COMMUNITY
THE ASF CONFERENCE
CODE

HTTP/3 where are we now? State of the art in our servers.

Jean-Frederic Clere @jfclere

What I will cover

- HTTP/2
  - HTTP/2 and ALPN
- HTTP/3
- Servers
  - Apache HTTPD
  - Tomcat
  - Traffic server
  - openssl demo server
- Demos
- Questions?

Who I am

Jean-Frederic Clere

Red Hat

Years writing JAVA code and server software

Tomcat committer since 2001

Doing OpenSource since 1999

Cyclist/Runner etc

Lived 15 years in Spain (Barcelona)

Now in Neuchâtel (CH)

Why HTTP/2

- HTTP/1.1: June 1999 (RFC 2616)
  - 1999:
    - 1 page ~ 1kB HTML
  - 2019:
    - 1 page ~ 3MB HTML + IMAGES + JS + CSS etc
- Protocol:
  - Not adapted / inefficient / etc

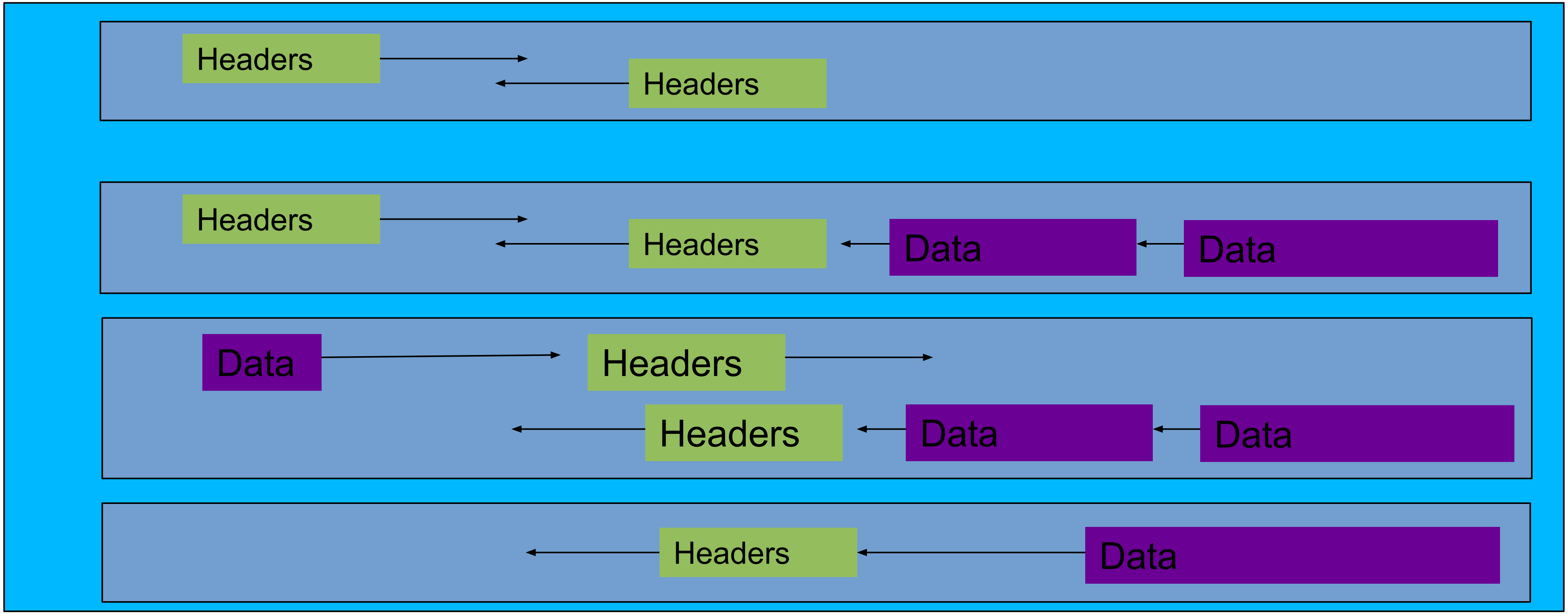
HTTP/2 general

- HTTP/2:
  - Binary
  - Frame
  - Multiplex
  - Based on SPDY
  - TLS everywhere:
    - Browser use https and strong ciphers
  - No forward proxy
  - h2c: Clear text only with reverse proxy (proxy to back-end server)

HTTP/2 general

- Two specifications:
  - Hypertext Transfer Protocol version 2 - RFC 7540
  - HPACK - Header Compression for HTTP/2 - RFC 7541
- By the Internet Engineering Task Force
- ALPN   Application-Layer Protocol Negotiation - RFC 7301

HTTP/2 Multiplexed



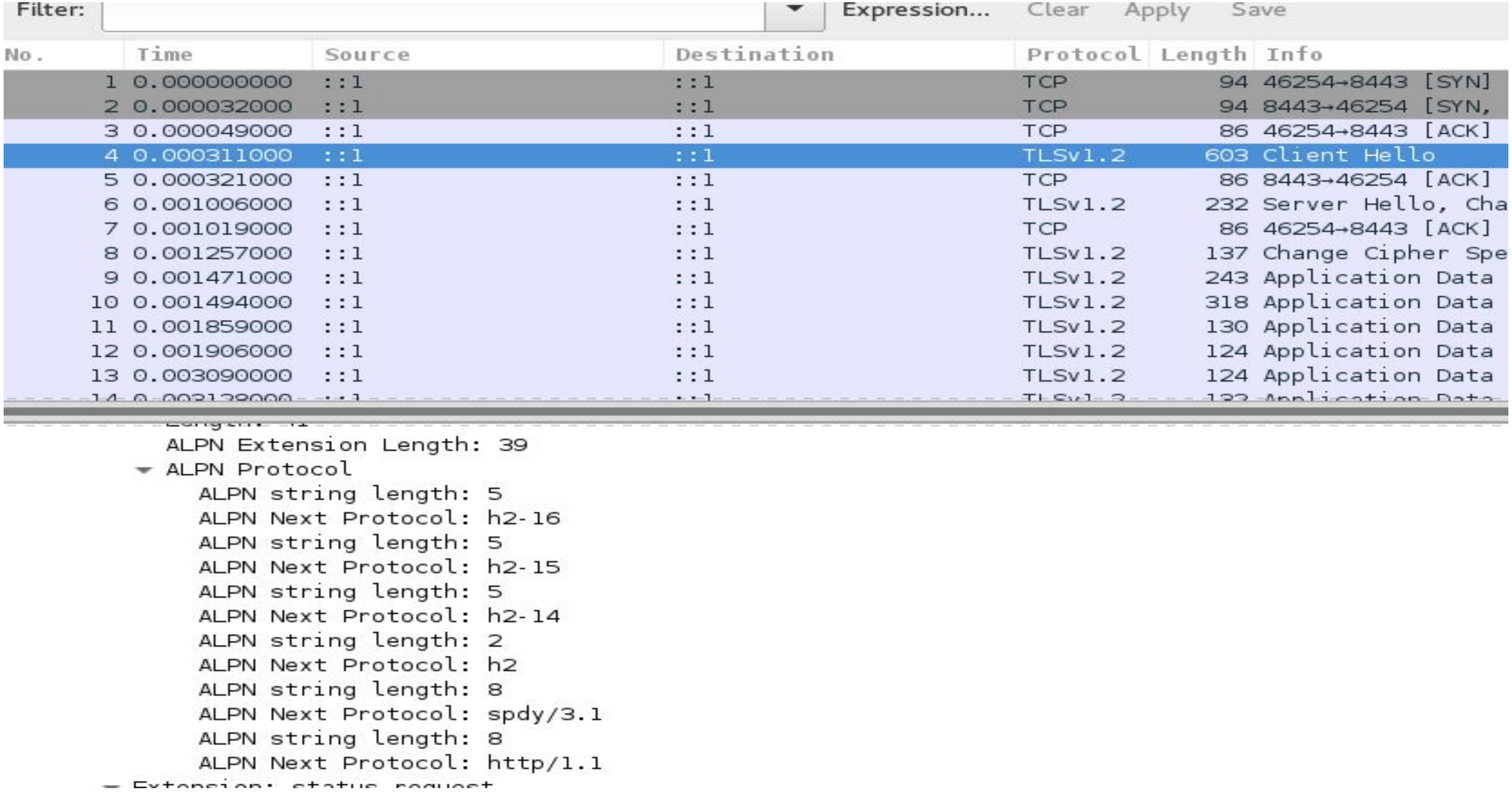
HTTP/2 : more

- HTTP headers compression
  - ~ 80 % save
- Request priority
  - Both sides
- Server Push
  - Prevent round trip to get element of a page
  - Faster / better rendering on browsers.

HTTP/2 With Browsers

- Browser with HTTP/2 and TLS
  - FireFox 34
  - Chrome 40 (with ALPN before was NPN)
  - IE 11
  - Opera and Safari 9
- → go for it now!

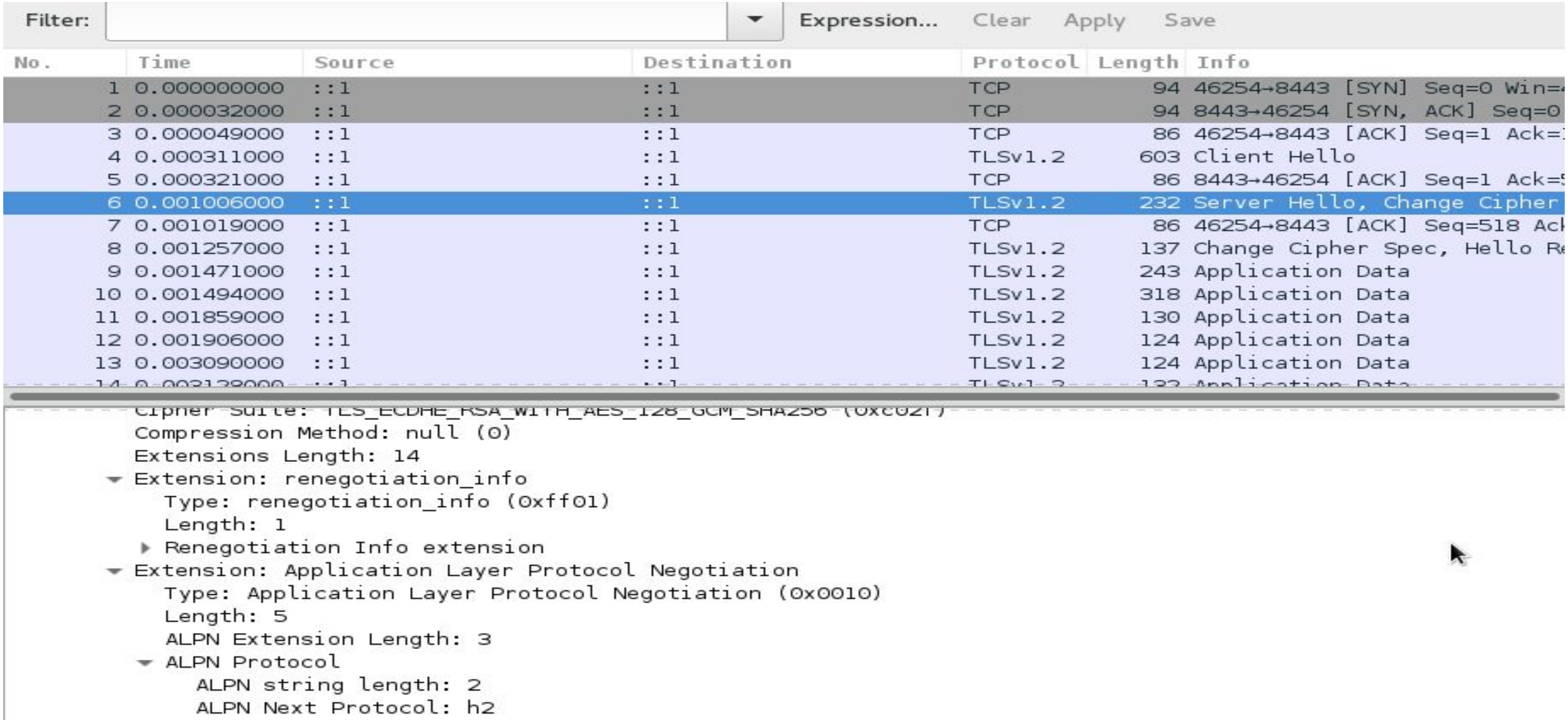
ALPN Client Hello (Firefox)



```
No.   Time           Source   Destination   Protocol  Length  Info
    1 0.000000000    ::1      ::1           TCP           94  46254→8443 [SYN]
    2 0.000032000    ::1      ::1           TCP           94  8443→46254 [SYN,
    3 0.000049000    ::1      ::1           TCP           86  46254→8443 [ACK]
    4 0.000311000    ::1      ::1           TLSv1.2      603  Client Hello
    5 0.000321000    ::1      ::1           TCP           86  8443→46254 [ACK]
    6 0.001006000    ::1      ::1           TLSv1.2      232  Server Hello, Cha
    7 0.001019000    ::1      ::1           TCP           86  46254→8443 [ACK]
    8 0.001257000    ::1      ::1           TLSv1.2      137  Change Cipher Spe
    9 0.001471000    ::1      ::1           TLSv1.2      243  Application Data
   10 0.001494000    ::1      ::1           TLSv1.2      318  Application Data
   11 0.001859000    ::1      ::1           TLSv1.2      130  Application Data
   12 0.001906000    ::1      ::1           TLSv1.2      124  Application Data
   13 0.003090000    ::1      ::1           TLSv1.2      124  Application Data
   14 0.003128000    ::1      ::1           TLSv1.2      123  Application Data
```

```
      Length: 41
      ALPN Extension Length: 39
    ▾ ALPN Protocol
        ALPN string length: 5
        ALPN Next Protocol: h2-16
        ALPN string length: 5
        ALPN Next Protocol: h2-15
        ALPN string length: 5
        ALPN Next Protocol: h2-14
        ALPN string length: 2
        ALPN Next Protocol: h2
        ALPN string length: 8
        ALPN Next Protocol: spdy/3.1
        ALPN string length: 8
        ALPN Next Protocol: http/1.1
  ▾ Extension: status_request
```

ALPN Server Hello (tomcat)



```
No.     Time          Source      Destination   Protocol  Length  Info
      1 0.000000000   ::1         ::1           TCP           94  46254→8443 [SYN] Seq=0 Win=
      2 0.000032000   ::1         ::1           TCP           94  8443→46254 [SYN, ACK] Seq=0
      3 0.000049000   ::1         ::1           TCP           86  46254→8443 [ACK] Seq=1 Ack=
      4 0.000311000   ::1         ::1           TLSv1.2      603  Client Hello
      5 0.000321000   ::1         ::1           TCP           86  8443→46254 [ACK] Seq=1 Ack=
      6 0.001006000   ::1         ::1           TLSv1.2      232  Server Hello, Change Cipher
      7 0.001019000   ::1         ::1           TCP           86  46254→8443 [ACK] Seq=518 Ack
      8 0.001257000   ::1         ::1           TLSv1.2      137  Change Cipher Spec, Hello Re
      9 0.001471000   ::1         ::1           TLSv1.2      243  Application Data
     10 0.001494000   ::1         ::1           TLSv1.2      318  Application Data
     11 0.001859000   ::1         ::1           TLSv1.2      130  Application Data
     12 0.001906000   ::1         ::1           TLSv1.2      124  Application Data
     13 0.003090000   ::1         ::1           TLSv1.2      124  Application Data
     14 0.003128000   ::1         ::1           TLSv1.2      133  Application Data
```

```
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
    Compression Method: null (0)
    Extensions Length: 14
  ▾ Extension: renegotiation_info
      Type: renegotiation_info (0xff01)
      Length: 1
    ▸ Renegotiation Info extension
  ▾ Extension: Application Layer Protocol Negotiation
      Type: Application Layer Protocol Negotiation (0x0010)
      Length: 5
      ALPN Extension Length: 3
    ▾ ALPN Protocol
        ALPN string length: 2
        ALPN Next Protocol: h2
```

HTTP/2

- HTTP/2:
  - TCP/IP.
  - “safer” crypto is good but expensive.
  - No need to rewrite application to get the gains.

HTTP/2 : GO FOR IT

Then Why HTTP/3?

- TCP/IP:
  - Windows acks: 1 packet lost → all the channels blocked.
- UPD:
  - Channels are independent.
  - Need higher protocol level to insure integrity.
  - Packets might not be received in order.
- Security:
  - Need a patched version of OpenSSL (and use TLS-1.3)
  - UDP: cloud → no… but DNS → used everywhere!

HTTP/3 (RFC 9114 published June 2022)

- Use QUIC / TLS-1.3 / UDP
- To “transport” HTTP/1.1 like HTTP/2
- Initial connection TCP + Alt-Svc or HTTP/2
  - Response Alt-Svc: h3=":56666":
  - HTTP/2   ALTSVC frame
- problems:
  - UDP ports closed
  - UDP slower than TCP in Kernels
  - Needs extra CPU (?)
- Specifications:
  - RC 9114

Features: HTTP/2 vs HTTP/3

	HTTP/2	HTTP/3
Transport	TCP	UPD/QUIC
Streams	HTTP/2	QUIC
Clear text	yes (h2c: reverse proxy)	no
Independent streams	no	yes
Header compression	HPACK	QPACK
Server push	yes	yes
Early data	no	yes
0-RTT handshake	no (TLS-1.2)	Yes (TLS-1.3+)

HTTP/3 implementations

- quiche:
  - https://docs.quic.tech/quiche/
- Curl: https://curl.se/docs/http3.html
  - ngtcp2 (nghttp3/ngtcp2, patched openssl or GnuTLS)
  - quiche
  - msh3
  - In experimental at build time.
- Browser: chrome / firefox (active by default: Apr 2021).

HTTP/3 in our servers:

- Apache Tomcat: need time (wait for HTTP/3 streams?)
- Apache HTTPD: need time (probably like http/2)
- Traffic Server: in the 9.1.x experimental (need patched openssl)
  - See ATS docs / curl docs
  - 11-dev: boringSSL and quiche

TrafficServer / Configuration

- records.yaml
  - traffic_ctl config set proxy.config.http.server_ports "4443:quic" -c records.yaml
  - traffic_ctl config set proxy.config.udp.threads 1 -c records.yaml
  - traffic_ctl config set proxy.config.quic.initial_max_streams_bidi_in 100000
  - traffic_ctl config set proxy.config.quic.initial_max_streams_bidi_out 100000
- ssl_multicert.config:
  - **dest_ip=* ssl_cert_name=newcert.pem ssl_key_name=newkey.txt.pem**
- remap.config:
  - **map / http://127.0.0.1:8080**

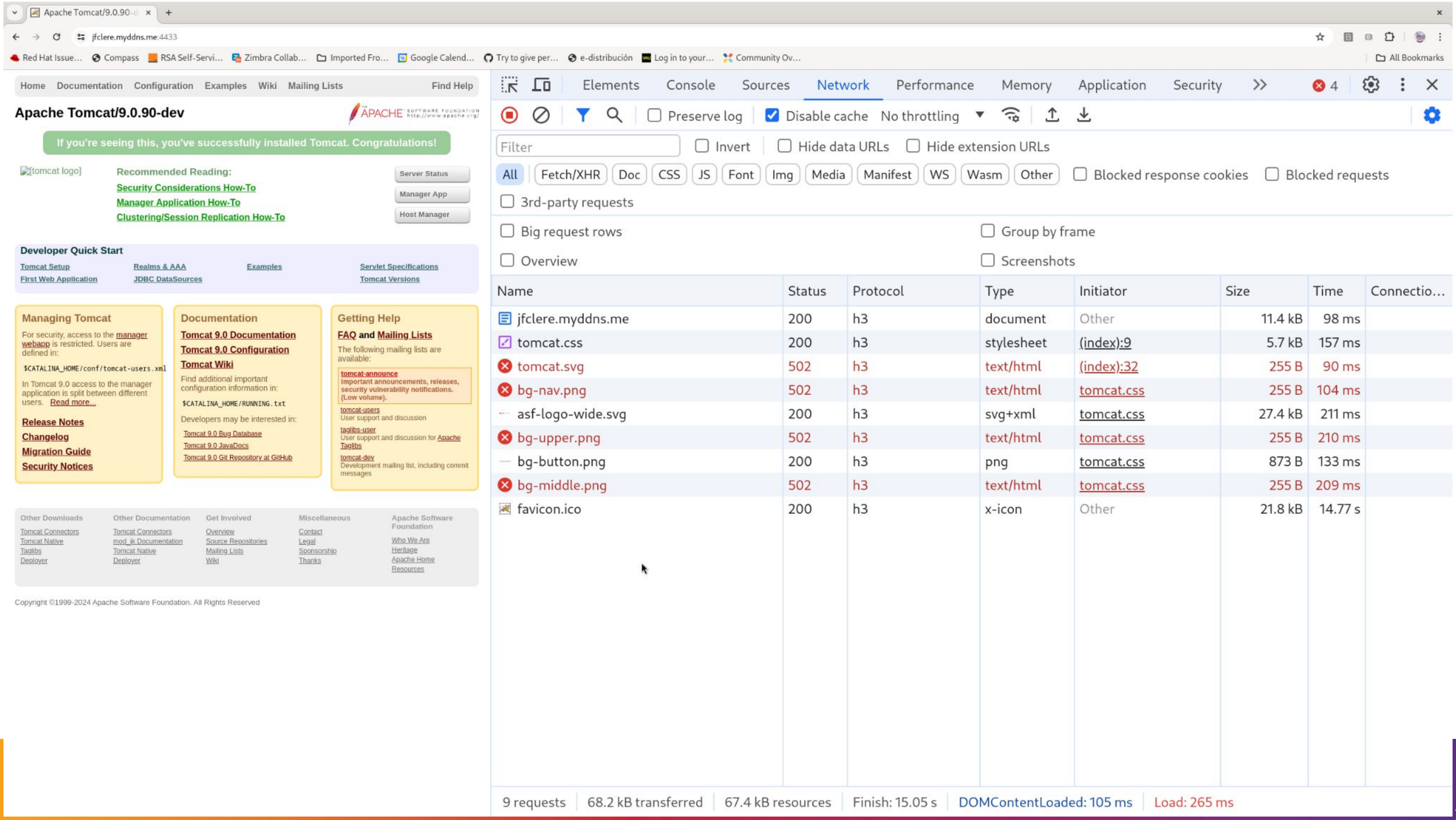
TrafficServer / H3 Demo

- Uses tomcat as backend
- Uses http/1.1 tomcat nio connector on 8080 as back-end.
- Uses Apache HTTPD https + mod_header to create the alt-svc

TrafficServer / Demo

- https://jfclere.myddns.me:4433/
- Response HTTP/1.1 (HTTP/2) header alt-svc
- alt-svc: h3=":4433"; ma=60; h3=":4433"; persist=1
- H3 (HTTP/3)
- ma=60 seconds = 1 minute.
- Next requests → HTTP/3

TrafficServer / Demo



Apache Tomcat/9.0.90-d

jfclere.myddns.me:4433

Red Hat Issue… · Compass · RSA Self-Servi… · Zimbra Collab… · Imported Fro… · Google Calend… · Try to give per… · e-distribución · Log in to your… · Community Ov… · All Bookmarks

Home · Documentation · Configuration · Examples · Wiki · Mailing Lists · Find Help

Apache Tomcat/9.0.90-dev

If you're seeing this, you've successfully installed Tomcat. Congratulations!

[tomcat logo]

Recommended Reading:

- Security Considerations How-To
- Manager Application How-To
- Clustering/Session Replication How-To

Server Status · Manager App · Host Manager

Developer Quick Start

Tomcat Setup · First Web Application · Realms & AAA · JDBC DataSources · Examples · Servlet Specifications · Tomcat Versions

Managing Tomcat

For security, access to the manager webapp is restricted. Users are defined in:

```
$CATALINA_HOME/conf/tomcat-users.xml
```

In Tomcat 9.0 access to the manager application is split between different users. Read more...

Release Notes

Changelog

Migration Guide

Security Notices

Documentation

Tomcat 9.0 Documentation

Tomcat 9.0 Configuration

Tomcat Wiki

Find additional important configuration information in:

```
$CATALINA_HOME/RUNNING.txt
```

Developers may be interested in:

- Tomcat 9.0 Bug Database
- Tomcat 9.0 JavaDocs
- Tomcat 9.0 Git Repository at GitHub

Getting Help

FAQ and Mailing Lists

The following mailing lists are available:

tomcat-announce
Important announcements, releases, security vulnerability notifications. (Low volume).

tomcat-users
User support and discussion

taglibs-user
User support and discussion for Apache Taglibs

tomcat-dev
Development mailing list, including commit messages

Other Downloads	Other Documentation	Get Involved	Miscellaneous	Apache Software Foundation
Tomcat Connectors	Tomcat Connectors	Overview	Contact	Who We Are
Tomcat Native	mod_jk Documentation	Source Repositories	Legal	Heritage
Taglibs	Tomcat Native	Mailing Lists	Sponsorship	Apache Home
Deployer	Deployer	Wiki	Thanks	Resources

Copyright ©1999-2024 Apache Software Foundation. All Rights Reserved

□ Preserve log ☑ Disable cache No throttling

Filter □ Invert □ Hide data URLs □ Hide extension URLs

All · Fetch/XHR · Doc · CSS · JS · Font · Img · Media · Manifest · WS · Wasm · Other □ Blocked response cookies □ Blocked requests

□ 3rd-party requests

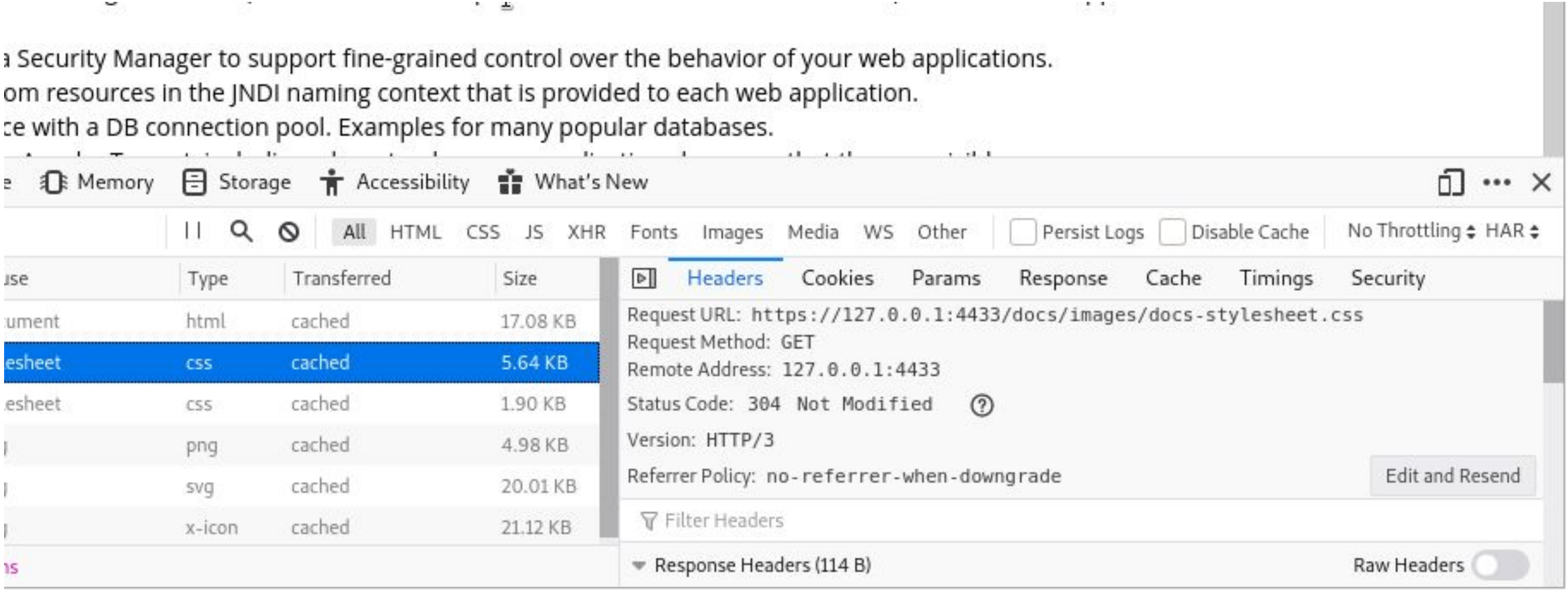
□ Big request rows □ Group by frame

□ Overview □ Screenshots

Name	Status	Protocol	Type	Initiator	Size	Time	Connectio…
jfclere.myddns.me	200	h3	document	Other	11.4 kB	98 ms	
tomcat.css	200	h3	stylesheet	(index):9	5.7 kB	157 ms	
tomcat.svg	502	h3	text/html	(index):32	255 B	90 ms	
bg-nav.png	502	h3	text/html	tomcat.css	255 B	104 ms	
asf-logo-wide.svg	200	h3	svg+xml	tomcat.css	27.4 kB	211 ms	
bg-upper.png	502	h3	text/html	tomcat.css	255 B	210 ms	
bg-button.png	200	h3	png	tomcat.css	873 B	133 ms	
bg-middle.png	502	h3	text/html	tomcat.css	255 B	209 ms	
favicon.ico	200	h3	x-icon	Other	21.8 kB	14.77 s	

9 requests · 68.2 kB transferred · 67.4 kB resources · Finish: 15.05 s · DOMContentLoaded: 105 ms · Load: 265 ms

TrafficServer / Demo



a Security Manager to support fine-grained control over the behavior of your web applications.
om resources in the JNDI naming context that is provided to each web application.
ce with a DB connection pool. Examples for many popular databases.

☐ Persist Logs ☐ Disable Cache

use	Type	Transferred	Size
ument	html	cached	17.08 KB
esheet	css	cached	5.64 KB
esheet	css	cached	1.90 KB
	png	cached	4.98 KB
	svg	cached	20.01 KB
	x-icon	cached	21.12 KB

ns

Request URL: `https://127.0.0.1:4433/docs/images/docs-stylesheet.css`
Request Method: GET
Remote Address: 127.0.0.1:4433
Status Code: 304 Not Modified
Version: HTTP/3
Referrer Policy: no-referrer-when-downgrade

Response Headers (114 B)

HTTP/3 more info:

- Playing with browsers:
  - Interop matrix
  - H3 activated by default since 2021 in Firefox/Chrome
- OpenSSL 3.3.x (3.2.x has a client QUIC API)

HTTP/3 openssl + nghttp3

- Basic client: (see also openssl one)
  - just testing.
  - using nghttp3 main. big callback and few functions
  - using openssl master to provide the QUIC layer.

```
SSL *new_ssl = SSL_accept_stream(s, 0);
```

HTTP/3 openssl + nghttp3

- Basic server:

  just testing.

  using nghttp3 main. big callback and few functions

  using openssl feature/quic-server to provide the QUIC layer.

HTTP/3 ready?

- Conclusion:
  - Not more a draft, last draft was H3-34.
  - UDP versus TCP.
  - Needs forked version of openssl… (0-RTT).
  - Or BoringSSL.
  - No need to rewrite application to get the gains.

HTTP/3 : wait

Questions?

COMMUNITY
THE ASF CONFERENCE
CODE

- jfclere@gmail.com
- users@tomcat.apache.org
- users@httpd.apache.org
- users@trafficserver.apache.org
- https://http2.github.io/ https://github.com/ngtcp2/nghttp3.git
- Client/Server: https://github.com/jfclere/openssl-h3-examples
- HTTP/3 see curl docs: http3-explained by Daniel
- More on HTP/3: https://github.com/jfclere/CoC23/tree/main/h3