TLS 1.3 Client Measurements

Tommy Pauly (tpauly@apple.com)

MAPRG
IETF 105, July 2019, Montreal

TLS 1.3 Rollout

RFC 8446 published in August 2018

TLS 1.3 enabled by default in iOS 12.2 and macOS 10.14.4 (March 2019)

Anecdotally, many server deployments have recently deployed TLS 1.3 or are in the midst of ramping up support

Questions

How much server adoption of TLS 1.3 do we see from the perspective of clients?

Does TLS 1.3 provide the expected performance benefits (by reducing round trips)?

Methodology

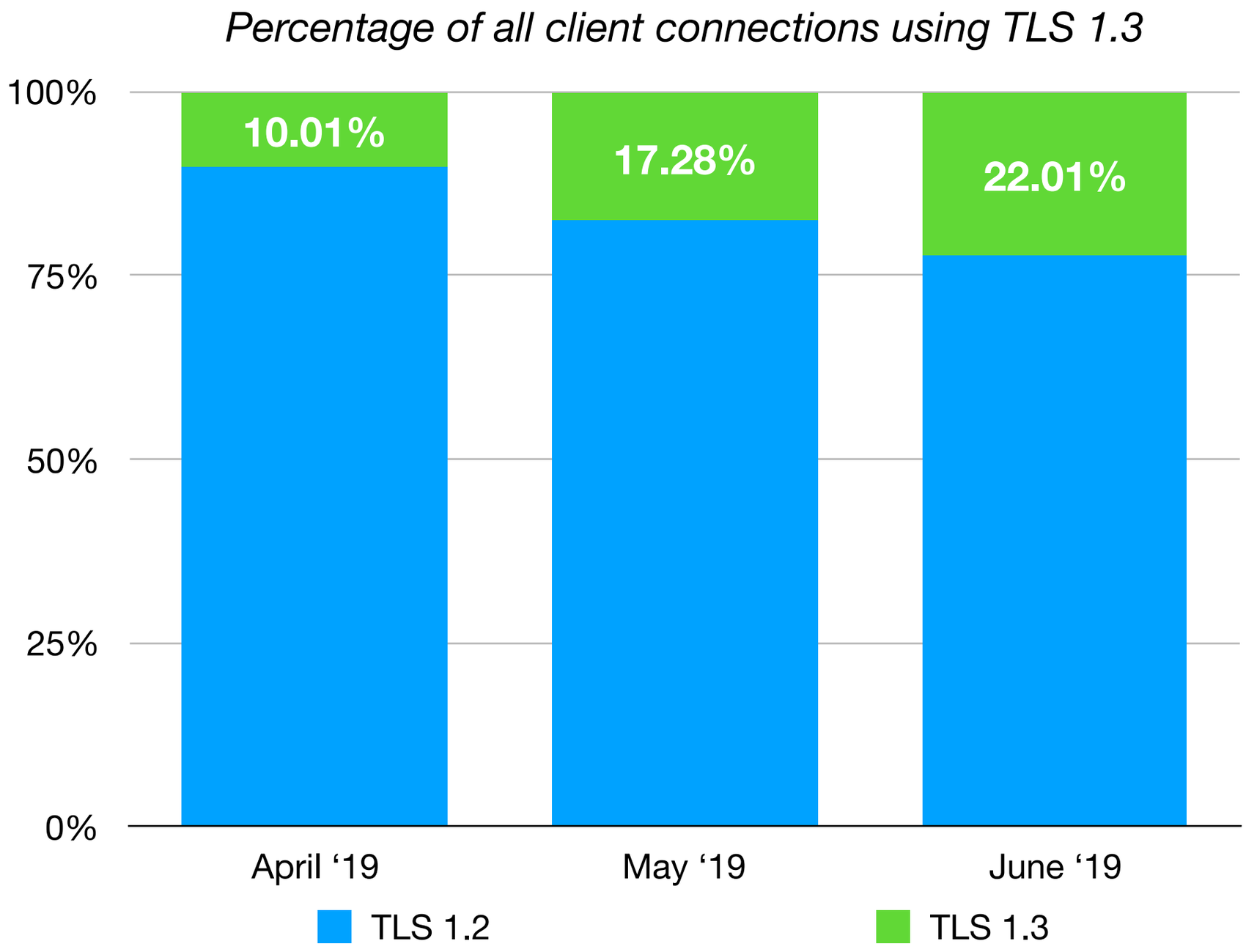
Metrics collected per-TLS connection

- TLS version
- TLS handshake time
- ALPN value
- Address family (IPv4/IPv6)

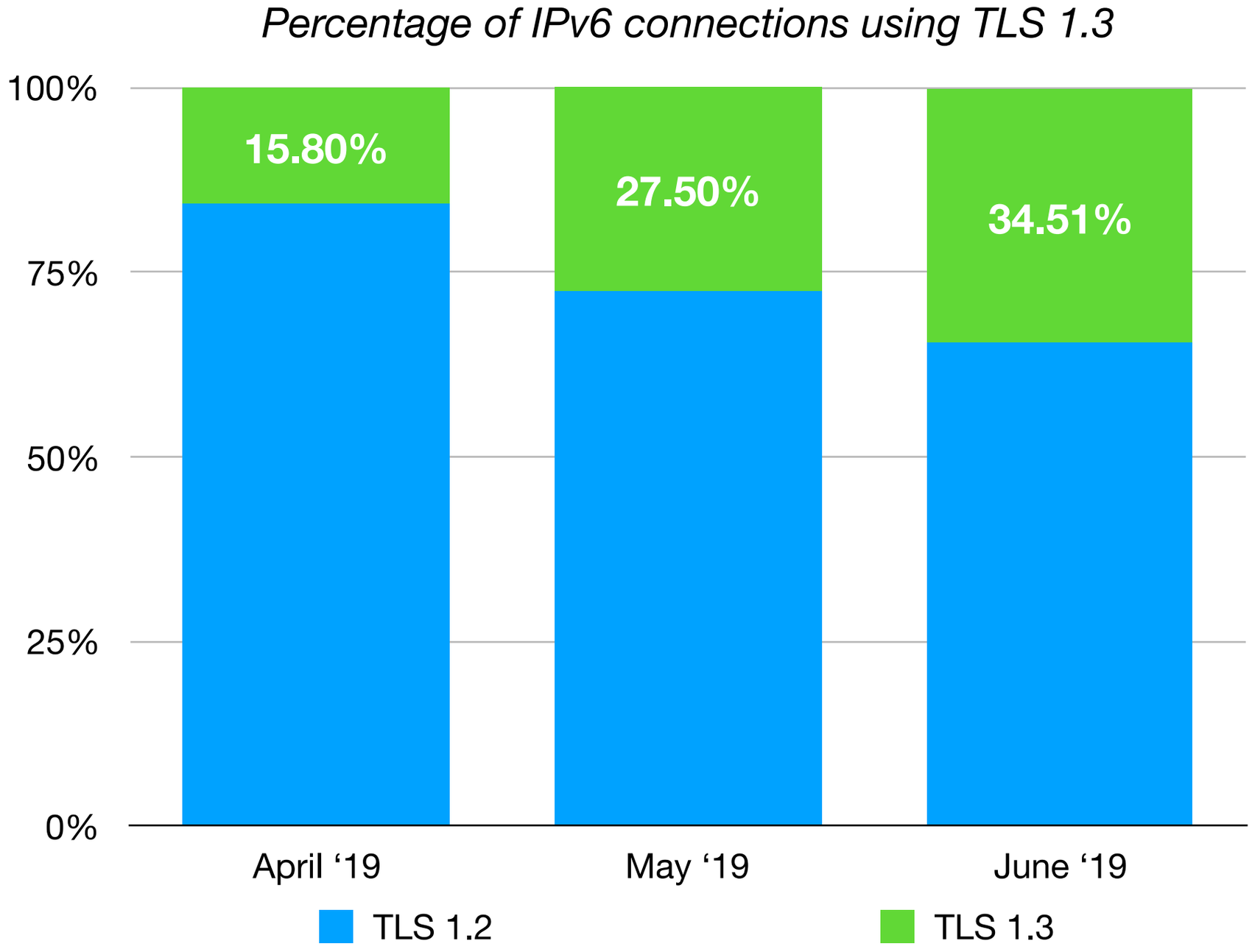
Represents the amount of TLS 1.3 being used, not the number of servers that have deployed TLS 1.3

Data in this presentation was collected from April-June 2019 on a random sample of 0.05% of eligible connection

Server Adoption

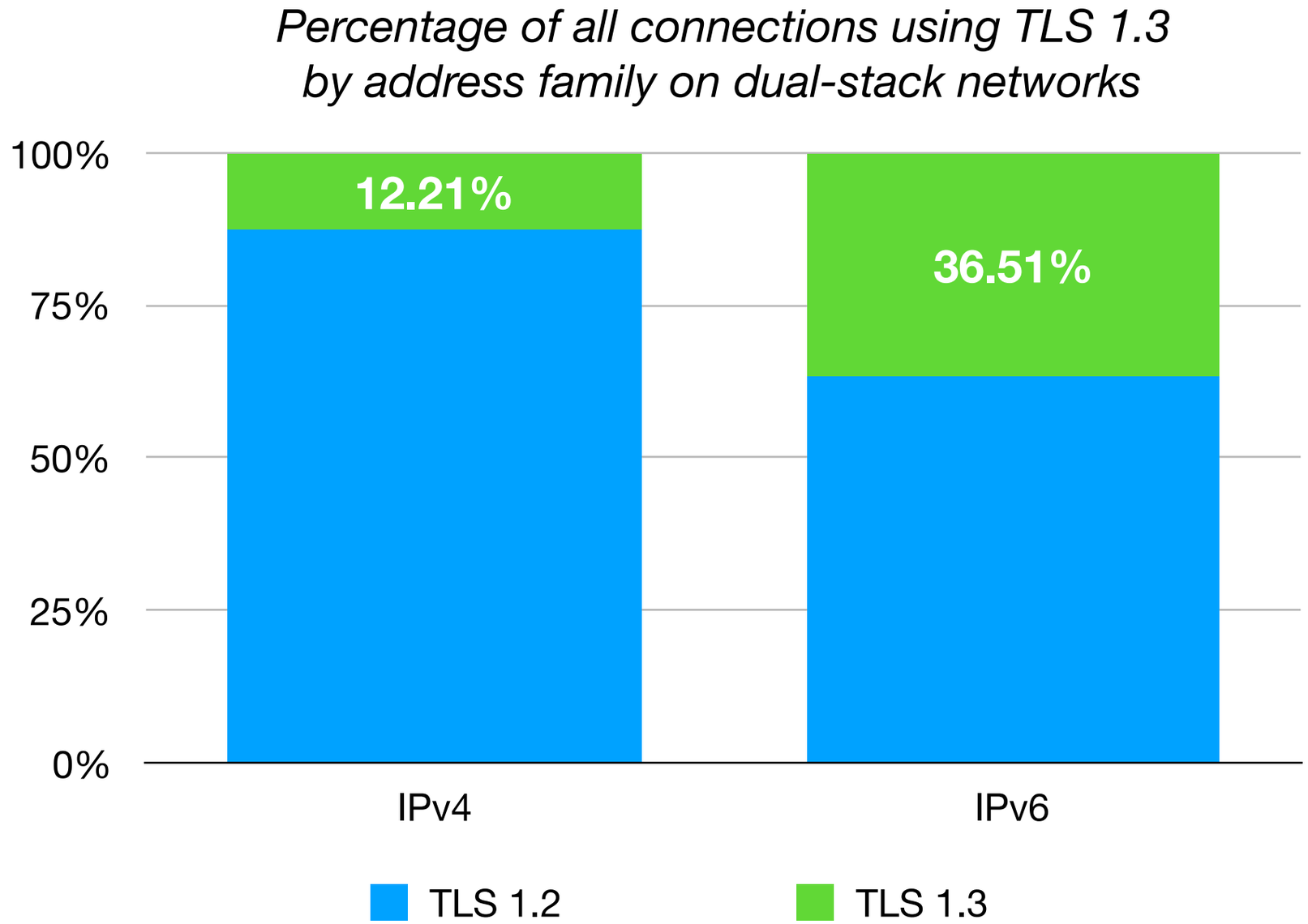


IPv6 Server Adoption



IPv6 Support Correlation

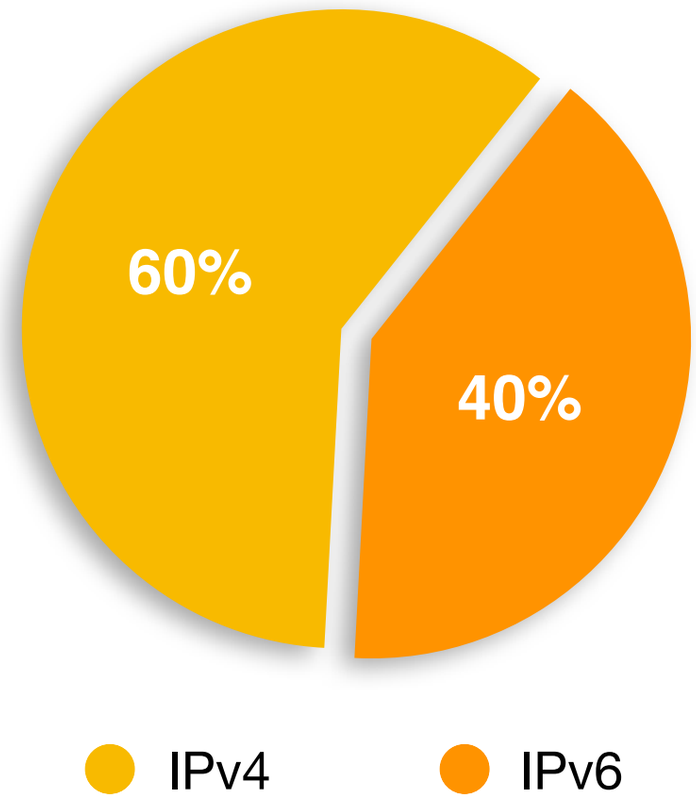
How likely is a server to support TLS 1.3 if it has also upgraded to support IPv6?



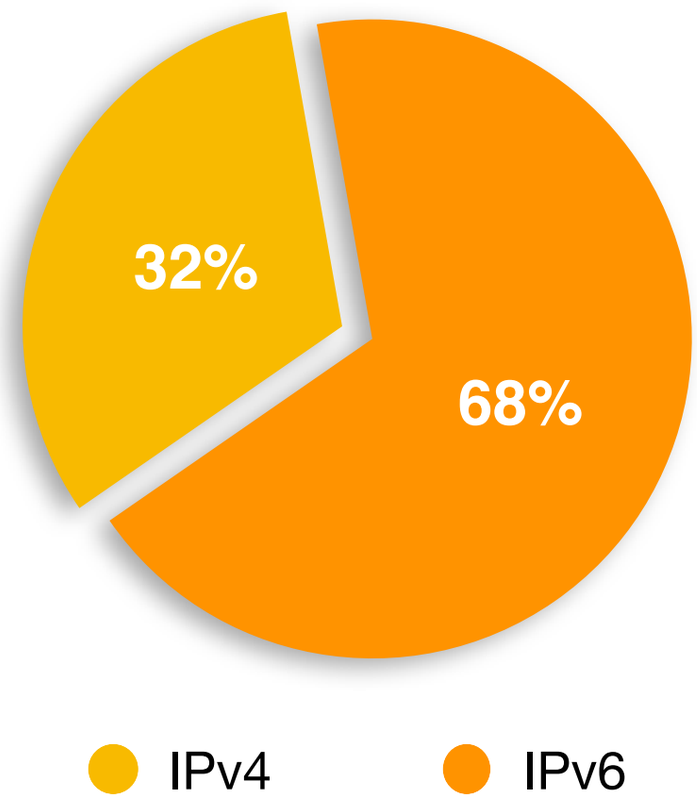
IPv6 Support Correlation

TLS 1.3 servers are more likely to support IPv6

Overall server IPv6 support with dual-stack connectivity

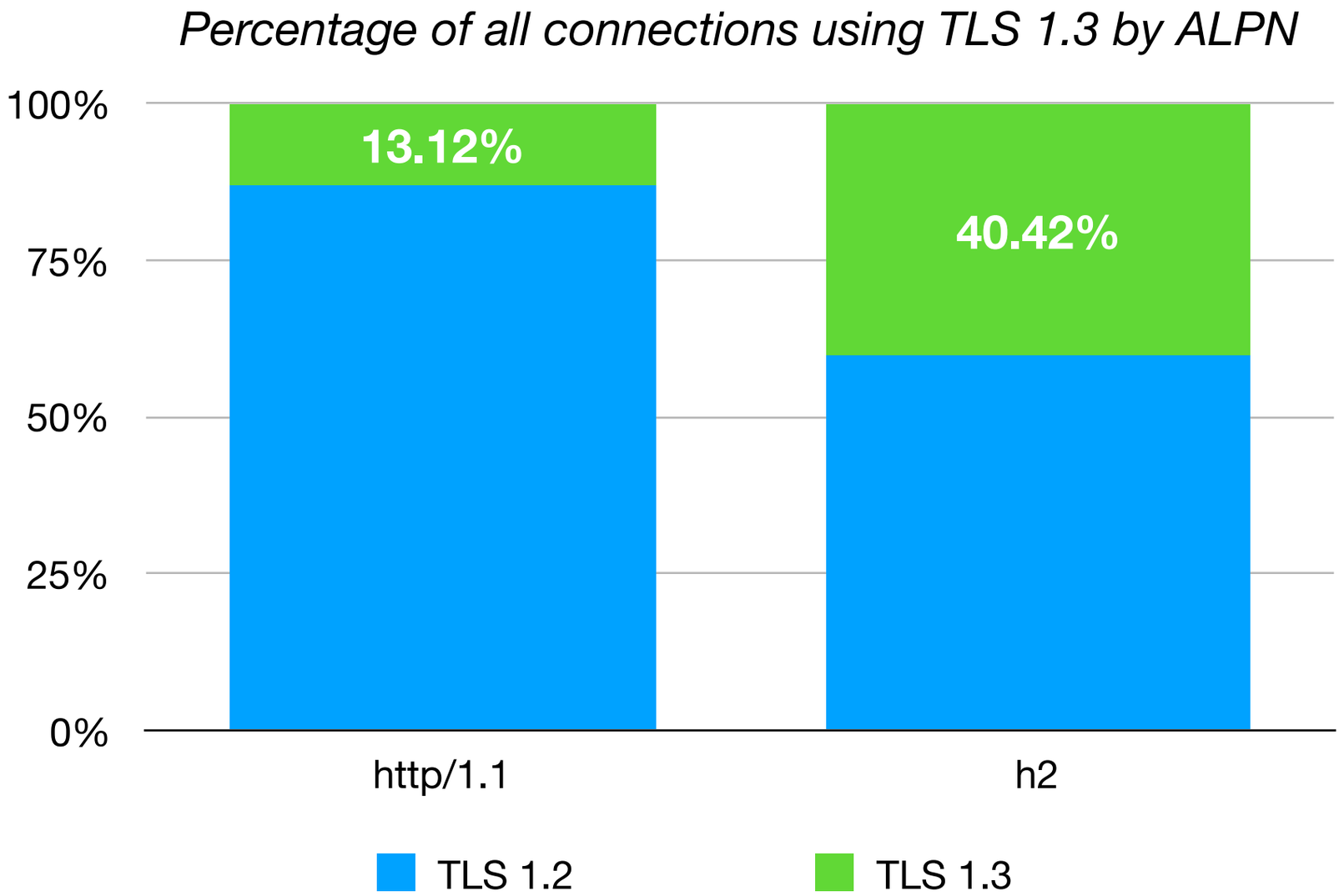


TLS 1.3 server IPv6 support with dual-stack connectivity



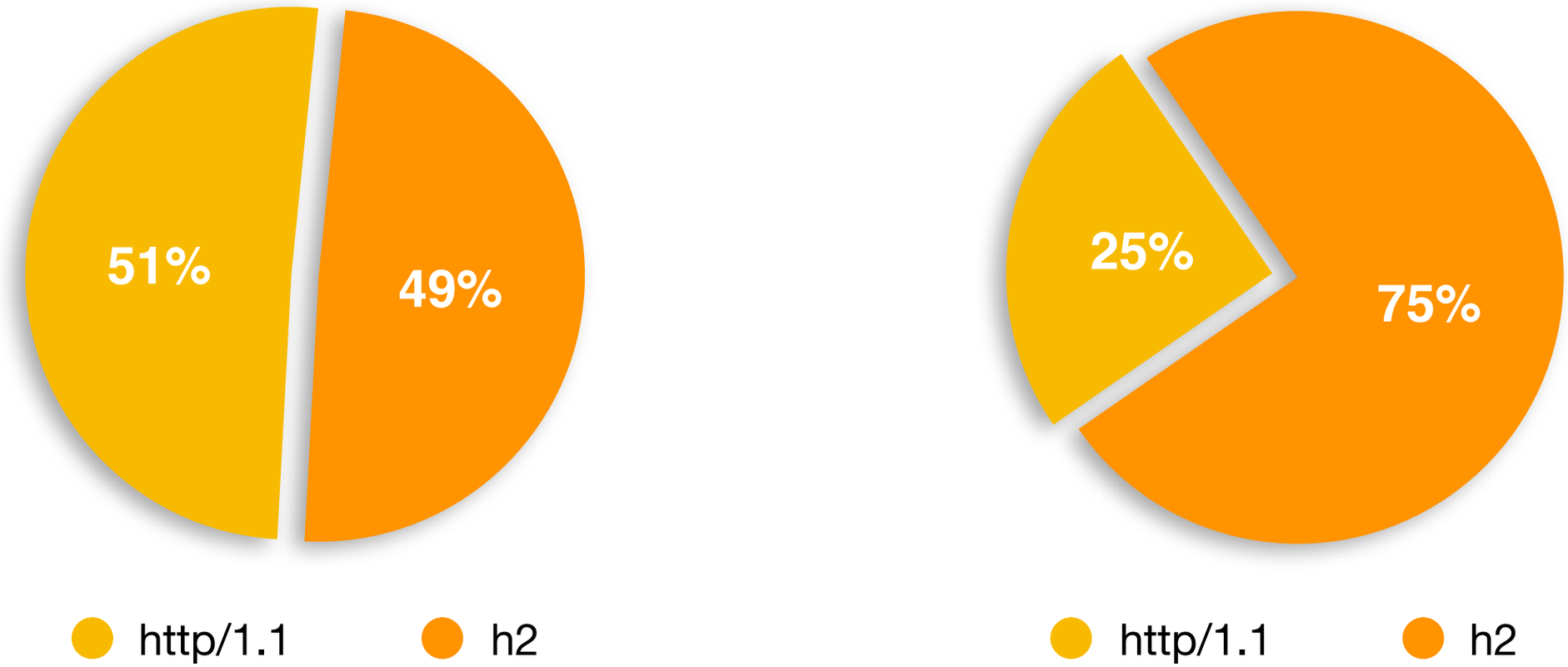
HTTP/2 Support Correlation

How likely is a server to support TLS 1.3 if it has also upgraded to support HTTP/2?

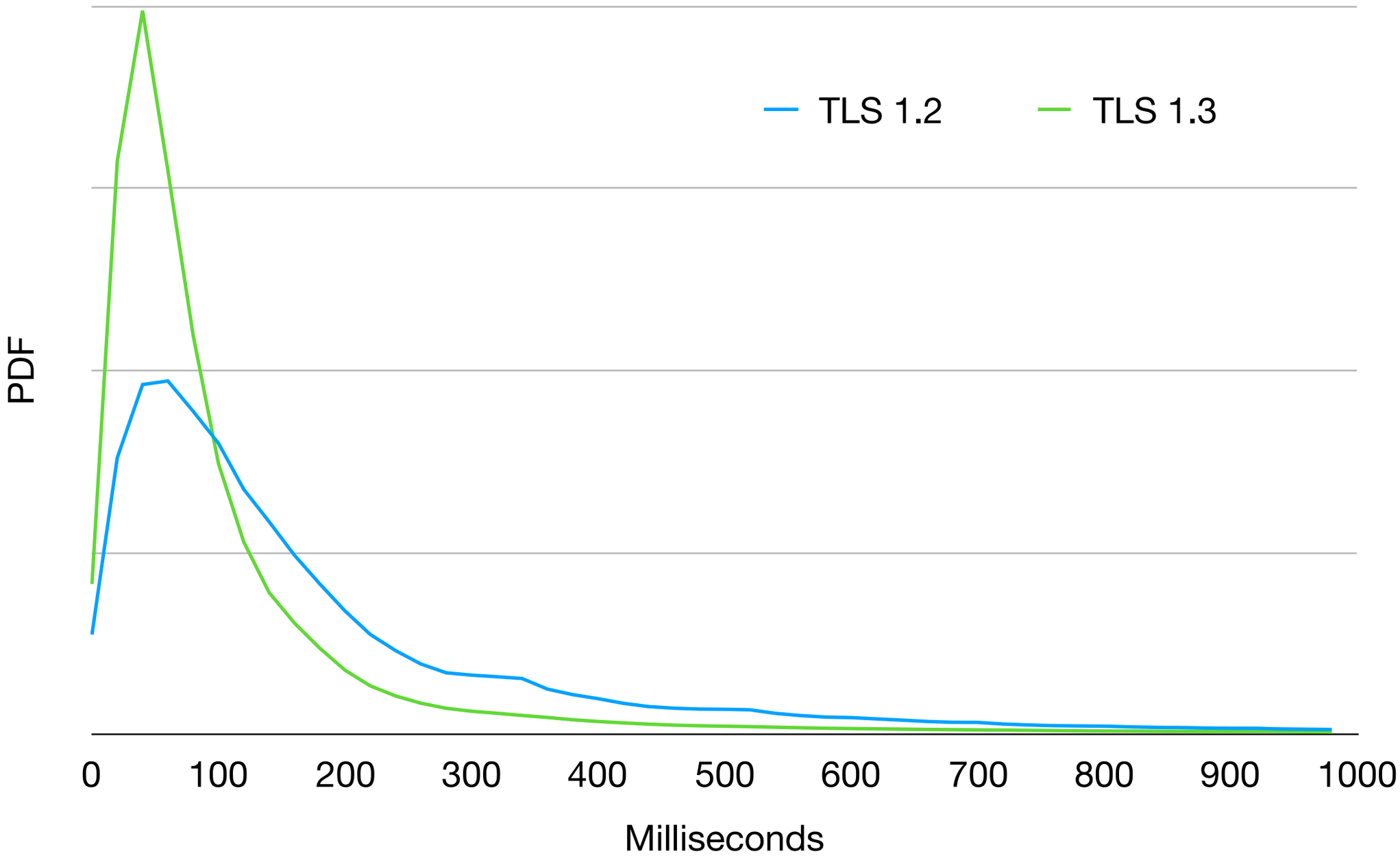


HTTP/2 Support Correlation

TLS 1.3 servers are more likely to support HTTP/2



Handshake Time



Observations

TLS 1.3 support has more than doubled in the past three months

Performance wins clearly demonstrated

Noticeable grouping of servers into:

- Leading Edge (TLS 1.3, HTTP/2, IPv6)
- Stragglers (TLS 1.2, HTTP/1.1, IPv4-only)