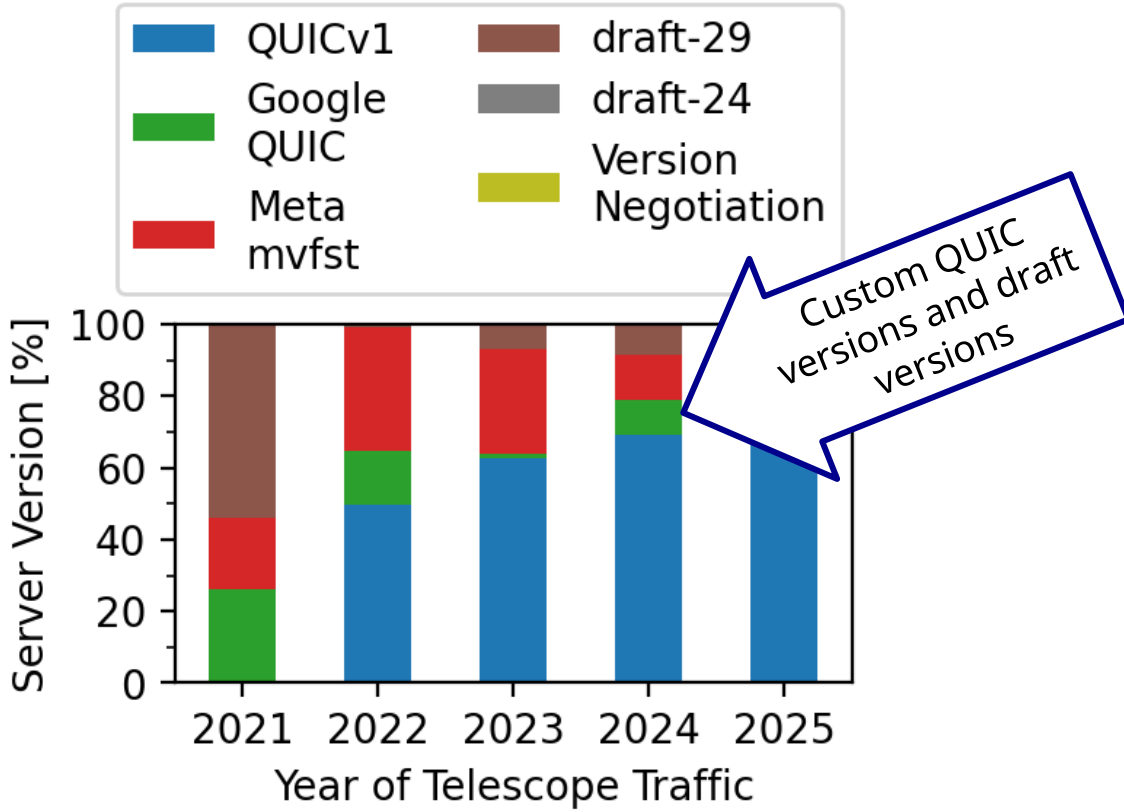


Clients and servers migrate to QUICv1 in 2022

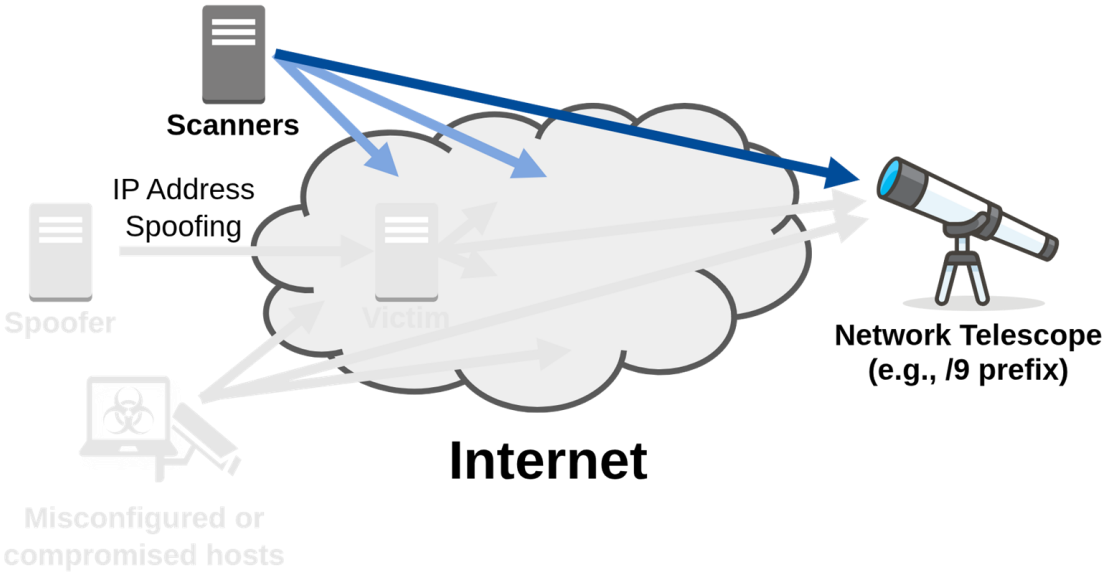
Client versions (scanners)

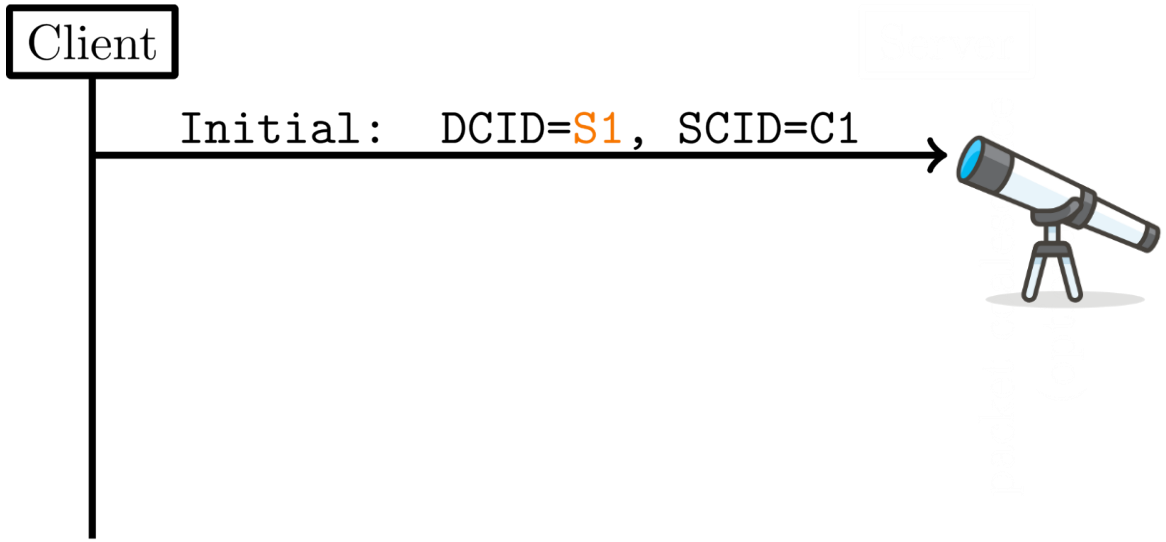


Server versions (Backscatter)



Network telescopes capture backscatter to spoofed Initials





Network telescopes capture unsolicited traffic to a silent prefix.

QUIC scans consist of Initial packets.

They convey version information and connection IDs.

After migration to Meta SCIDv2 host IDs are reused

Until 2023

- ➔ In 2023, host IDs are globally unique
  ⇒ 31,733 unique host IDs
- ➔ Host IDs indicate the number of L7LBs.
- ➔ Multiple VIPs form a cluster, when they share at least one host ID.
- ➔ Each cluster is placed in one /24 prefix.
- ➔ VIPs forward to all L7LBs of that cluster.

Migration in 2023

- ➔ Host IDs are reused across clusters
  ⇒ 4,193 unique host IDs
- ➔ Total number of L7LBs doesn't change

Cluster structure changes in 2024

- ➔ Number of clusters increases while the number of VIPs per cluster decreases.

Inferred QUIC Stack Configurations (2025)

		Hypergiant						
		Akamai	Amazon	Apple	Cloudflare	Fastly	Google	Meta	Microsoft
First backscatter visible		2023	2022	2022	2021	2023	2021	2021	2022
Features	Coalescence	✓	✓	✓	✓	✓	✓	✘	✓
	Structured SCIDs	✓	✓	✓	✓	✓	✓	✓	✓
	Retry observed	✘	✘	✘	✓	✘	✘	✘	✓
	L7 load balancers	n/a	n/a	n/a	n/a	n/a	n/a	✓	n/a
	SCID length	20 B	20 B	20 B	20 B	17 B	8 B	8 B	14/20 B
	Initial RTO	1 s	0.3 s	1 s	1 s	0.2 s	0.3 s	0.1 s	1 s
	Mean # retransmissions	2.1	4.0	2.7	1.5	6.0	3.4	7.5	1.3

QUIC packet types

	Relative number of packets from source network per year [%]																			
	Cloudflare					Google					Meta					Others				
QUIC Packet Type	'21	'22	'23	'24	'25	'21	'22	'23	'24	'25	'21	'22	'23	'24	'25	'21	'22	'23	'24	'25
Initial	42	56	54	49	45	34	23	7	9	35	65	48	47	43	47	69	46	33	36	43
Handshake	28	41	43	42	44	21	24	26	34	33	35	52	53	57	53	29	43	41	40	41
0-RTT	-	-	-	-	-	2	<1	<1	-	-	-	-	-	-	-	1	<1	<1	<1	-
Retry	-	-	-	-	3	-	-	-	-	-	-	-	-	-	-	<1	<1	<1	<1	<1
Version Negotiation	-	-	-	<1	-	-	-	-	-	-	-	-	-	-	-	-	3	<1	3	1
Colaesced Packets																				
Initial+Initial	10	-	-	-	-	-	-	-	-	-	-	-	-	-	-	<1	-	<1	-	-
Initial+Handshake	10	3	3	8	9	44	53	67	57	32	-	-	-	-	-	1	9	26	20	14
Handshake+Handshake	10	-	-	-	-	-	-	-	-	-	-	-	-	-	-	<1	-	-	-	-

Hypergiant frontend cluster deployment