

Fixing HTTP/2 and preparing for HTTP/3 over QUIC

Robin Marx

@programmingart





Robin Marx

@programmingart

PhD Student

Web Performance

Internet Protocols

Contributor to QUIC and HTTP/3

I list my **references**

<https://bit.ly/velocityquic>

01 Fixing HTTP/2

- Denialing of Services
- Pushing the wrong things
- Buggy prioritization



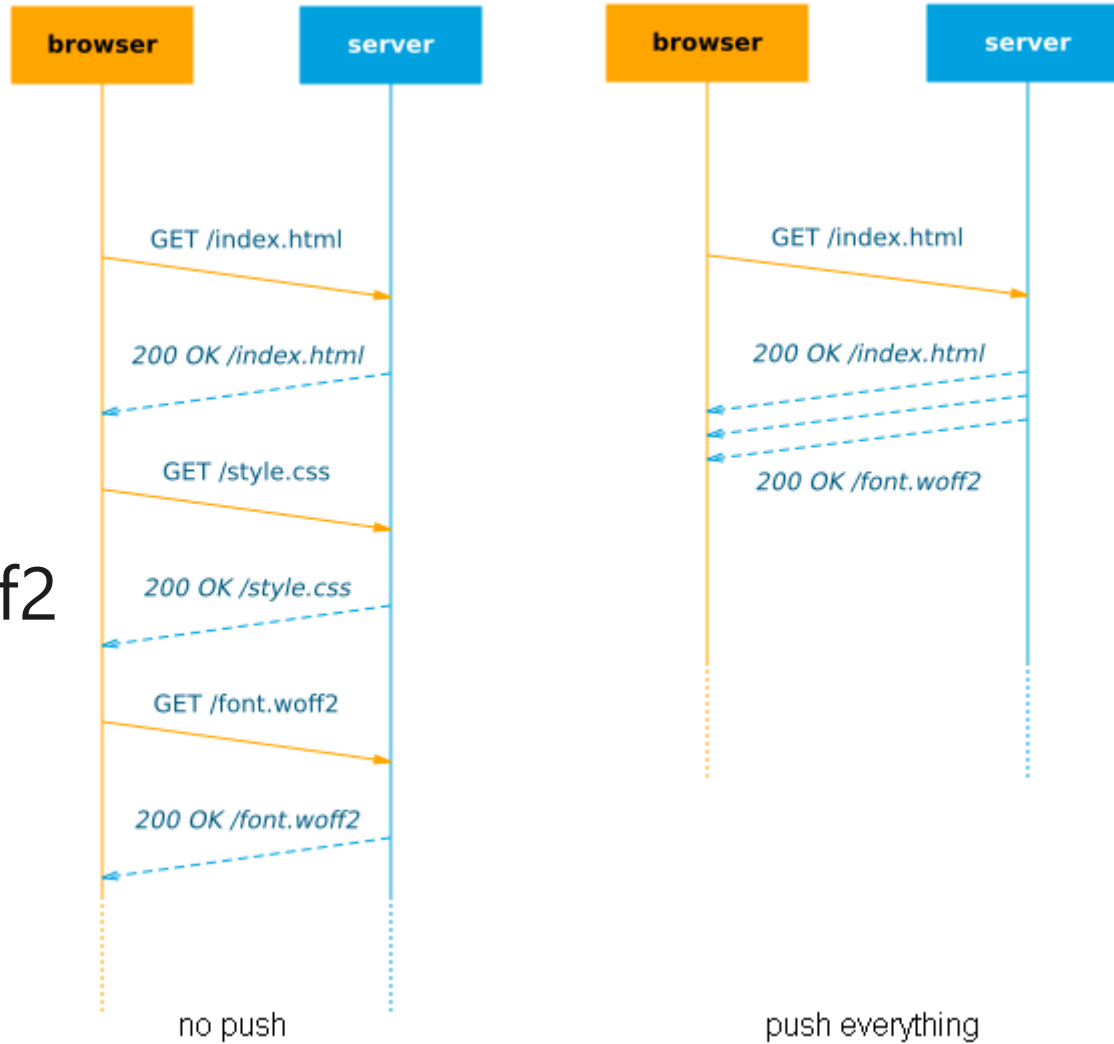
1. Flooding HTTP/2

1. CVE-2019-9511 "Data Dribble"
2. CVE-2019-9512 "Ping Flood"
3. CVE-2019-9513 "Resource Loop"
4. CVE-2019-9514 "Reset Flood"
5. CVE-2019-9515 "Settings Flood"
6. CVE-2019-9516 "0-Length Headers Leak"
7. CVE-2019-9517 "Internal Data Buffering"
8. CVE-2019-9518 "Empty Frames Flood"

- Tomcat
- macOS X
- nginx
- Go
- H2O
- LiteSpeed
- Windows
- NodeJS

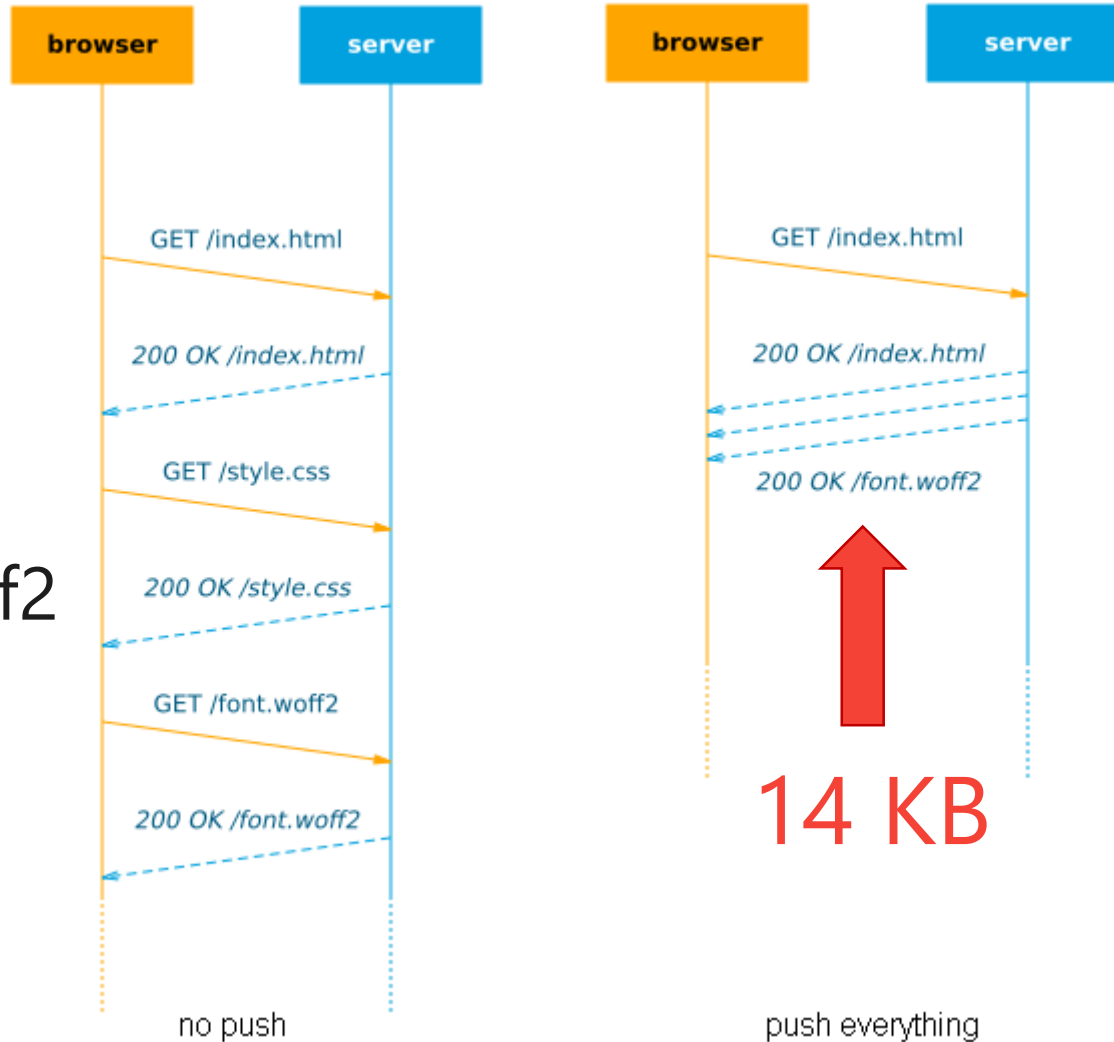
2. Push in theory

index.html
↳ style.css
↳ font.woff2

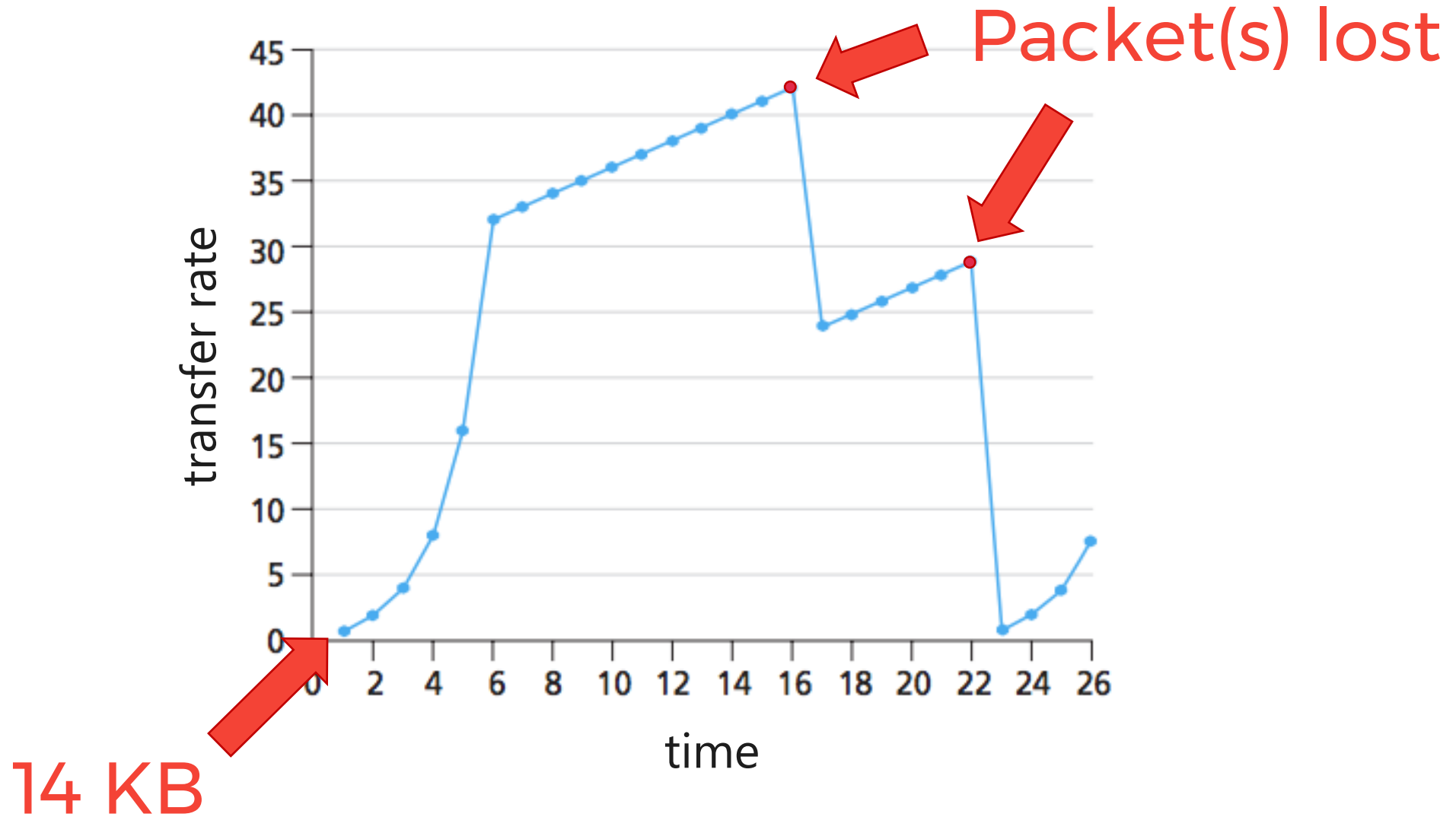


2. Push in practice

index.html
↳ style.css
↳ font.woff2



2. Congestion Control



2. Push in practice

index.html
↳ style.css
↳ font.woff2



Other issues

Cache Digests are **dead**

- No standard way to know **what the client has cached**
- Can work around that with **cookies**, service workers or other heuristics

Quirks in browsers and servers

- e.g., no push for fetch() or XHR, <iframe>

Push is **per-connection**

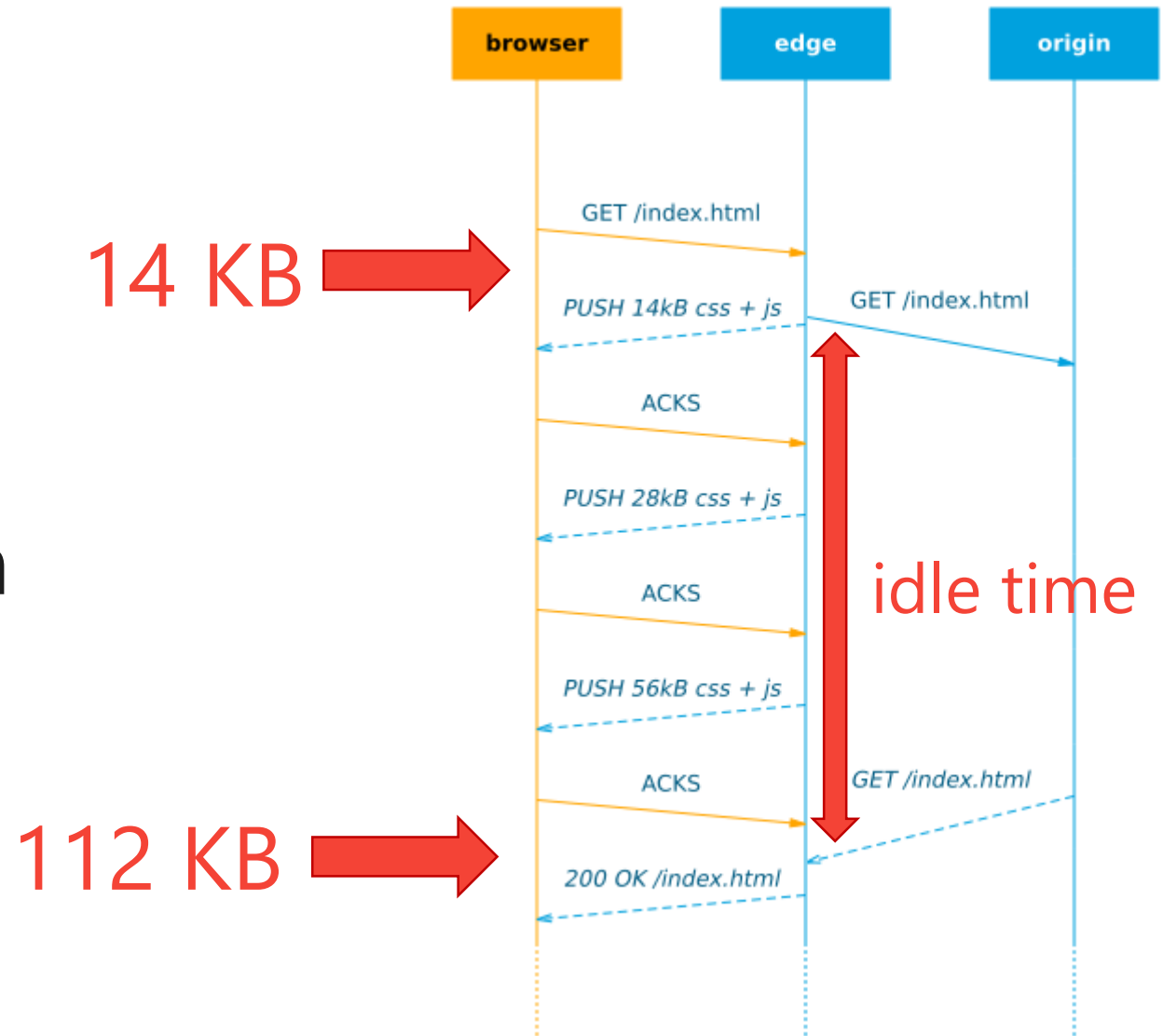
- could end up sending things twice

Used by
0.5% of sites

<https://almanac.httparchive.org>
<https://tools.ietf.org/html/draft-ietf-httpbis-cache-digest-05>
<https://jakearchibald.com/2017/h2-push-tougher-than-i-thought/>
<https://lists.w3.org/Archives/Public/ietf-http-wg/2019JanMar/0033.html>
<http://blog.kazuhooku.com/2015/10/performance-of-http2-push-and-server.html>

CDNs

"warm up" the
connection from
client to CDN



Beyond the initial page load!

Speed up **API calls**

```
{  
  "id": 666,  
  "images": [  
    "https://example.com/big_image1.jpg",  
    "https://example.com/big_image2.jpg",  
    "https://example.com/big_image3.jpg"  
  ],  
  "details": "https://example.com/details/666"  
}
```

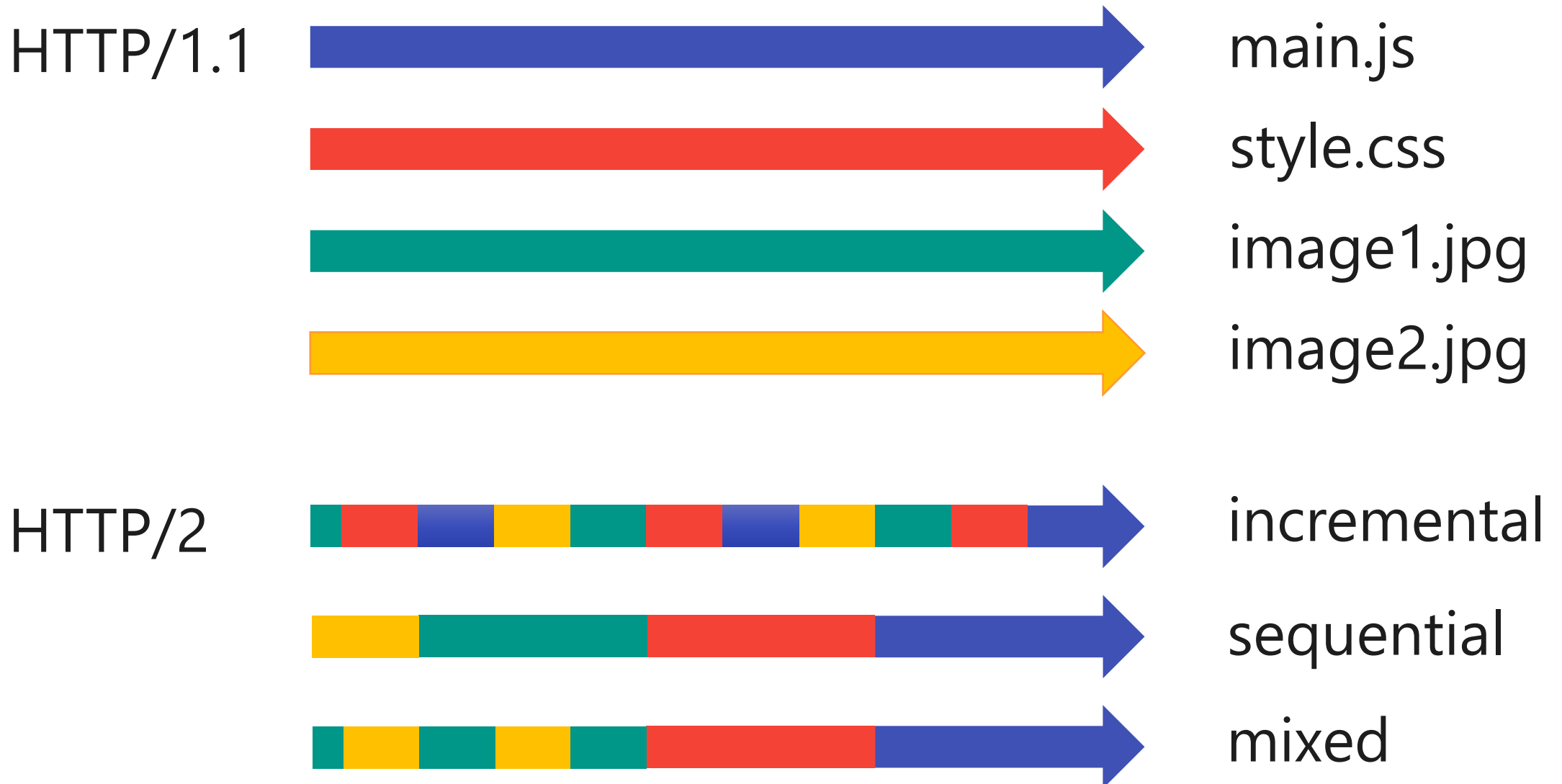
See also: "**edge workers**"

<https://github.com/gabesullice/hades>
<https://evertpot.com/h2-push-for-apis/>
<https://biblio.ugent.be/download/8552455/8552457.pdf>
<https://calendar.perfplanet.com/2016/http2-push-the-details/>

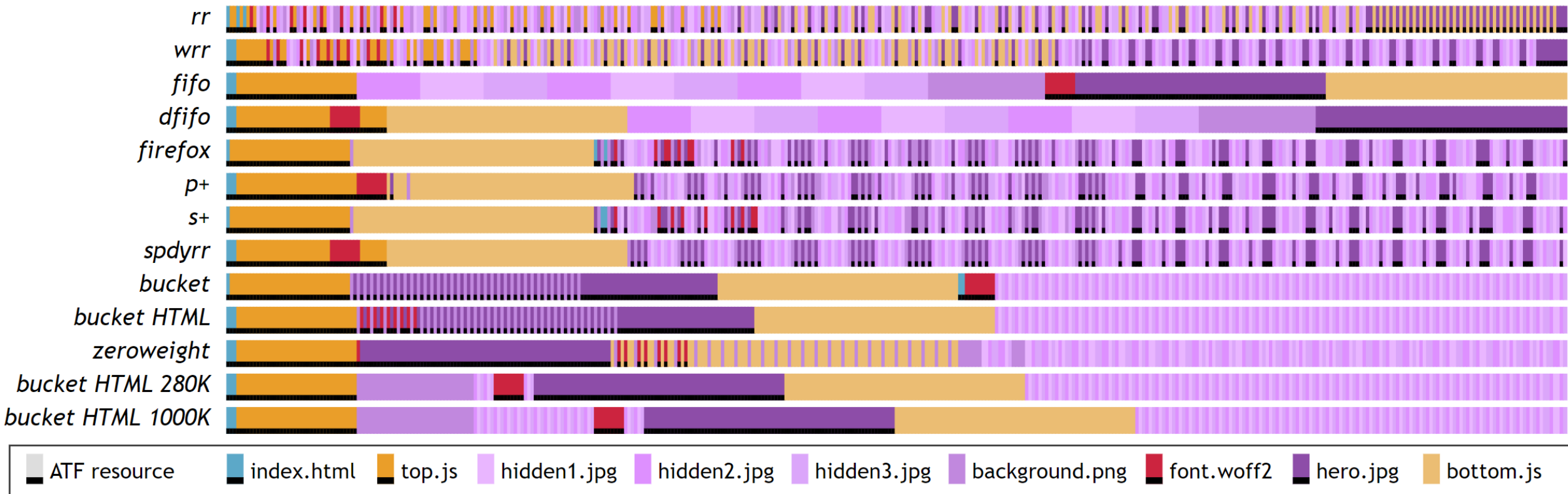
3. Multiplexing and Prioritization



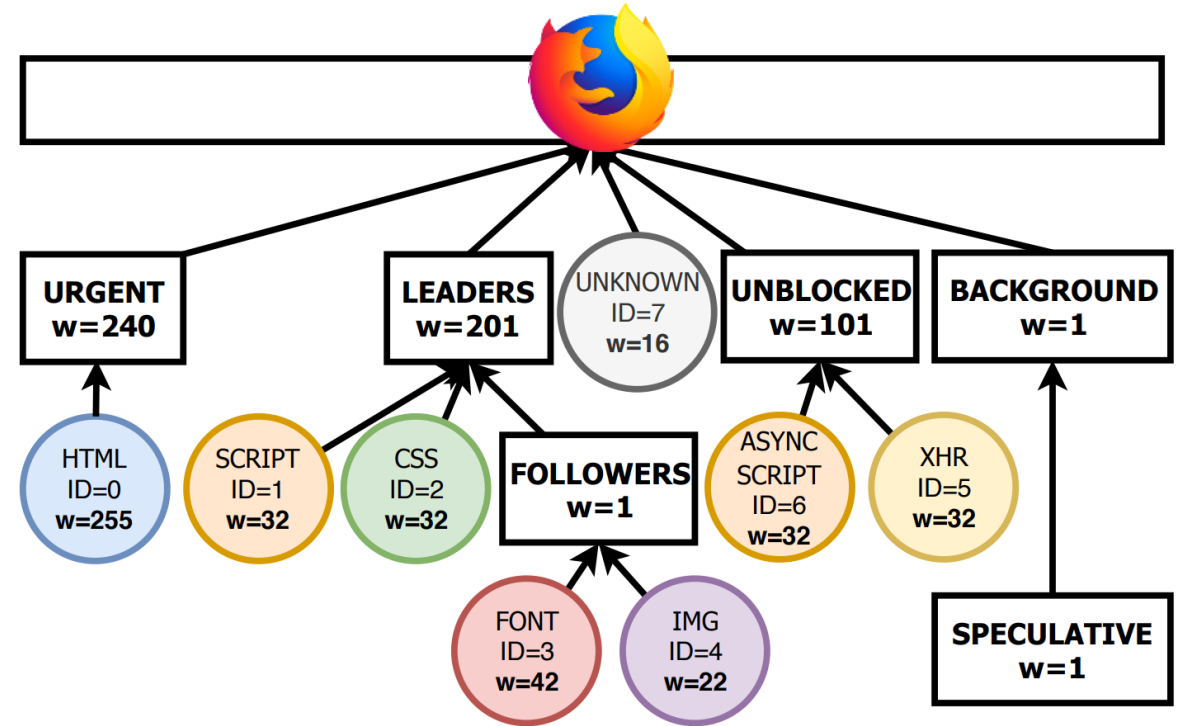
3. Multiplexing and Prioritization



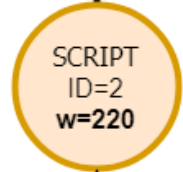
Welcome to the jungle



HTTP/2 Prioritization in Browsers

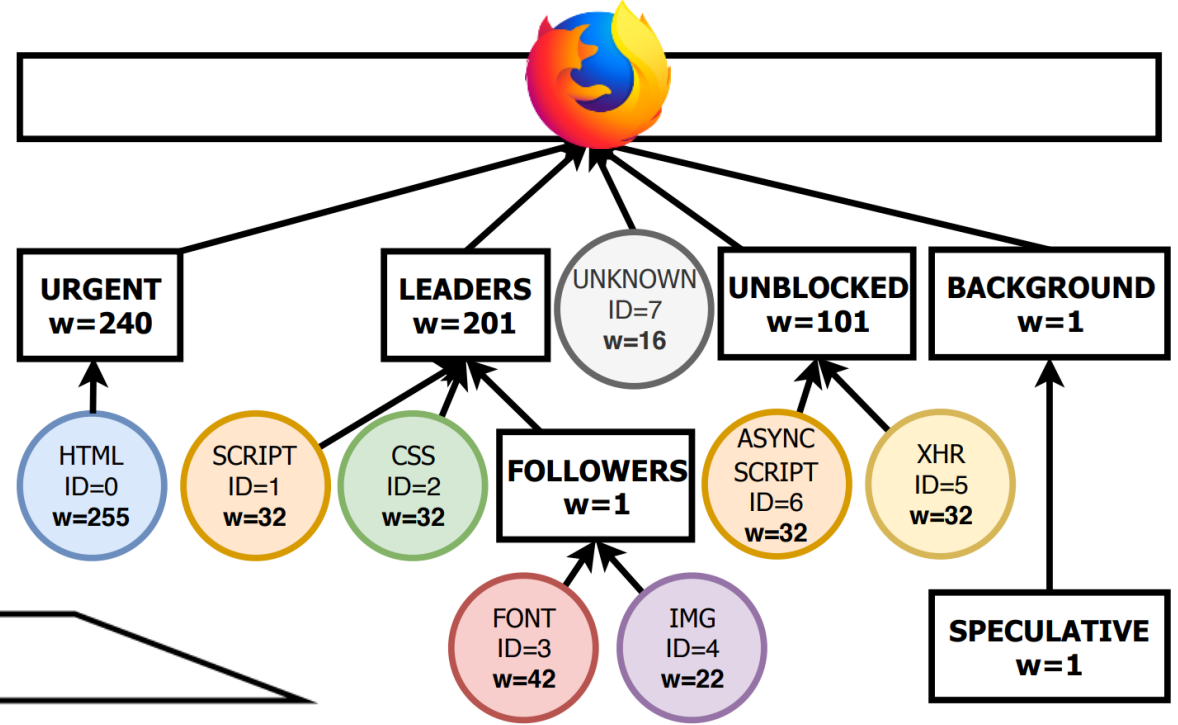
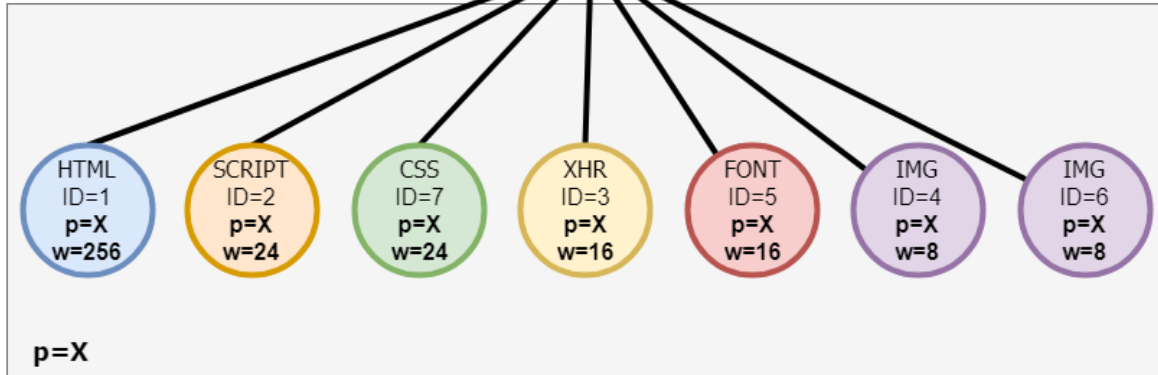


HTTP/2 Prioritization in Browsers

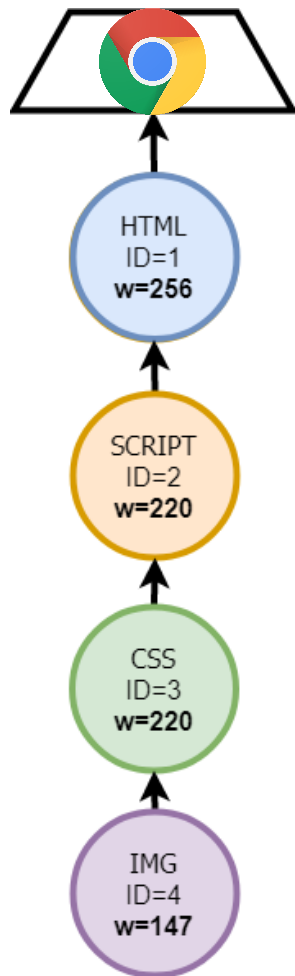


“sequential”
everything

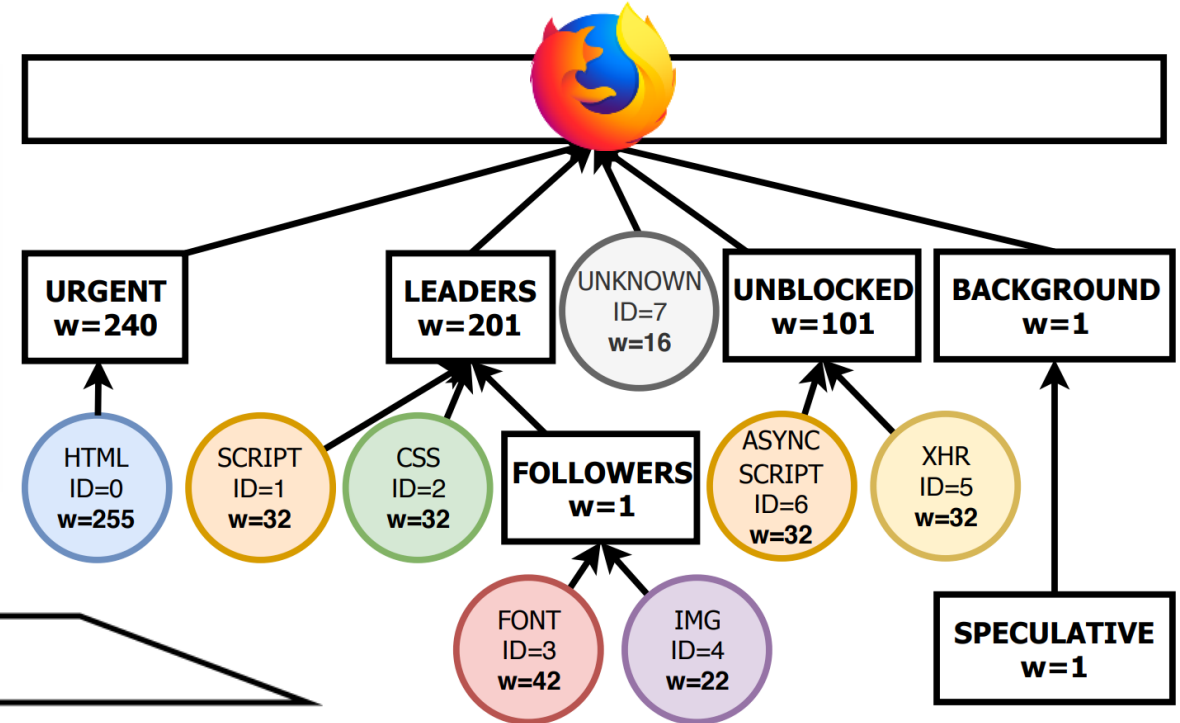
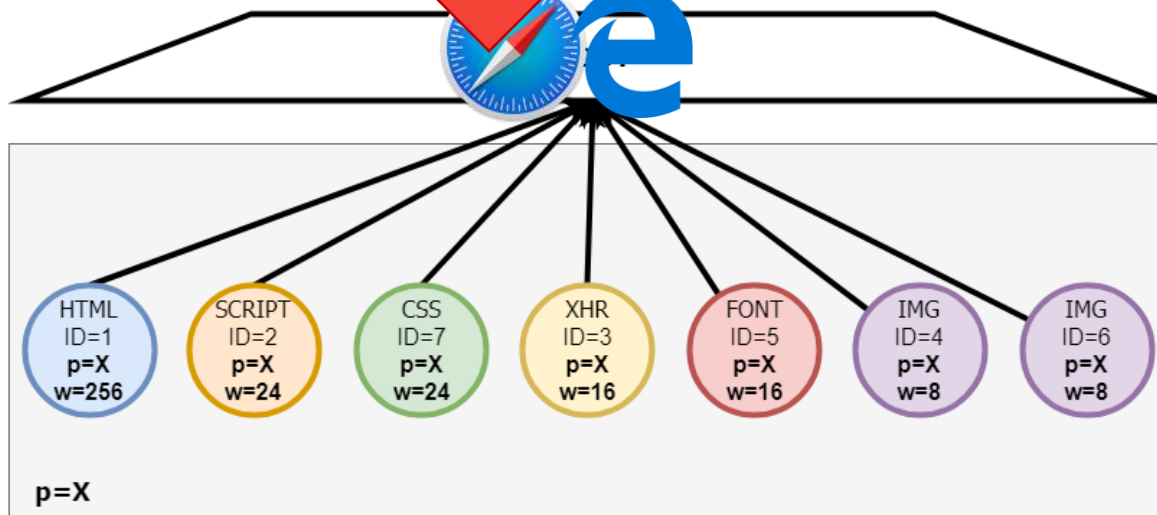
“incremental”
everything



HTTP/2 Prioritization in Browsers



Up to **50%**
slower than
Chrome



<https://h3.edm.uhasselt.be>

<https://speeder.edm.uhasselt.be/www18/>

<https://blog.cloudflare.com/better-http-2-prioritization-for-a-faster-web>

<https://blog.cloudflare.com/nginx-structural-enhancements-for-http-2-performance>

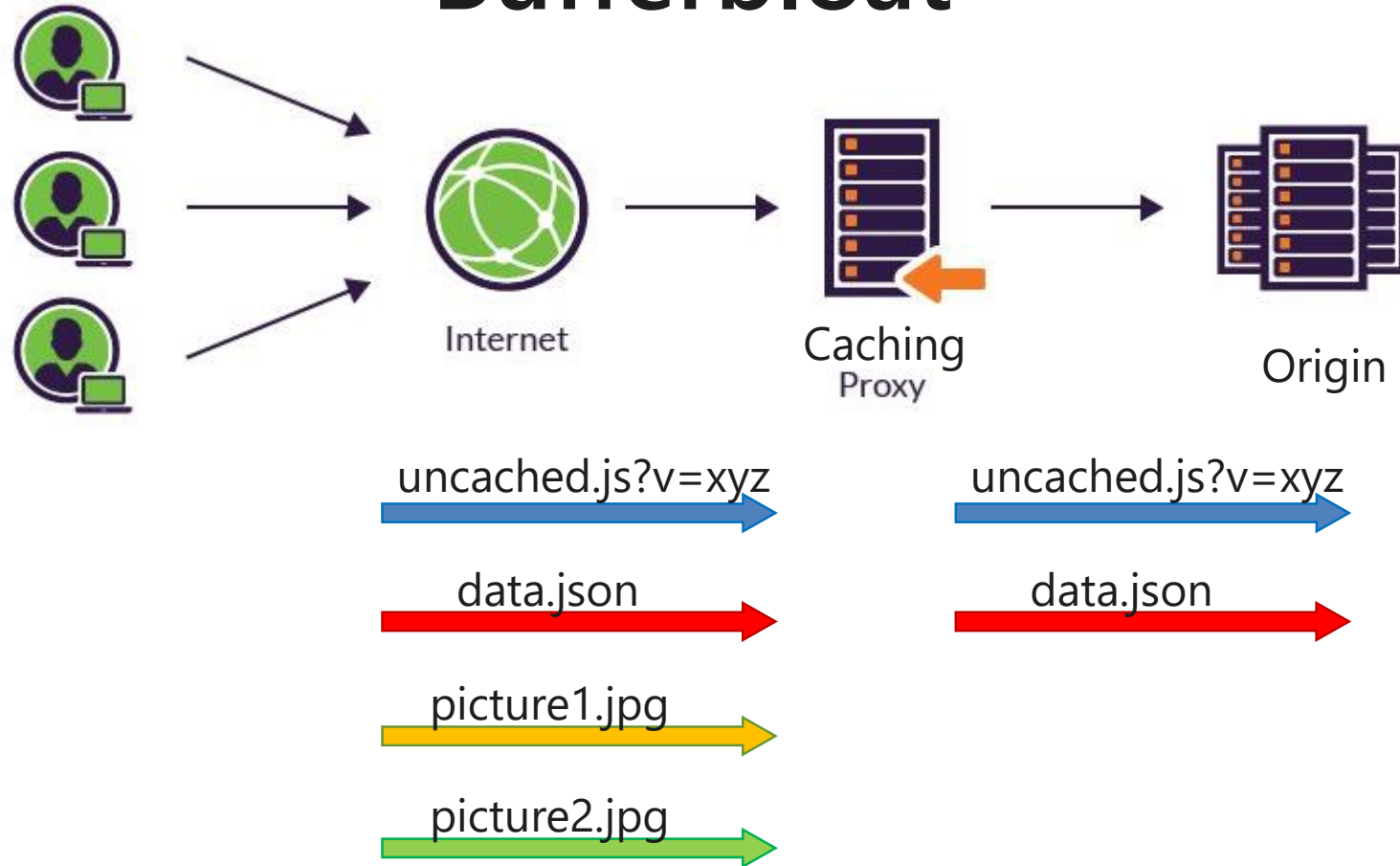
HTTP/2 Prioritization in Servers

CDN / Hosting	Status	Test Result		
Amazon	Pass	Dec 22, 2018		
Amazon CloudFront	FAIL	Dec 22, 2018	FAIL	Dec 22, 2018
Bitly	FAIL	Dec 22, 2018	FAIL	Dec 22, 2018
Cachify	FAIL	Dec 22, 2018	FAIL	Dec 22, 2018
CDN77	FAIL *	Dec 22, 2018	FAIL	Dec 22, 2018
CDNetworks	FAIL	Dec 22, 2018	FAIL	Dec 22, 2018
CDNuse	Pass	Dec 22, 2018	FAIL	Dec 22, 2018
CloudCache	FAIL	Dec 22, 2018	FAIL	Dec 22, 2018
CloudFlare	Pass	Dec 22, 2018	FAIL	Dec 22, 2018
DreamHost	Pass	Dec 22, 2018	FAIL	Dec 22, 2018
Edgemail	FAIL	Dec 22, 2018	FAIL	Dec 22, 2018
Fastlink	Pass	Dec 22, 2018	FAIL	Dec 22, 2018
Fasty	Pass	Dec 22, 2018	Pass	Jan 1, 2019
Google Firebase	Pass	Dec 22, 2018	FAIL *	Dec 22, 2018
Google Storage	FAIL	Dec 22, 2018	FAIL	Dec 22, 2018
Highwinds	FAIL	Dec 22, 2018	Pass	Dec 22, 2018
			FAIL	Dec 22, 2018
			FAIL	Dec 22, 2018
			FAIL	Dec 22, 2018

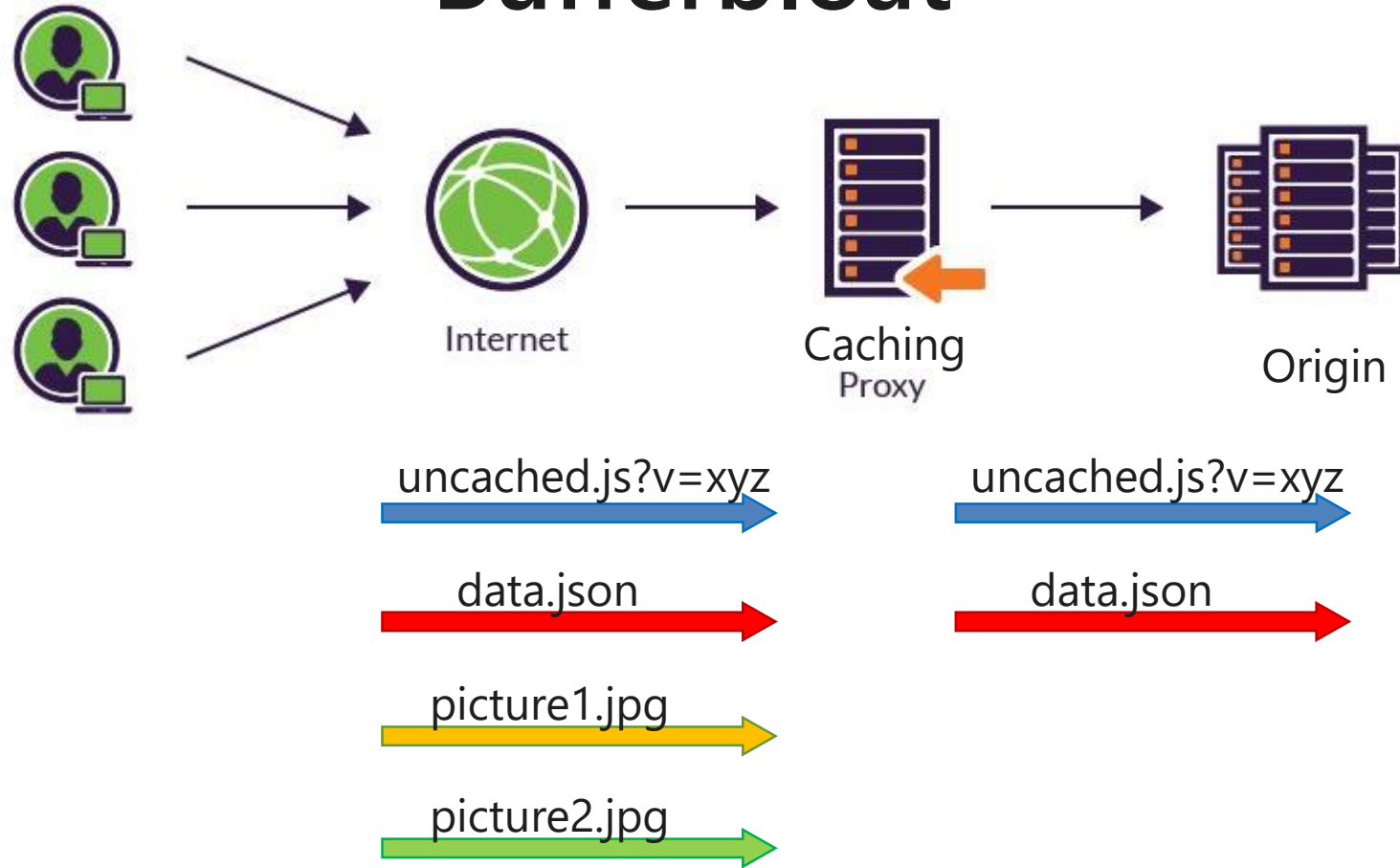
9 / 34 deployments pass

<https://www.youtube.com/watch?v=ct5MvtmL1NM>
<https://github.com/andydavies/http2-prioritization-issues>
<https://www.slideshare.net/patrickmeenan/http2-in-practice>

Bufferbloat



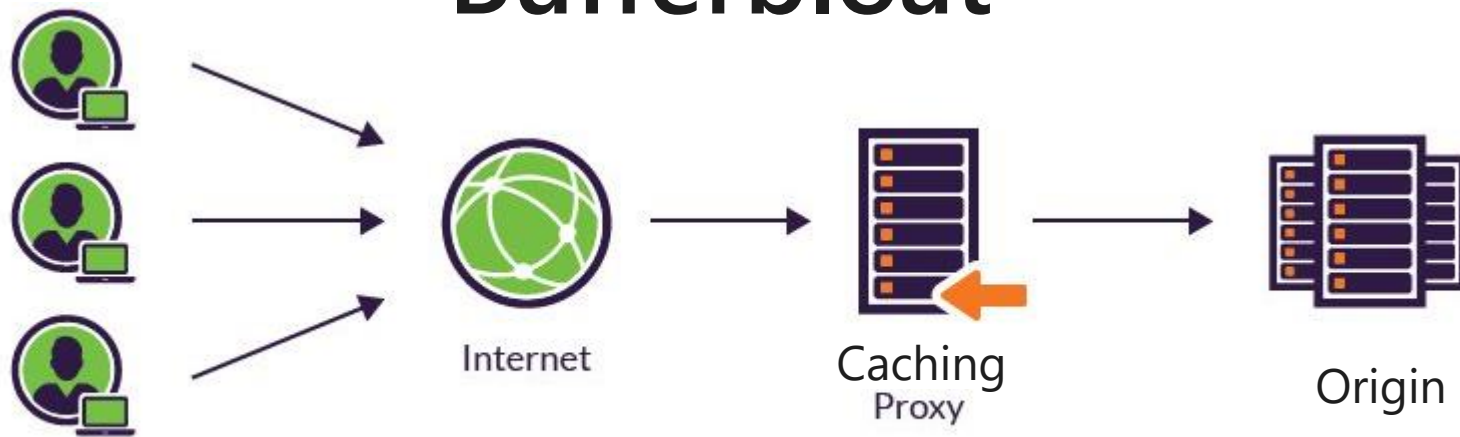
Bufferbloat



Expected:



Bufferbloat



`uncached.js?v=xyz`

`data.json`

`picture1.jpg`

`picture2.jpg`

`uncached.js?v=xyz`

`data.json`

Expected:



Actual:



Types of Headaches

Migraine



Hypertension



Stress

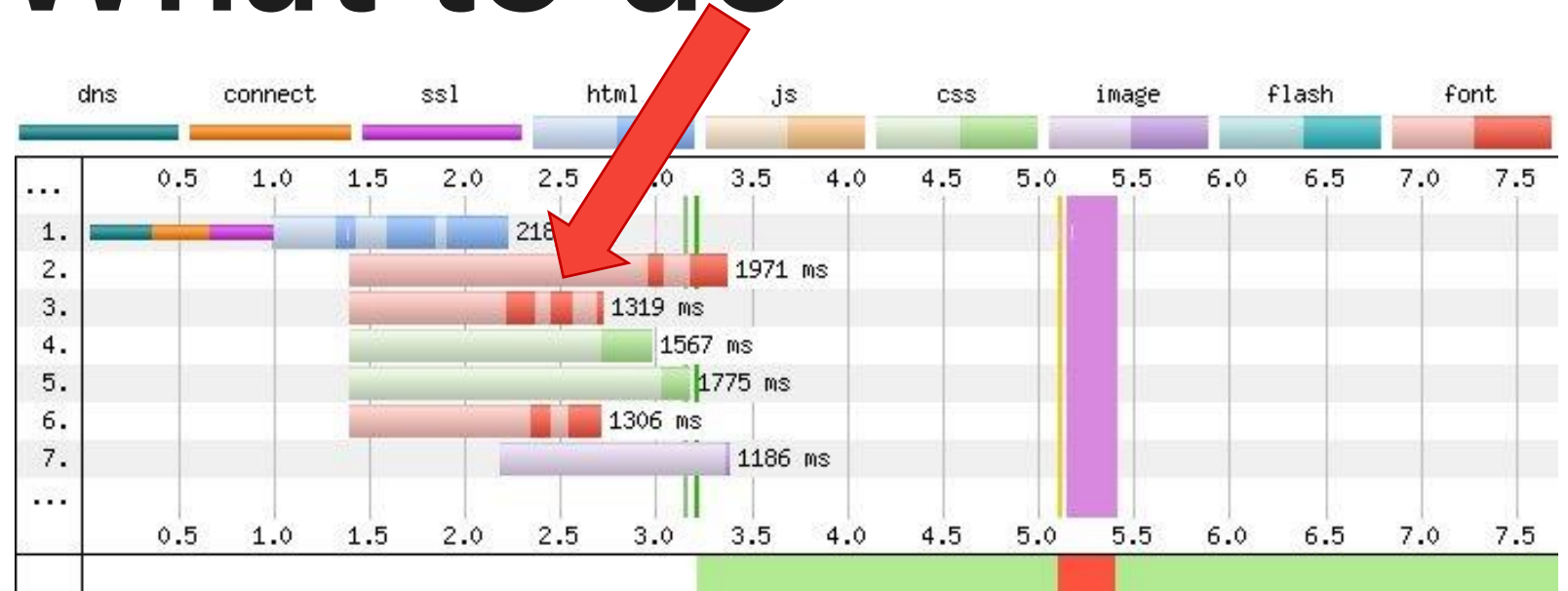


Prioritization



What to do

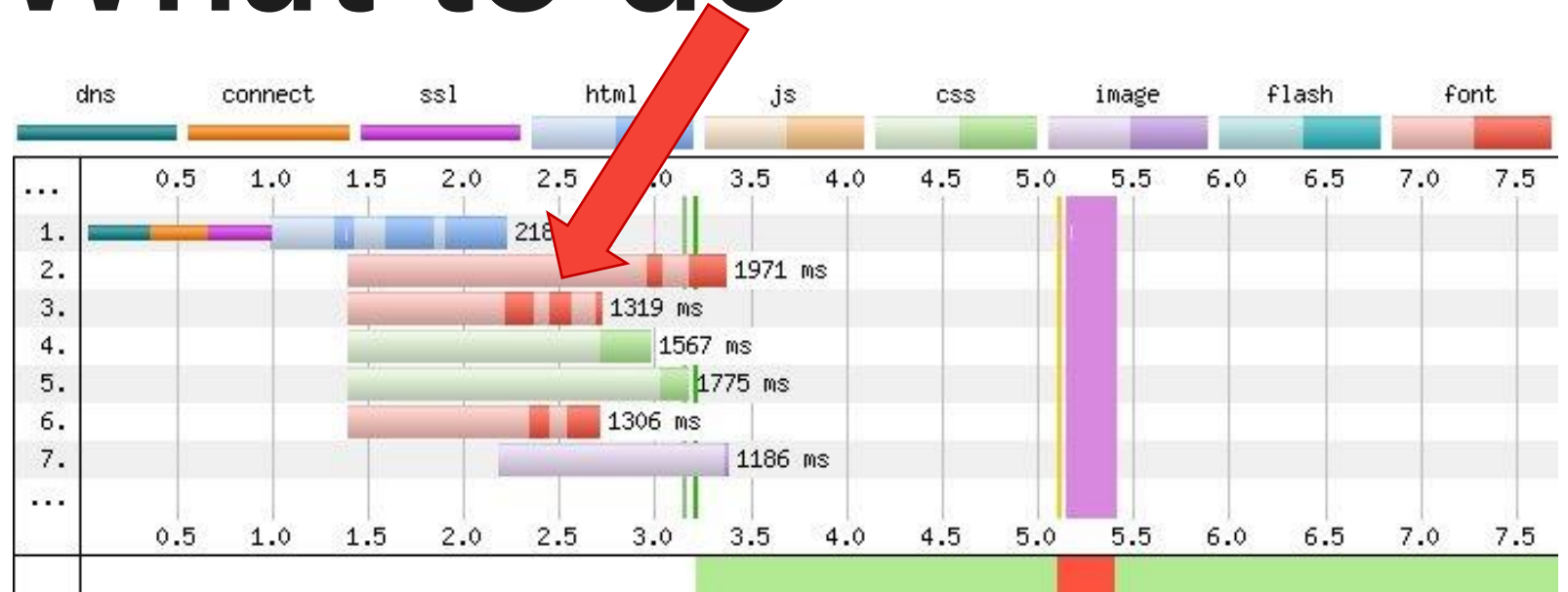
- **Test** your pages
webpagetest.org



<https://www.youtube.com/watch?v=ct5MvtmL1NM>
<https://www.slideshare.net/patrickmeenah/http2-in-practice>
<https://blog.cloudflare.com/http-2-prioritization-with-nginx>
<https://twitter.com/csswizardry/status/1180810824862064646?s=20>
<https://andydavies.me/blog/2019/02/12/preloading-fonts-and-the-puzzle-of-priorities/>

What to do

- **Test** your pages
webpagetest.org



- **Pick a different server / CDN**
- Reduce buffer sizes
- Use BBR congestion controller
- Override browser-sent priorities on the server
- Be careful with `<link rel="preload" />`

<https://www.youtube.com/watch?v=ct5MvtmL1NM>
<https://www.slideshare.net/patrickmeenah/http2-in-practice>
<https://blog.cloudflare.com/http-2-prioritization-with-nginx>
<https://twitter.com/csswizardry/status/1180810824862064646?s=20>
<https://andydavies.me/blog/2019/02/12/preloading-fonts-and-the-puzzle-of-priorities/>

HTTP/3 prioritization proposal

Header-based, simpler

```
:method = GET  
:scheme = https  
:path = /image.jpg  
priority = urgency=3, progressive=?1
```



Urgency Definition

-1 prerequisite (Section 2.1.1)

0 default (Section 2.1.2)

between 1 and 5 supplementary (Section 2.1.3)

6 background (Section 2.1.4)



02

HTTP/3 over QUIC

- Encrypted UDP
- Load balancing and routing
- 0-RTT setup
- QUIC and HTTP/3 discovery
- Debugging and tooling

QUIC is **TCP 2.0**

application

HTTP/2

TLS

transport

TCP

HTTP/3

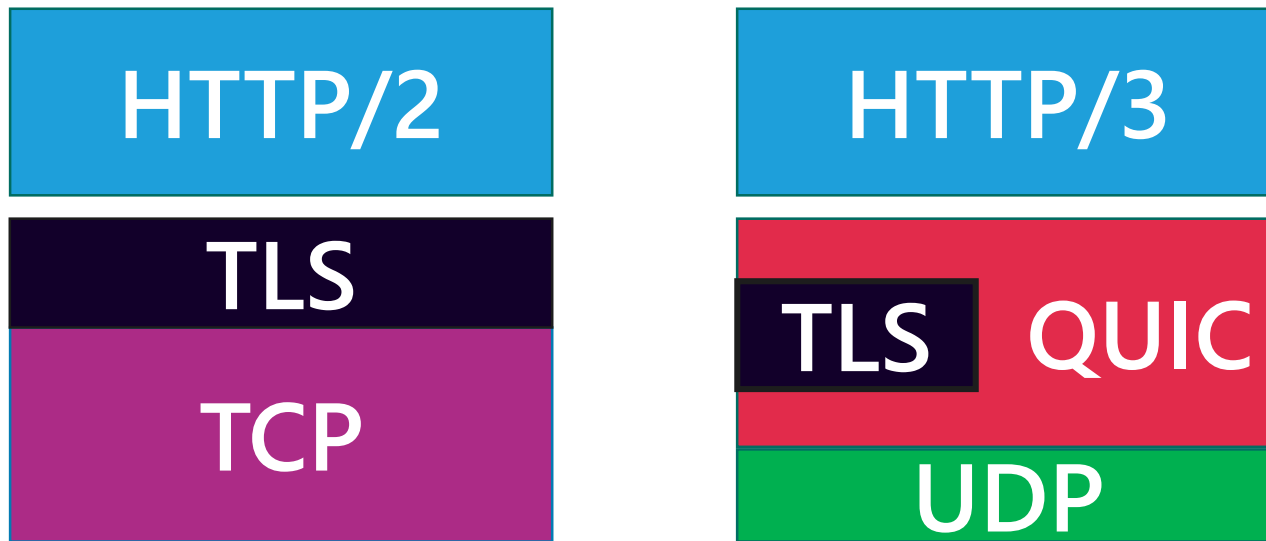
TLS

QUIC

application

transport

UDP



HTTP/3 is HTTP/2 for QUIC

2015

Single connection
Multiplexing
Header Compression
Server Push
Prioritization

application

HTTP/2

TLS

transport

TCP

2019

Single connection
Multiplexing
Header Compression
Server Push
~Prioritization

application

HTTP/3

TLS QUIC

transport

UDP

QUIC encrypts the Transport layer

application

SECURE

transport

ports,
packet seq nr,
acknowledgements,
flow control, retransmits,
flags, options

SECURE

flags, connection id

SECURE

ports

application

transport

1. Networks blocking QUIC

3¹-20²% of networks block QUIC/UDP

“The websites will still work, so you might as well choose security over a tiny increase in performance”³

¹ <https://www.ietf.org/proceedings/96/slides/slides-96-quic-3.pdf>

² <https://conferences2.sigcomm.org/co-next/2018/slides/epiq-keynote.pdf>

³ <https://www.fastvue.co/fastvue/blog/googles-quic-protocols-security-and-reporting-implications/>

1. Networks blocking QUIC

3¹-20²% of networks block QUIC/UDP

“The websites will still work, so you might as well choose security over a tiny increase in performance”³



dschinazi 9:17 PM

QUIC uses the local store but it fails the handshake if the root CA is not in the default set. This was done by policy to prevent antivirus software from MITM QUIC so we can keep evolving QUIC.

¹ <https://www.ietf.org/proceedings/96/slides/slides-96-quic-3.pdf>

² <https://conferences2.sigcomm.org/co-next/2018/slides/epiq-keynote.pdf>

³ <https://www.fastvue.co/fastvue/blog/googles-quic-protocols-security-and-reporting-implications/>

1. Built-in security features

“SYN flood”

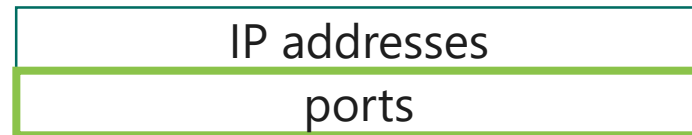
- Stateless Retry



UDP reflection / amplification

- Maximum amplification factor of 3

2. Connection ID



0-20 bytes

2. NAT rebinding + connection migration

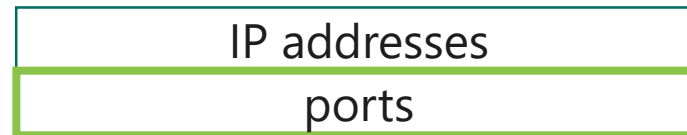


193.190.10.140:12345

Conn. ID: 0xDEADBEEF

185.194.187.142:23456

Conn. ID: 0xDEADBEEF



0-20 bytes

2. NAT rebinding + connection migration

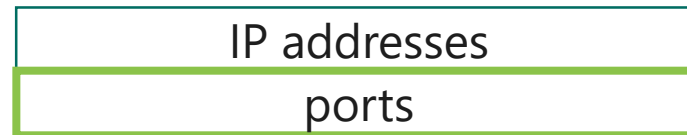


193.190.10.140:12345

Conn. ID: 0xDEADBEEF

185.194.187.142:23456

Conn. ID: **0x8BADFOOD**



0-20 bytes

2. NAT rebinding + connection migration



193.190.10.140:12345

Conn. ID: 0xDEADBEEF

185.194.187.142:23456

Conn. ID: **0x8BADFOOD**

0xDEADBEEF
0x8BADF00D
0xFACEB00C
0xDEADC0DE

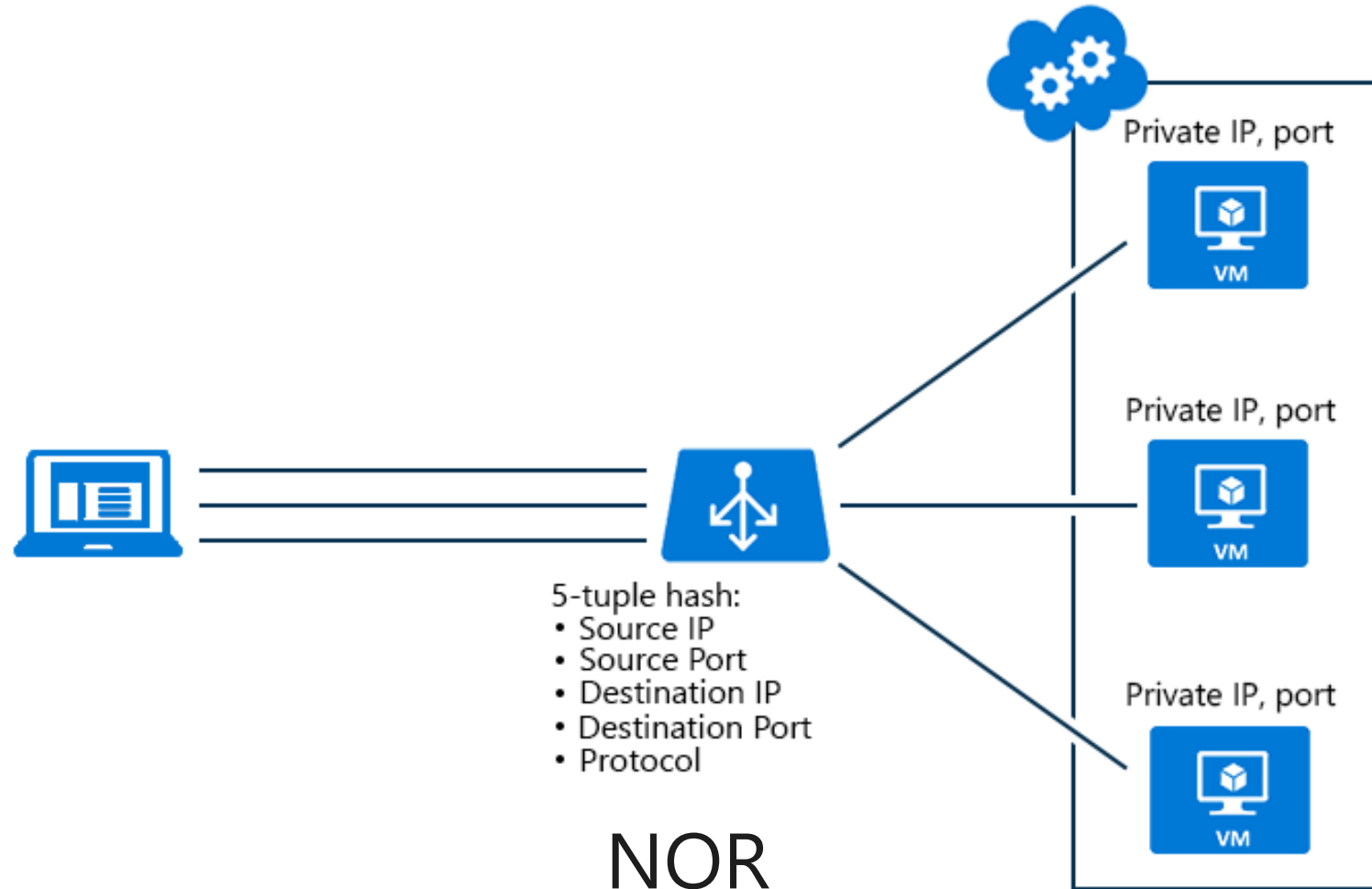
Connection #5

0xDEADBEEF
0x8BADF00D
0xFACEB00C
0xDEADC0DE

Client

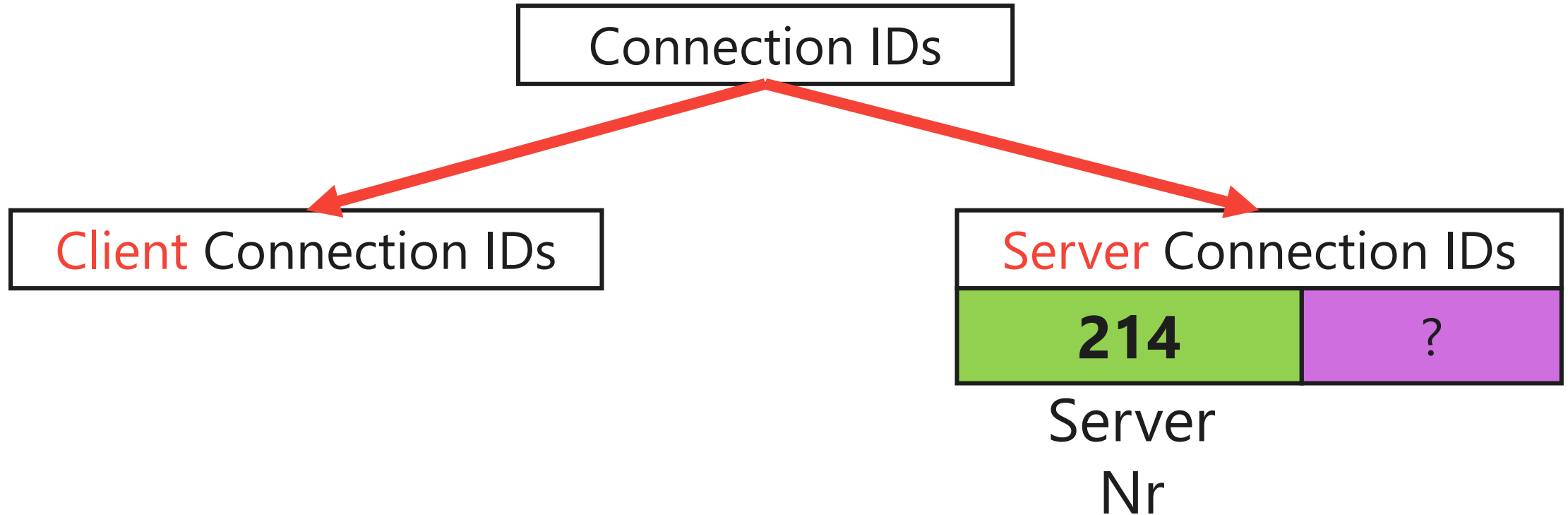
Server

2. Load balancing and routing breaks

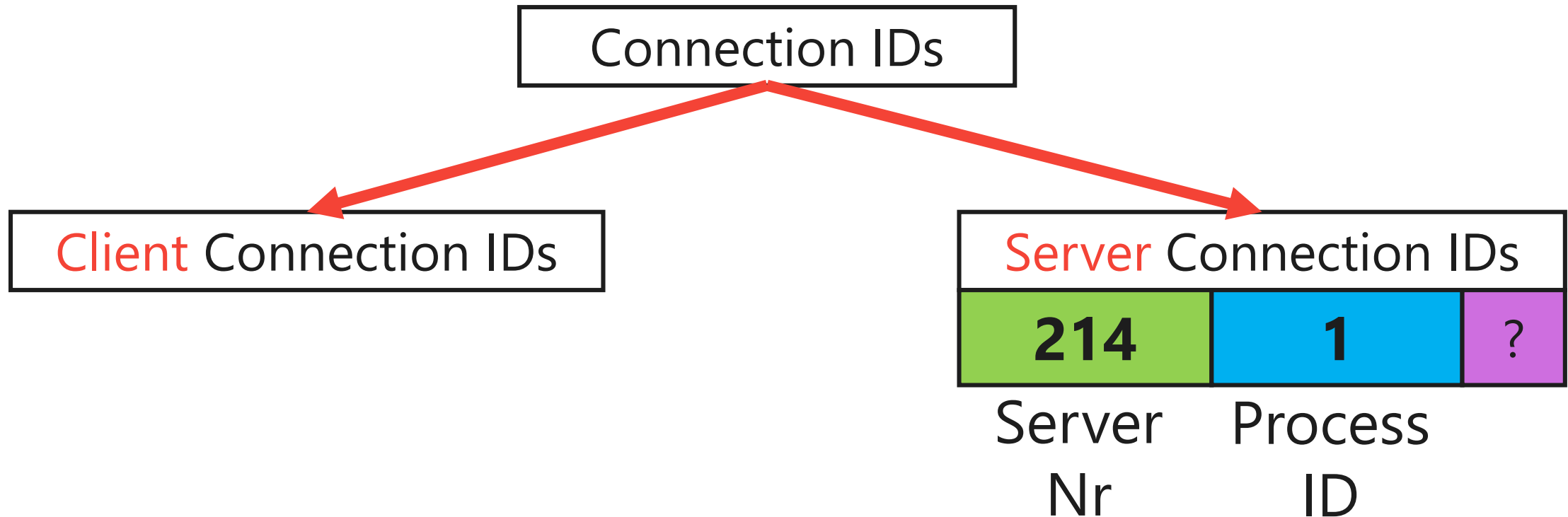


Connection ID

2. Stateless load balancing and routing

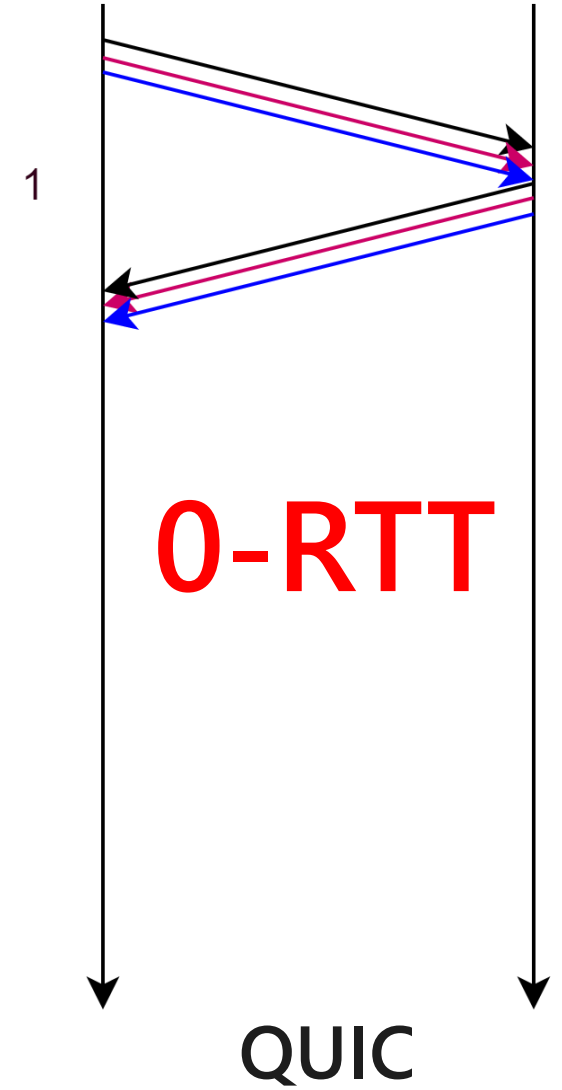
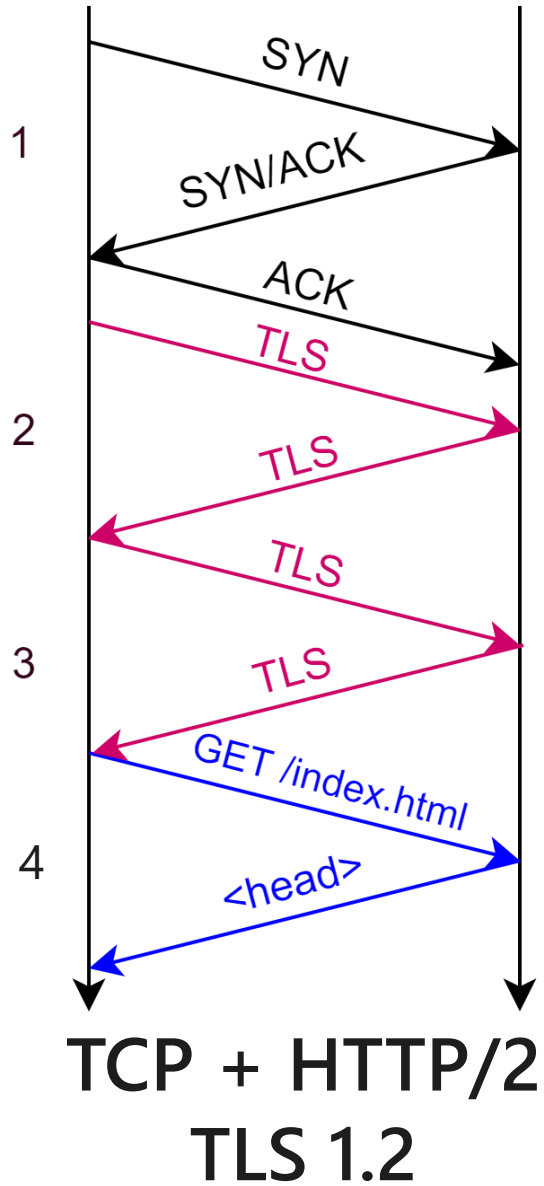


2. Stateless load balancing and routing

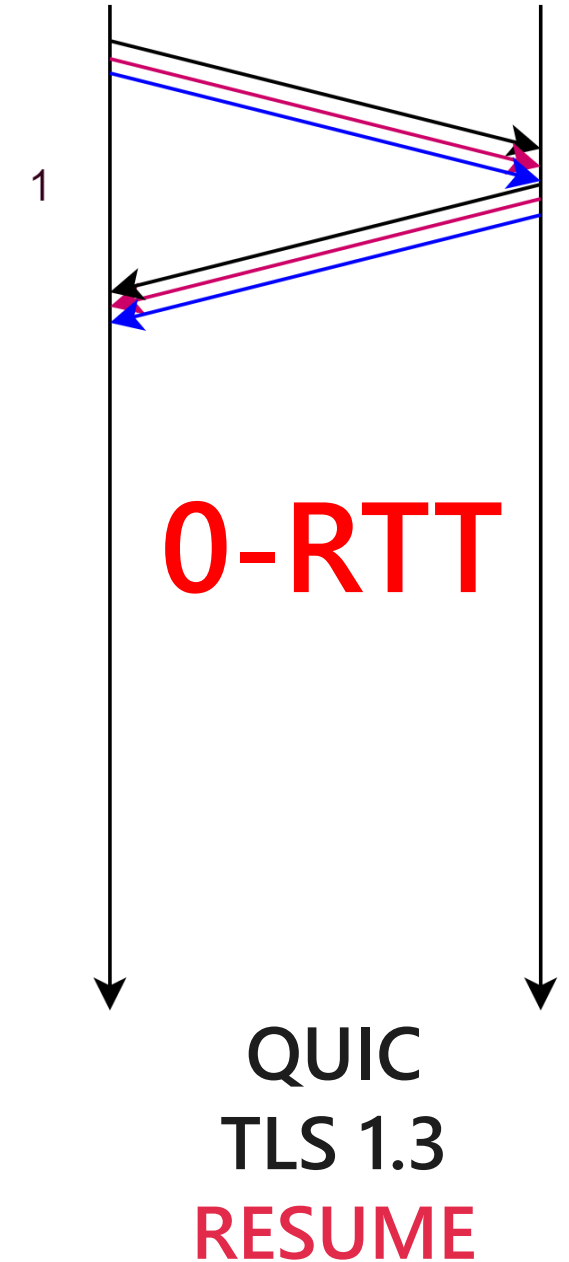
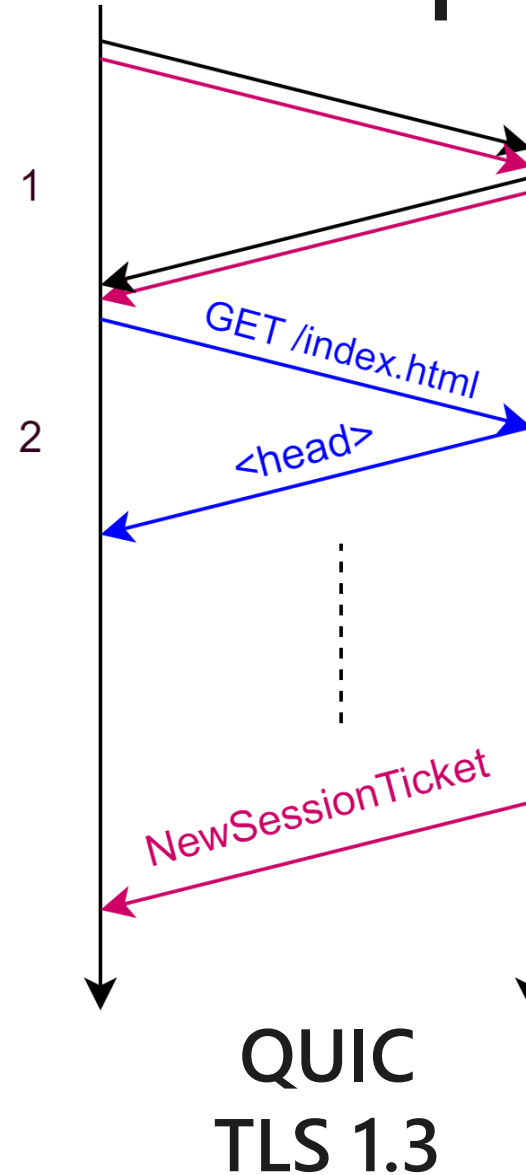
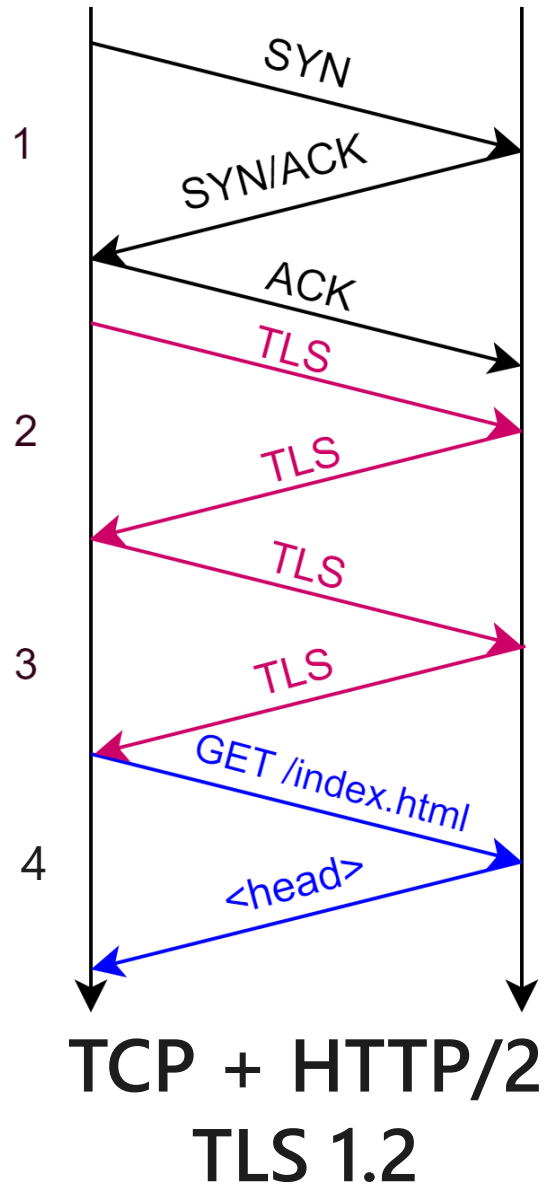


Load balancers and servers need to use the same semantics

3. Connection setup



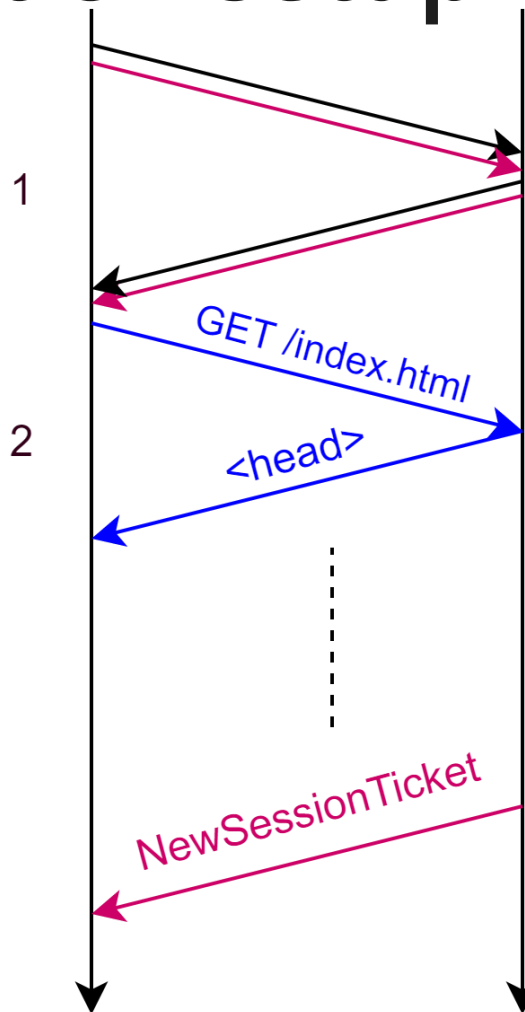
3. Connection setup



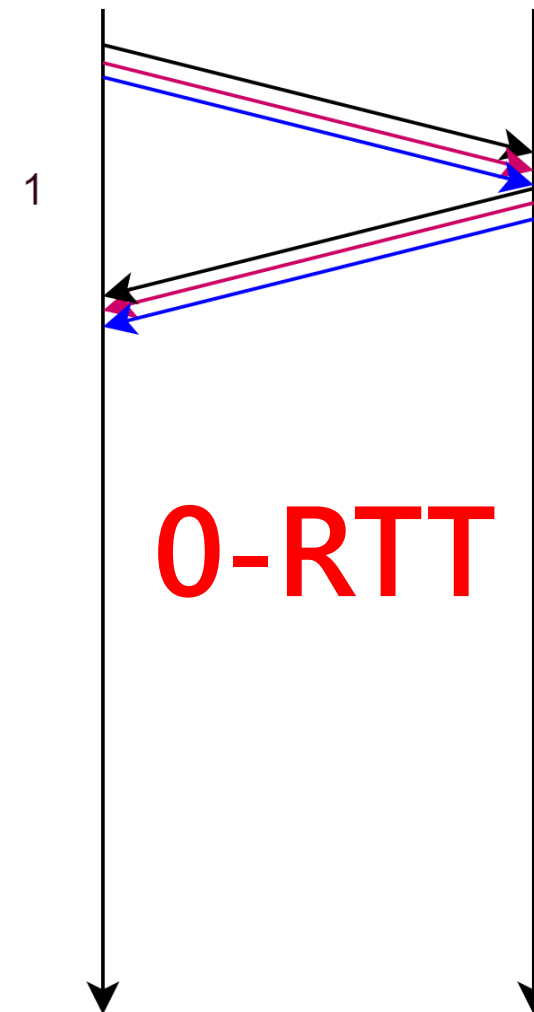
3. Connection setup

0-RTT

- Store state on the server
 - Share across server pool...
- Store state in tickets themselves
 - Encrypt tickets separately
 - Share ticket keys...
 - Rotate ticket keys frequently



QUIC
TLS 1.3

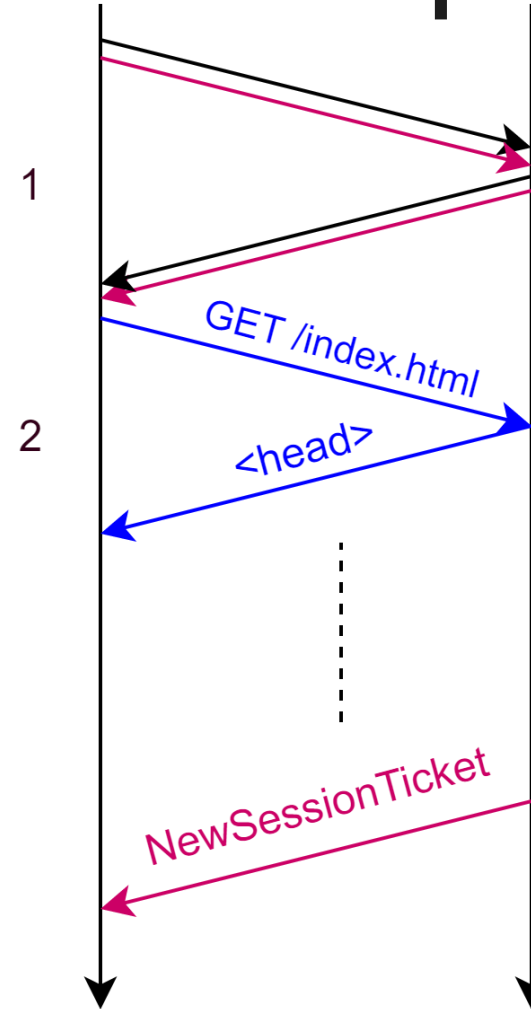


QUIC
TLS 1.3
RESUME

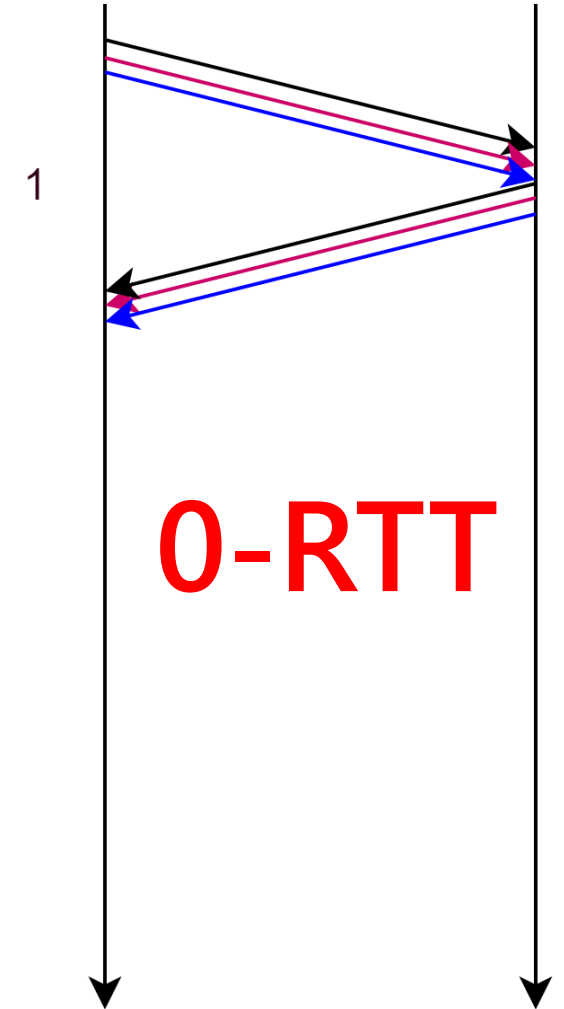
3. Connection setup

0-RTT

- Store state on the server
 - Share across server pool...
- Store state in tickets themselves
 - Encrypt tickets separately
 - Share ticket keys...
 - Rotate ticket keys frequently
- **Replay attacks**: idempotent only



QUIC
TLS 1.3



QUIC
TLS 1.3
RESUME

4. QUIC discovery

QUIC



4. QUIC discovery

QUIC



TCP



4. QUIC discovery



4. QUIC discovery

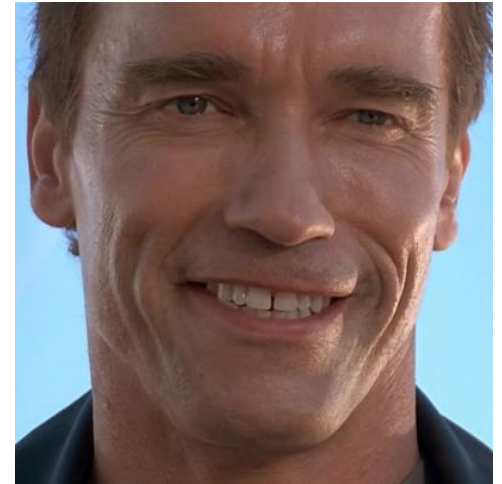
QUIC



TCP



100 ms
delay



Happy eyeballs

4. QUIC discovery

QUIC IPv6



TCP IPv6



100 ms

QUIC IPv4



200 ms

TCP IPv4



300 ms

Replay "attacks"...



Happy eyeballs

4. QUIC and HTTP/3 discovery with alt-svc

TCP

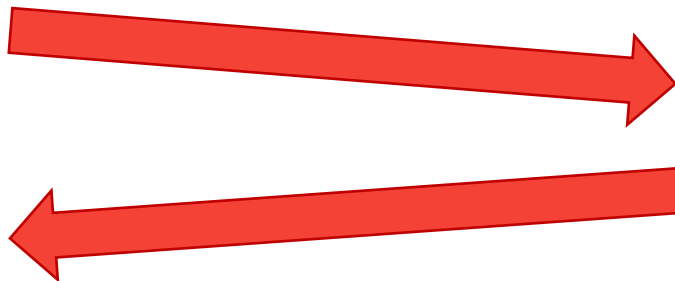


Alt-Svc: h3=":49288";quic="1,1abadaba,51303334"

UDP
PORT

QUIC versions

QUIC



¹ <https://tools.ietf.org/html/rfc7838>

² <https://github.com/MikeBishop/dns-alt-svc>

<https://daniel.haxx.se/blog/2019/03/03/alt-svc-in-curl/>

<https://tools.ietf.org/html/draft-ietf-quic-http-23#section-3.2.1>

⁵ <https://bugs.chromium.org/p/chromium/issues/detail?id=1015101#c1>

4. QUIC and HTTP/3 discovery with alt-svc

TCP

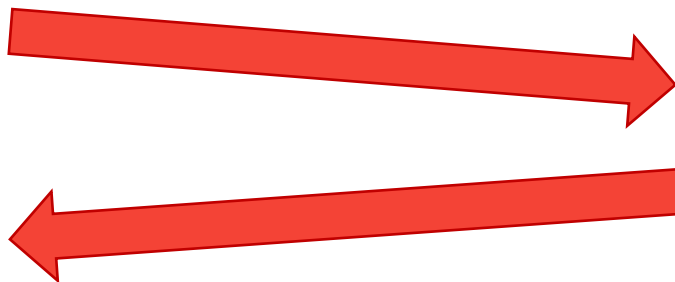


Alt-Svc: h3=":49288";quic="1,1abadaba,51303334"

UDP
PORT

QUIC versions

QUIC



- Need alt-svc cache

¹ <https://tools.ietf.org/html/rfc7838>

² <https://github.com/MikeBishop/dns-alt-svc>

<https://daniel.haxx.se/blog/2019/03/03/alt-svc-in-curl/>

<https://tools.ietf.org/html/draft-ietf-quic-http-23#section-3.2.1>

⁵ <https://bugs.chromium.org/p/chromium/issues/detail?id=1015101#c1>

4. QUIC and HTTP/3 discovery with alt-svc

TCP

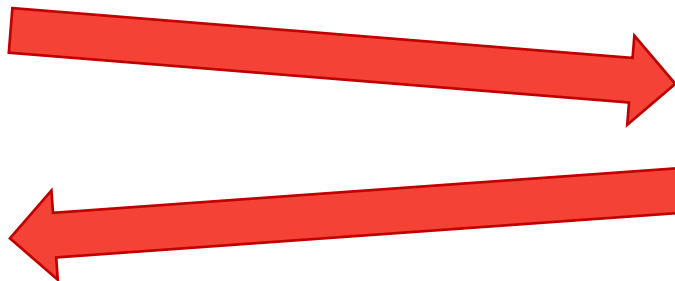


Alt-Svc: h3=":49288";quic="1,1abadaba,51303334"

UDP
PORT

QUIC versions

QUIC



- Need alt-svc cache
- Still needs racing
 - Networks block QUIC

¹ <https://tools.ietf.org/html/rfc7838>

² <https://github.com/MikeBishop/dns-alt-svc>

<https://daniel.haxx.se/blog/2019/03/03/alt-svc-in-curl/>

<https://tools.ietf.org/html/draft-ietf-quic-http-23#section-3.2.1>

⁵ <https://bugs.chromium.org/p/chromium/issues/detail?id=1015101#c1>

4. QUIC and HTTP/3 discovery with alt-svc

TCP

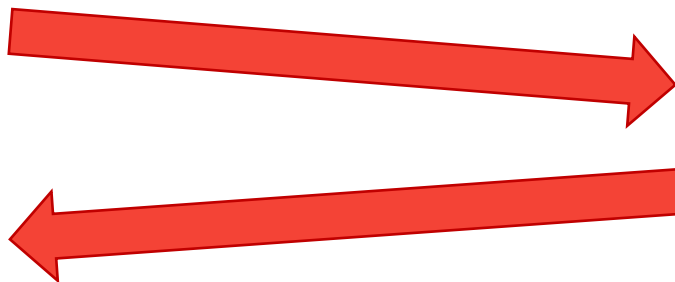


Alt-Svc: h3=":49288";quic="1,1abadaba,51303334"

UDP
PORT

QUIC versions

QUIC



- Need alt-svc cache
- Still needs racing
 - Networks block QUIC
- TCP first
 - Unless we hi-jack DNS!²

¹ <https://tools.ietf.org/html/rfc7838>

² <https://github.com/MikeBishop/dns-alt-svc>

<https://daniel.haxx.se/blog/2019/03/03/alt-svc-in-curl/>

<https://tools.ietf.org/html/draft-ietf-quic-http-23#section-3.2.1>

⁵ <https://bugs.chromium.org/p/chromium/issues/detail?id=1015101#c1>

4. QUIC and HTTP/3 discovery with alt-svc

TCP

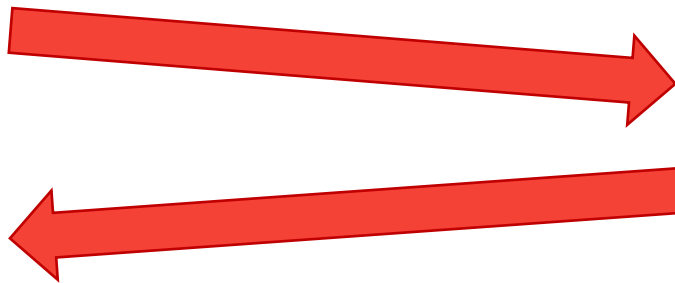


Alt-Svc: h3=":49288";quic="1,1abadaba,51303334"

UDP
PORT

QUIC versions

QUIC



- Need alt-svc cache
- Still needs racing
 - Networks block QUIC
- TCP first
 - Unless we hi-jack DNS!²
- PITA to test locally

¹ <https://tools.ietf.org/html/rfc7838>

² <https://github.com/MikeBishop/dns-alt-svc>

<https://daniel.haxx.se/blog/2019/03/03/alt-svc-in-curl/>

<https://tools.ietf.org/html/draft-ietf-quic-http-23#section-3.2.1>

⁵ <https://bugs.chromium.org/p/chromium/issues/detail?id=1015101#c1>

Types of Headaches

Migraine



Hypertension



Stress



ALT-SVC



5. Debugging QUIC and HTTP/3

capture1 [Wireshark 1.6.2]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	173.194.72.125	192.168.0.4	TLSv1	103	Application Data
2	0.000125	192.168.0.4	173.194.72.125	TCP	66	45955 > https [ACK] Seq=1 Ack=38 Win=2230 Len=0 TSval=114955745 TSecr=47235863
3	12.700958	192.168.0.4	192.168.0.7	TCP	74	35795 > 5001 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=114958921 TSecr=0
4	12.703503	IntelCor_bf:0d:24	Broadcast	ARP	42	Who has 192.168.0.4? Tell 192.168.0.7
5	12.703548	GemtekTe_8c:ae:6d	IntelCor_bf:0d:24	ARP	42	192.168.0.4 is at 00:21:00:8c:ae:6d
6	12.706336	192.168.0.7	192.168.0.4	TCP	66	5001 > 35795 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM=1
7	12.706433	192.168.0.4	192.168.0.7	TCP	54	35795 > 5001 [ACK] Seq=1 Ack=1 Win=14608 Len=0
8	12.709152	192.168.0.4	192.168.0.7	TCP	78	35795 > 5001 [PSH, ACK] Seq=1 Ack=1 Win=14608 Len=24
9	12.709315	192.168.0.4	192.168.0.7	TCP	1514	35795 > 5001 [ACK] Seq=25 Ack=1 Win=14608 Len=1460
10	12.709363	192.168.0.4	192.168.0.7	TCP	1514	35795 > 5001 [ACK] Seq=1485 Ack=1 Win=14608 Len=1460
11	12.709390	192.168.0.4	192.168.0.7	TCP	1514	35795 > 5001 [ACK] Seq=2945 Ack=1 Win=14608 Len=1460
12	12.709414	192.168.0.4	192.168.0.7	TCP	1514	35795 > 5001 [ACK] Seq=4405 Ack=1 Win=14608 Len=1460
13	12.709437	192.168.0.4	192.168.0.7	TCP	1514	35795 > 5001 [ACK] Seq=5865 Ack=1 Win=14608 Len=1460

Frame 9: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)

Ethernet II, Src: GemtekTe_8c:ae:6d (00:21:00:8c:ae:6d), Dst: IntelCor_bf:0d:24 (00:27:10:bf:0d:24)

Internet Protocol Version 4, Src: 192.168.0.4 (192.168.0.4), Dst: 192.168.0.7 (192.168.0.7)

Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
Total Length: 1500
Identification: 0xdbd6 (56278)
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 64
Protocol: TCP (6)
Header checksum: 0xd7e9 [correct]
Source: 192.168.0.4 (192.168.0.4)
Destination: 192.168.0.7 (192.168.0.7)

Transmission Control Protocol, Src Port: 35795 (35795), Dst Port: 5001 (5001), Seq: 25, Ack: 1, Len: 1460

Source port: 35795 (35795)
Destination port: 5001 (5001)
[Stream index: 1]
Sequence number: 25 (relative sequence number)
[Next sequence number: 1485 (relative sequence number)]
Acknowledgement number: 1 (relative ack number)
Header length: 20 bytes
Flags: 0x10 (ACK)
Window size value: 913
[calculated window size: 14608]

0000 00 27 10 bf 0d 24 00 21 00 8c ae 6d 08 00 45 00 ...\$.! ...m..E.
0010 05 dc db d6 40 00 40 06 d7 e9 c0 a8 00 04 c0 a8 ...@.@..
0020 00 07 8b d3 13 89 cc 35 f9 b3 19 0d 85 b3 50 105P.
0030 03 91 a6 1b 00 00 00 00 00 00 00 00 01 00 00
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0210 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0220 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0230 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0240 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0250 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0260 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0270 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0280 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0290 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
02a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
02b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
02c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
02d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
02e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
02f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0310 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0320 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0330 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0340 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0350 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0360 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0370 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0380 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0390 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
03a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
03b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
03c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
03d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
03e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
03f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0410 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0420 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0430 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0440 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0450 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0460 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0470 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0480 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0490 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
04a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
04b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
04c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
04d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
04e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
04f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0500 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0510 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0520 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0530 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0540 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0550 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0560 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0570 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0580 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0590 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
05a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
05b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
05c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
05d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
05e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
05f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0600 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0610 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0620 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0630 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0640 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0650 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0660 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0670 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0680 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0690 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
06a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
06b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
06c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
06d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
06e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
06f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0700 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0710 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0720 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0730 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0740 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0750 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0760 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0770 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0780 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0790 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
07a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
07b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
07c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
07d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
07e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
07f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0800 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0810 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0820 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0830 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0840 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0850 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0860 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0870 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0880 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0890 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
08a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
08b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
08c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
08d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
08e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
08f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0900 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0910 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0920 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0930 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0940 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0950 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0960 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0970 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0980 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0990 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
09a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
09b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
09c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
09d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
09e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
09f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0a00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0a10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0a20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0a30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0a40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0a50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0a60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0a70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0a80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0a90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0aa0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0ab0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0ac0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0ad0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0ae0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0af0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0b00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0b10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0b20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0b30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0b40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0b50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0b60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0b70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0b80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0b90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0ba0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0bb0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0bc0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0bd0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0be0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0bf0 00 00

5. qlog: structured endpoint logging

```
{
  "event_fields": [
    "time", "group_id", "category", "event", "data"
  ],
  "events": [
    [1553986553579, 0, "transport", "packet_received", {"header": {} }],
    [1553986553580, 0, "recovery", "metrics_updated", {"smoothed_rtt": 85}],
    [1553986553588, 1, "http", "frame_parsed", {"frame_type": "DATA"}],
    [1553986553598, 0, "transport", "packet_sent", {"header": {} }]
  ]
}
```


5. qlog: structured endpoint logging

```
{
  "event_fields": [
    "time", "group_id", "category", "event", "data"
  ],
  "events": [
    [1553986553579, 0, "transport", "packet_received", {"header": {} }],
    [1553986553580, 0, "recovery", "metrics_updated", {"smoothed_rtt": 85}],
    [1553986553588, 1, "http", "frame_parsed", {"frame_type": "DATA"}],
    [1553986553598, 0, "transport", "packet_sent", {"header": {} }]
  ]
}
```

Nine QUIC implementations currently output qlog



mjoras 10:35 PM

@rmarx

we currently have qlog enabled in prod with similar



amounts of events being recorded a day as I quoted before (dozens of billions).

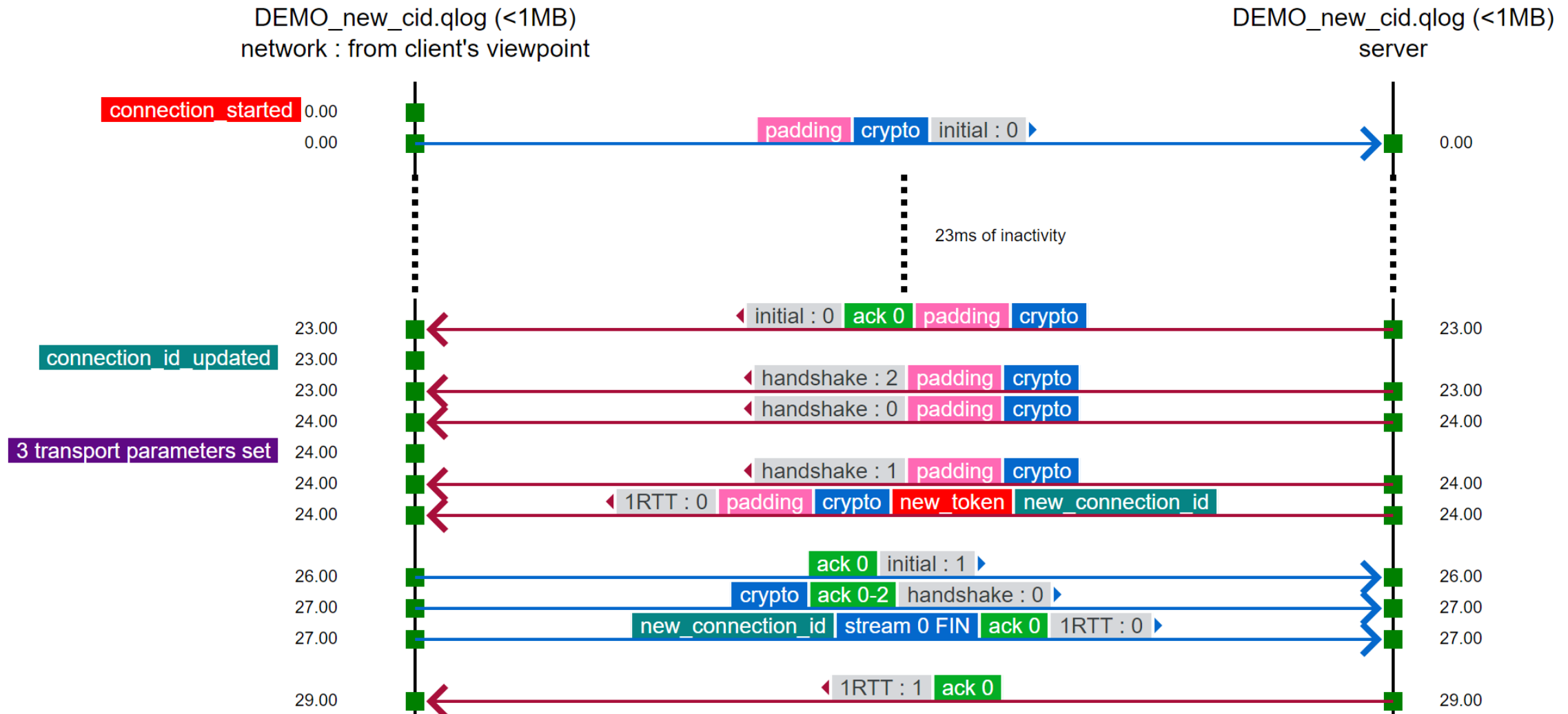
<https://quic.edm.uhasselt.be/>

<https://tools.ietf.org/html/draft-marx-qlog-main-schema-01>

<https://tools.ietf.org/html/draft-marx-qlog-event-definitions-quic-h3-01>



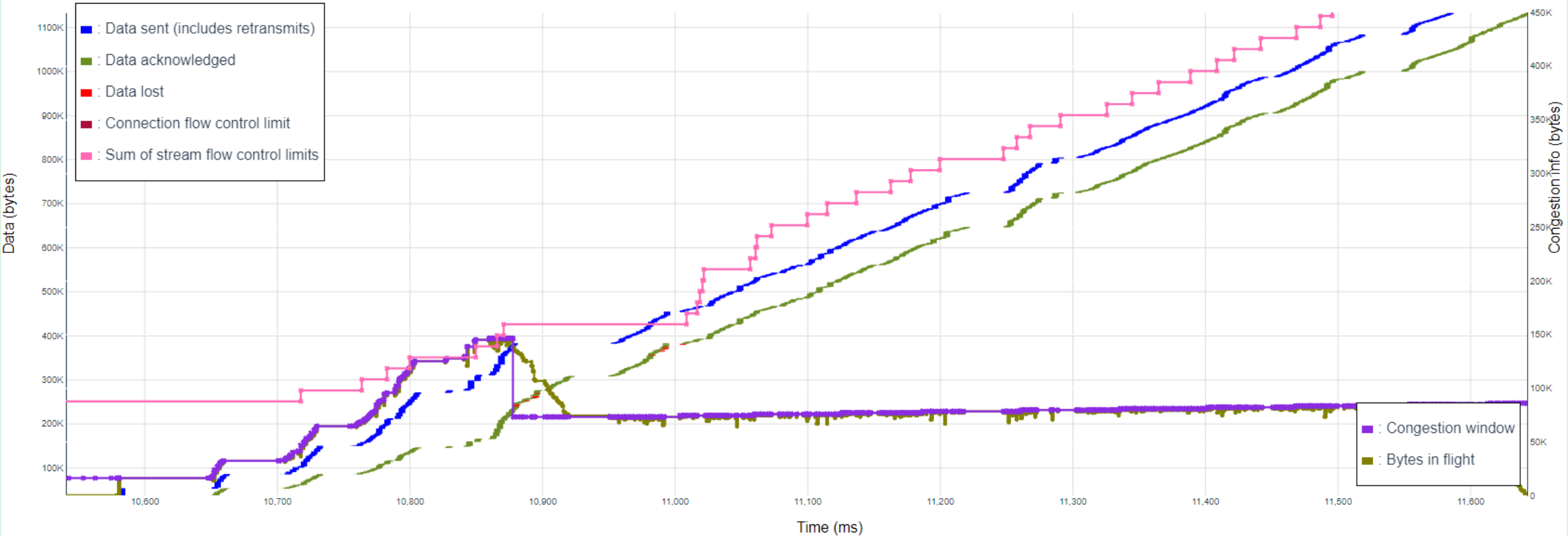
5. qvis: tooling and visualization



<https://qvis.edm.uhasselt.be>

<https://quic.edm.uhasselt.be/>
<https://tools.ietf.org/html/draft-marx-qlog-main-schema-01>
<https://tools.ietf.org/html/draft-marx-qlog-event-definitions-quic-h3-01>

5. qvis: tooling and visualization



<https://qvis.edm.uhasselt.be>

<https://quic.edm.uhasselt.be/>
<https://tools.ietf.org/html/draft-marx-qlog-main-schema-01>
<https://tools.ietf.org/html/draft-marx-qlog-event-definitions-quic-h3-01>

Benefits from all this complexity?

Some

~8% **faster**

Up to -26% at p99



Others

Users don't
care

2-9x CPU needed

Benefits from all this complexity?

Some

~8% **faster**

Up to -26% at p99

Remember

Google and
Facebook
deploy QUIC
at scale

Huge part of internet traffic
today is QUIC

Others

Users don't
care

2-9x CPU needed

<https://arxiv.org/pdf/1910.07729.pdf>

<https://conferences2.sigcomm.org/co-next/2018/slides/epiq-keynote.pdf>

<https://www2.cs.duke.edu/courses/fall18/compsci514/readings/QUIC-sigcomm2017.pdf>

Practical way forward

Experiment now, test in June, deploy end of 2020

Practical way forward

Experiment now, test in June, deploy end of 2020

Use a CDN

- Cloudflare, Fastly, Google and Microsoft : heavily invested
- Akamai : does google QUIC already
- Amazon : also working on –something–

<https://github.com/quicwg/base-drafts/wiki/Implementations>

<https://blog.cloudflare.com/experiment-with-http-3-using-nginx-and-quiche/>

<https://www.zdnet.com/article/cloudflare-google-chrome-and-firefox-add-http3-support/>

Practical way forward

Experiment now, test in June, deploy end of 2020

Use a CDN

- Cloudflare, Fastly, Google and Microsoft : heavily invested
- Akamai : does google QUIC already
- Amazon : also working on –something–

Server support is coming

- nginx announced (*for now: cloudflare patch*)
- LiteSpeed, NodeJS, aioquic open source

Browser support is coming

- Chrome, Edge, Firefox in 'Canary'
- Safari in progress

<https://github.com/quicwg/base-drafts/wiki/Implementations>

<https://blog.cloudflare.com/experiment-with-http-3-using-nginx-and-quiche/>

<https://www.zdnet.com/article/cloudflare-google-chrome-and-firefox-add-http3-support/>



GO FORTH and **REPRODUCE!**

Please provide feedback @programmingart

Cyberconflict: A new era of war, sabotage, and fear

Sarah Connor

9:55am-10:10am Wednesday, March 27, 2019

Location: Ballroom

Secondary topics: Security and Privacy

[Rate This Session](#)

[See passes & pricing](#)

[Add to Your Schedule](#)
[Add Comment or Question](#)

We're living in a new era of constant sabotage, misinformation, and fear, in which everyone is a target, and you're often the collateral damage in a growing conflict among states. From crippling infrastructure to sowing discord and doubt, cyber is now the weapon of choice for democracies, dictators, and terrorists.

Sarah Connor explains how the rise of cyberweapons has transformed geopolitics like nothing since the invention of the atomic bomb. Moving from the White House Situation Room to the dens of Chinese, Russian, North Korean, and Iranian hackers to the boardrooms of Silicon Valley, David reveals a world coming face-to-face with the perils of technological revolution—a conflict that the United States helped start when it began using cyberweapons against Iranian nuclear plants and North Korean missile launches. But now we find ourselves in a conflict we're uncertain how to control, as our adversaries exploit vulnerabilities in our hyperconnected nation and we struggle to figure out how to deter these complex, short-of-war attacks.

Sarah Connor

The New York Times

Sarah Connor is the national security correspondent for the *New York Times* as well as a national security and political contributor for CNN and a frequent guest on *CBS This Morning*, *Face the Nation*, and many PBS shows.



Session page on conference website

[Attending](#) [Notes](#) [Remove](#)

Cyberconflict: A new era of war, sabotage, and fear

9:55 AM - 10:10 AM, Wed, Mar 27, 2019

Speakers



Sarah Connor
National Security Correspondent
The New York Times



Sarah Connor explains how the rise of cyberweapons has transformed geopolitics like nothing since the invention of the atomic bomb. From crippling infrastructure to sowing discord and doubt, cyber is now the weapon of choice for democracies, dictators, and terrorists.

[SESSION EVALUATION](#)

O'Reilly Events App

Image sources

- <https://www.wallpaperflare.com/terminator-genisys-t-800-copy-space-black-background-close-up-wallpaper-qyrlz>
- <https://wall.alphacoders.com/big.php?i=400118>
- <https://http3-explained.haxx.se/en/why-tcp-hol.html>
- <https://stackoverflow.com/questions/30818925/tcp-congestion-control-fast-recovery-in-graph>
- <https://www.incapsula.com/cdn-guide/glossary/reverse-proxy.html>
- <https://twitter.com/AndyDavies/status/1065916677408346112>
- <https://uk.movies.yahoo.com/terminator-2-3d-interview-robert-patrick-wants-return-t1000-exclusive-123420663.html>
- <https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-distribution-mode>
- <http://makertech.dk/3-games-in-6-months-what-i-learned-and-why-i-quit/>
- https://www.reddit.com/r/Terminator/comments/9bb3kf/happy_judgment_day/
- <https://www.techrepublic.com/blog/linux-and-open-source/two-simple-filters-for-wireshark-to-analyze-tcp-and-udp-traffic/>
- [https://en.wikipedia.org/wiki/Sarah_Connor_\(Terminator\)](https://en.wikipedia.org/wiki/Sarah_Connor_(Terminator))
- <https://www.cinemablend.com/news/2467164/is-terminator-dark-fate-wrapping-up-sarah-connors-story-for-good>
- <https://tenor.com/search/terminator-gatling-gun-gifs>
- https://hitek.fr/actualite/terminator-dark-fate-retour-edward-furlong-role-john-connor_20152
- <https://i.ytimg.com/vi/rmmF11TKueA/maxresdefault.jpg>
- <http://static.comicvine.com/uploads/original/11114/111142257/4907278-5635399158-termi.jpg>

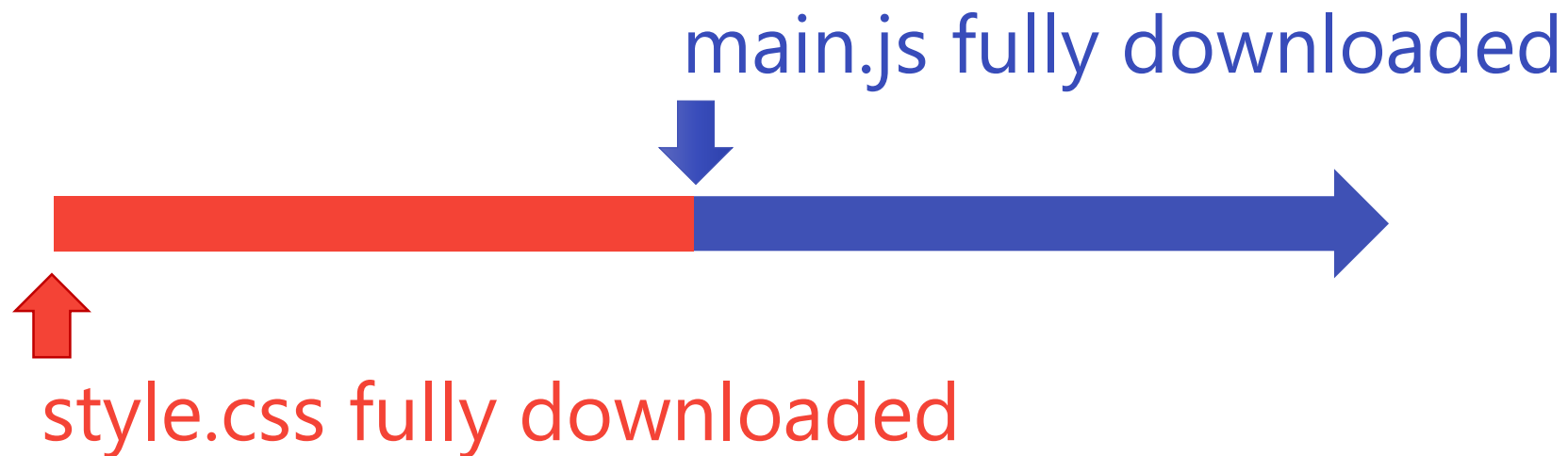


03

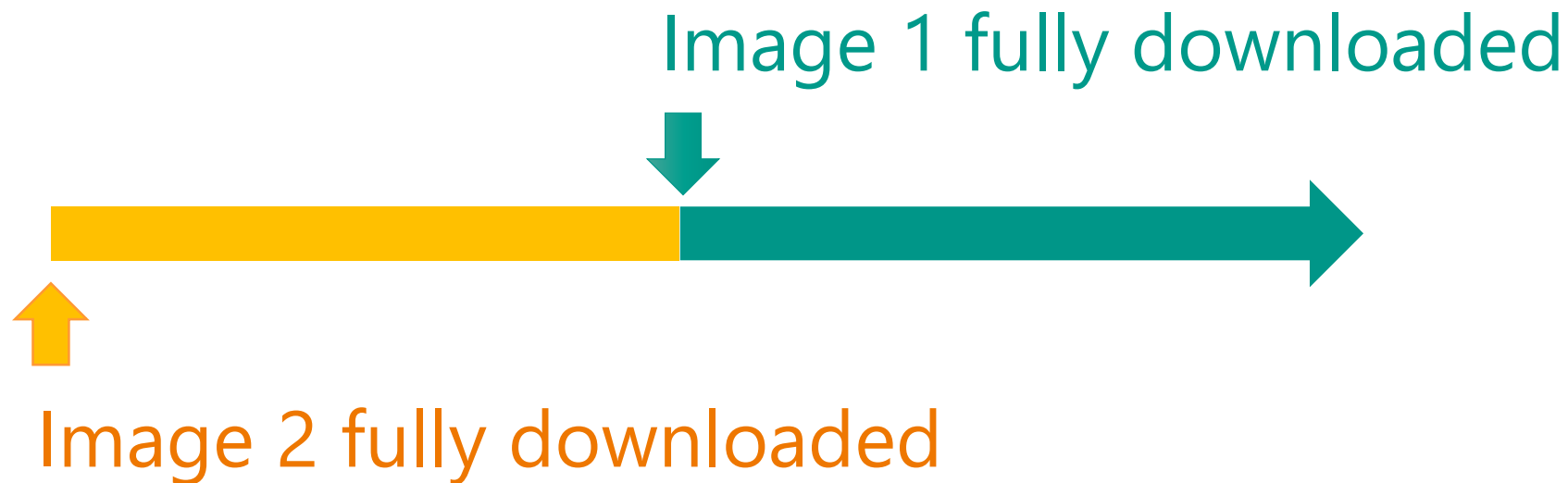
Extra slides

- Too much content, too little time

Prioritization matters



Prioritization matters



Other HTTP/2 (implementation) issues

- Mixed content (HTTP to HTTPS)
- Coalescing connections can be flaky
- Support from intermediaries/libraries (e.g., proxies, caches, native libraries)
- ...

<https://jakearchibald.com/2017/h2-push-tougher-than-i-thought/>

<https://daniel.haxx.se/blog/2016/08/18/http2-connection-coalescing/>

<https://tweakers.net/reviews/4555/3/tweakers-stapt-over-op-https-mixed-content.html>

<https://medium.com/bbc-design-engineering/http-2-is-easy-just-turn-it-on-34baad2d1fb1>

Google QUIC != QUIC + HTTP/3

Been around
for **years**

Mainly Google
and Akamai

Being
standardized
by the IETF

Same concepts,
**-very- different
execution**



A free PowerPoint Template made by Slidor.

VISIT US >