TLS

SSL (secure socket layer) 3

~~SSL (secure socket layer) 3~~

TLS (transport layer security)

Why should we use TLS?

- data protection
- Encryption

  "A mechanism to obfuscate what is sent from one host to another."
- Authentication

  "A mechanism to verify the validity of provided identification material."
- Integrity

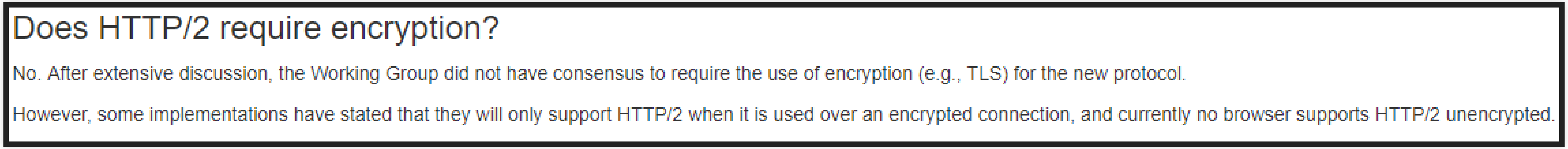
  "A mechanism to detect message tampering and forgery."
- HTTP/2!

https://hpbn.co/tls

This is Fine

HTTP/2

- no HTTP/2 (h2) without TLS
- h2c(leartext) not available in browsers

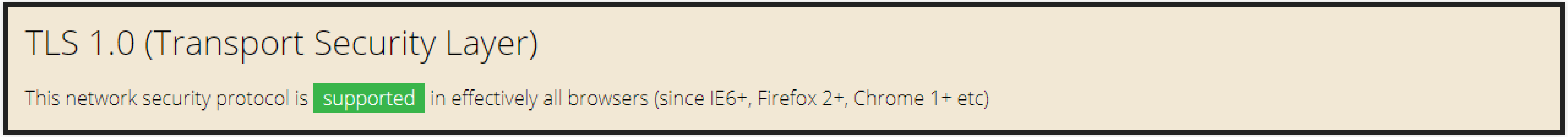


Does HTTP/2 require encryption?

No. After extensive discussion, the Working Group did not have consensus to require the use of encryption (e.g., TLS) for the new protocol.

However, some implementations have stated that they will only support HTTP/2 when it is used over an encrypted connection, and currently no browser supports HTTP/2 unencrypted.

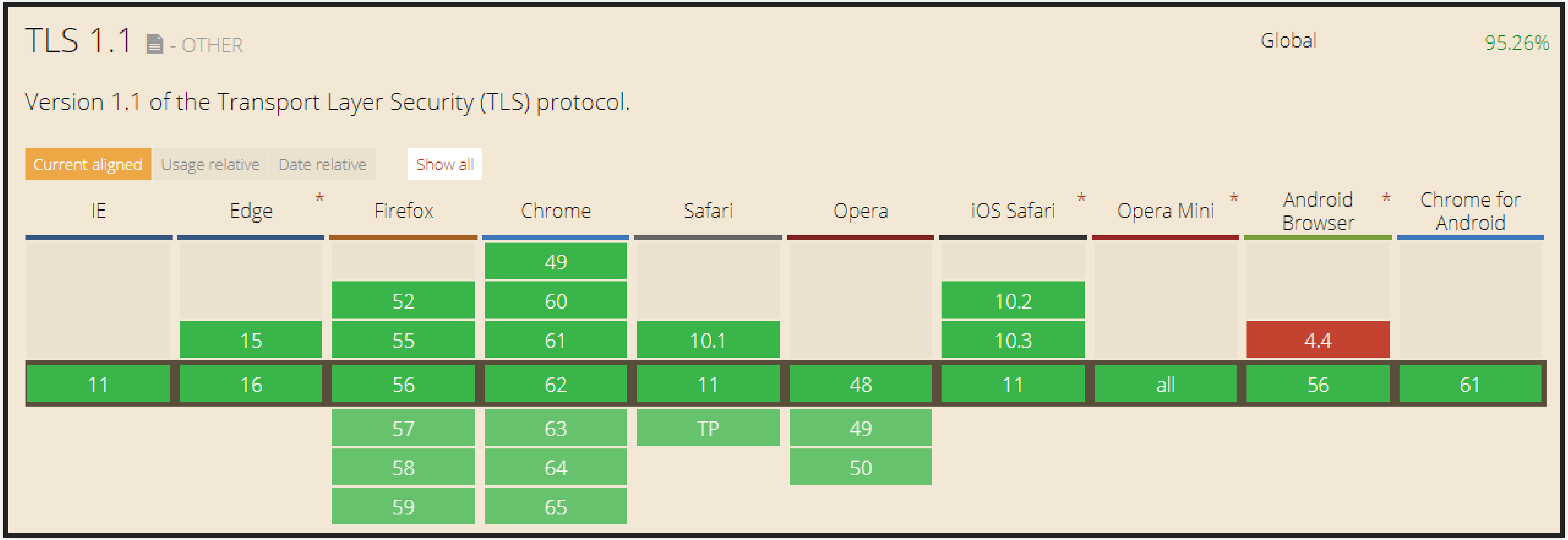
https://http2.github.io/faq/#does-http2-require-encryption



TLS 1.0 (Transport Security Layer)

This network security protocol is supported in effectively all browsers (since IE6+, Firefox 2+, Chrome 1+ etc)

https://caniuse.com/#search=tls



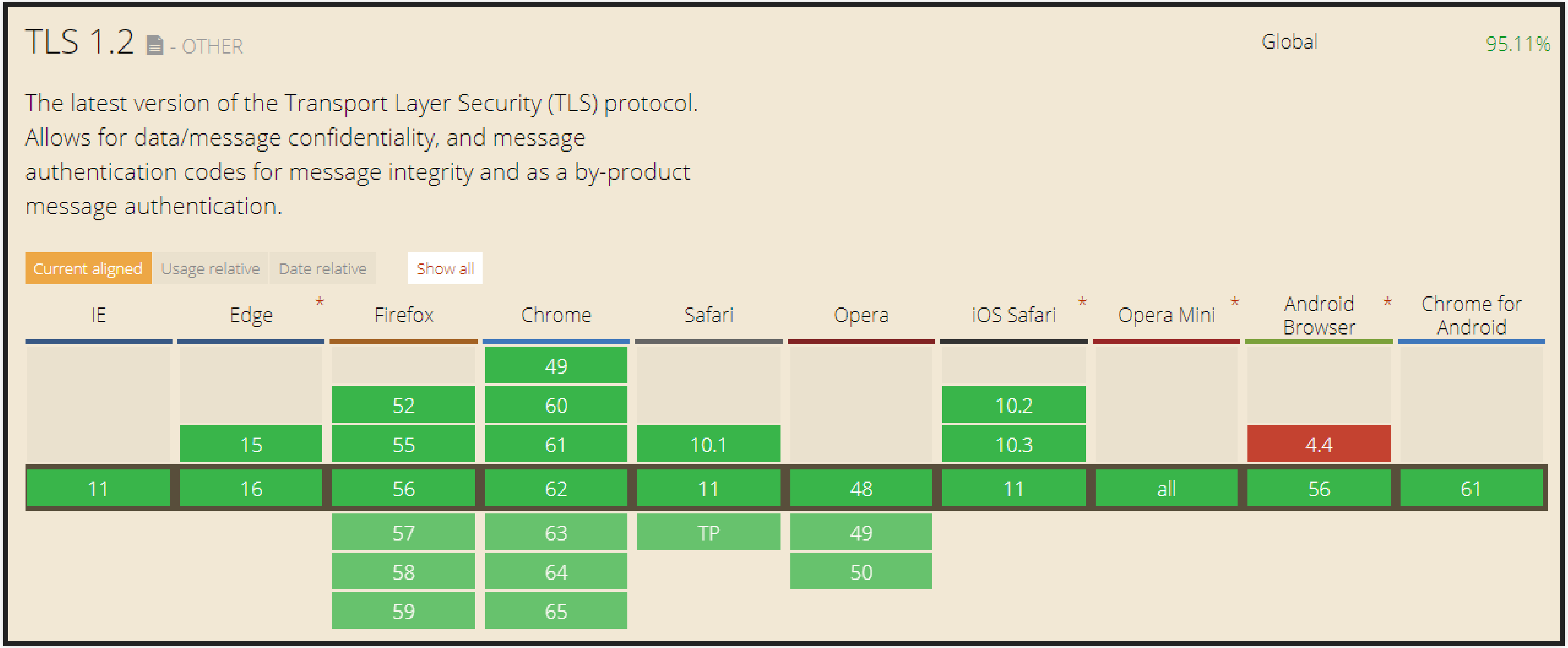
TLS 1.1 - OTHER

Global 95.26%

Version 1.1 of the Transport Layer Security (TLS) protocol.

IE	Edge *	Firefox	Chrome	Safari	Opera	iOS Safari *	Opera Mini *	Android Browser *	Chrome for Android
			49						
		52	60			10.2			
	15	55	61	10.1		10.3		4.4	
11	16	56	62	11	48	11	all	56	61
		57	63	TP	49				
		58	64		50				
		59	65						

https://caniuse.com/#search=tls



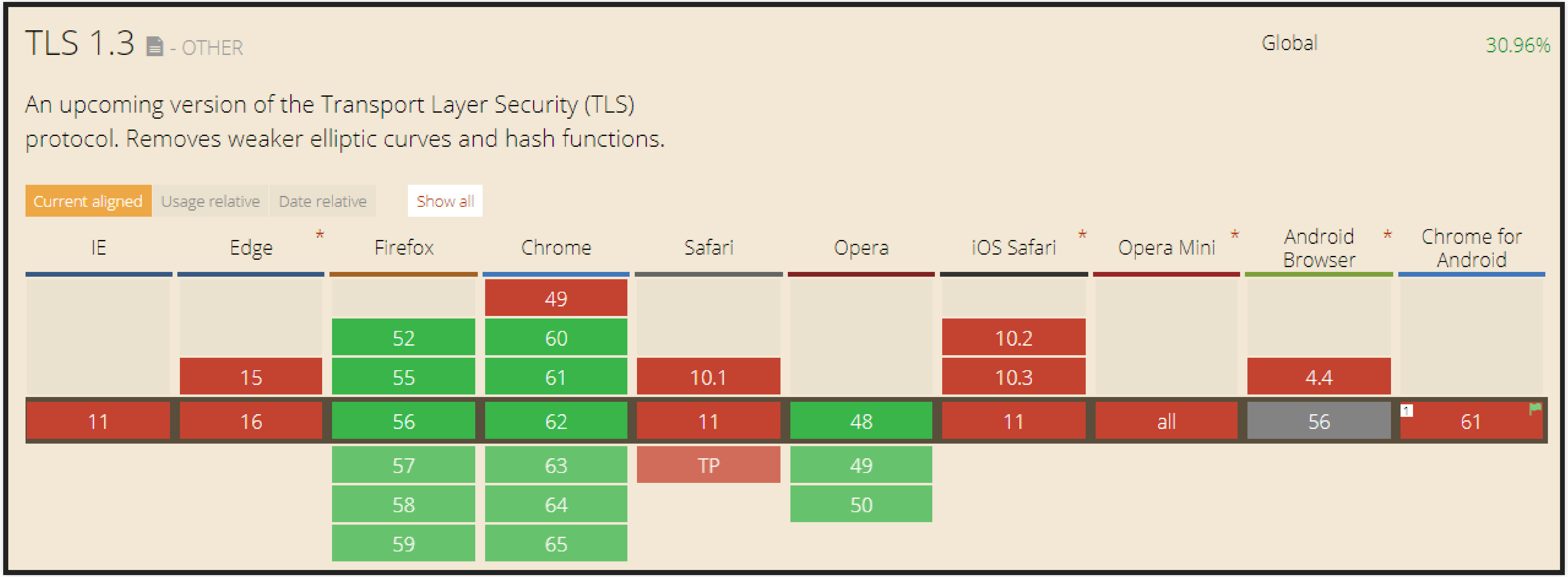
TLS 1.2 - OTHER

Global 95.11%

The latest version of the Transport Layer Security (TLS) protocol. Allows for data/message confidentiality, and message authentication codes for message integrity and as a by-product message authentication.

IE	Edge *	Firefox	Chrome	Safari	Opera	iOS Safari *	Opera Mini *	Android Browser *	Chrome for Android
			49						
		52	60			10.2			
	15	55	61	10.1		10.3		4.4	
11	16	56	62	11	48	11	all	56	61
		57	63	TP	49				
		58	64		50				
		59	65						

https://caniuse.com/#search=tls



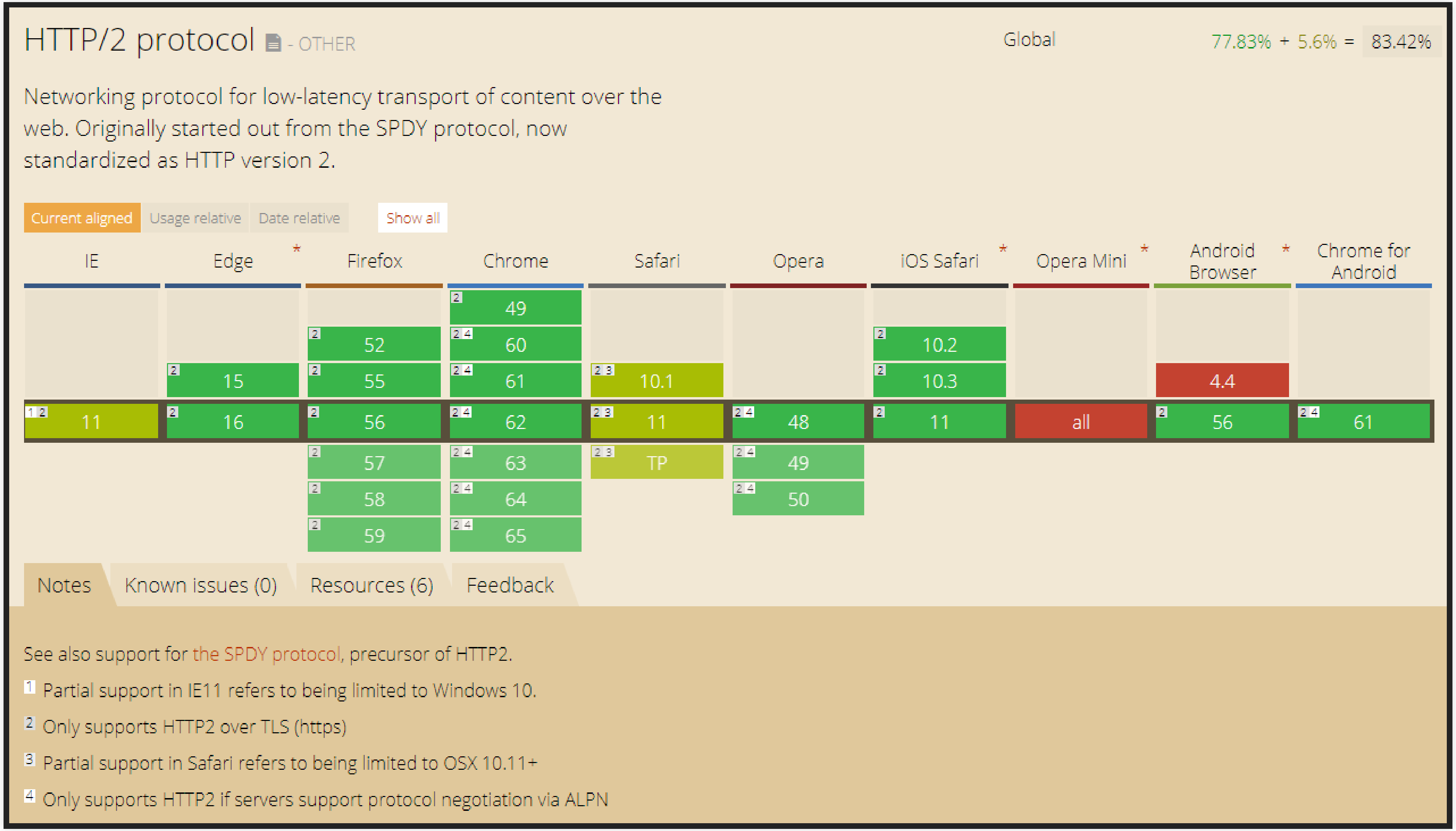
TLS 1.3 - OTHER

Global 30.96%

An upcoming version of the Transport Layer Security (TLS) protocol. Removes weaker elliptic curves and hash functions.

IE	Edge *	Firefox	Chrome	Safari	Opera	iOS Safari *	Opera Mini *	Android Browser *	Chrome for Android
			49						
		52	60			10.2			
	15	55	61	10.1		10.3		4.4	
11	16	56	62	11	48	11	all	56	1 61
		57	63	TP	49				
		58	64		50				
		59	65						

https://caniuse.com/#search=tls



HTTP/2 protocol - OTHER

Global 77.83% + 5.6% = 83.42%

Networking protocol for low-latency transport of content over the web. Originally started out from the SPDY protocol, now standardized as HTTP version 2.

IE	Edge *	Firefox	Chrome	Safari	Opera	iOS Safari *	Opera Mini *	Android Browser *	Chrome for Android
			[2] 49						
		[2] 52	[2 4] 60			[2] 10.2			
	[2] 15	[2] 55	[2 4] 61	[2 3] 10.1		[2] 10.3		4.4	
[1 2] 11	[2] 16	[2] 56	[2 4] 62	[2 3] 11	[2 4] 48	[2] 11	all	[2] 56	[2 4] 61
		[2] 57	[2 4] 63	[2 3] TP	[2 4] 49				
		[2] 58	[2 4] 64		[2 4] 50				
		[2] 59	[2 4] 65						

See also support for the SPDY protocol, precursor of HTTP2.

[1] Partial support in IE11 refers to being limited to Windows 10.

[2] Only supports HTTP2 over TLS (https)

[3] Partial support in Safari refers to being limited to OSX 10.11+

[4] Only supports HTTP2 if servers support protocol negotiation via ALPN

https://caniuse.com/#feat=http2

Is TLS slow?

it depends

- round-trip time (RTT)
- TLS handshake
- TLS session resumption
- TLS False Start
- TLS record size optimization
- Early termination
- HTTP Strict Transport Security (HSTS)
- OCSP(Online Certificate Status Protocol) stapling

https://hpbn.co/transport-layer-security-tls/#optimizing-for-tls

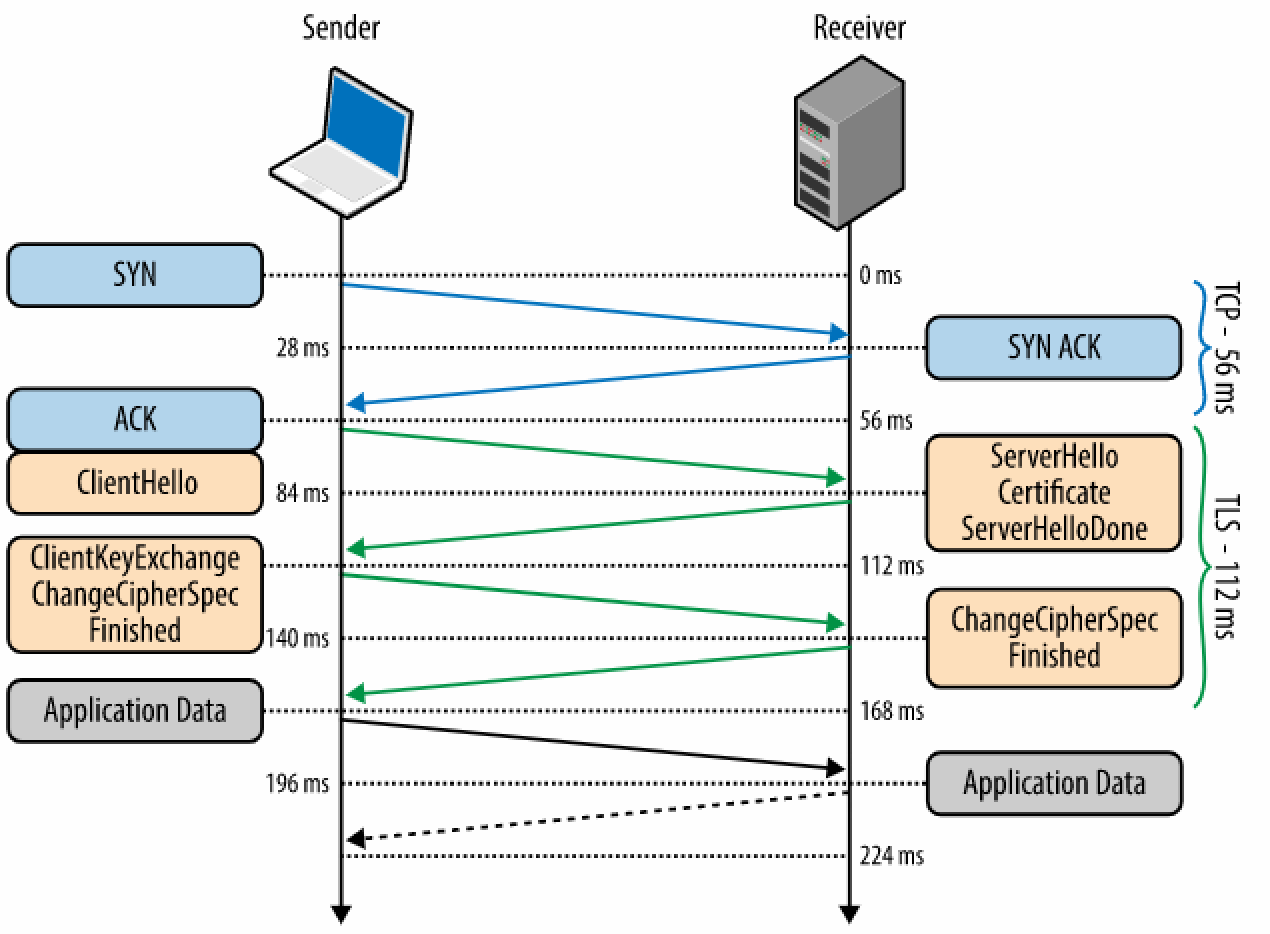


Figure 4-2. TLS handshake protocol

https://hpbn.co/transport-layer-security-tls/#optimizing-for-tls

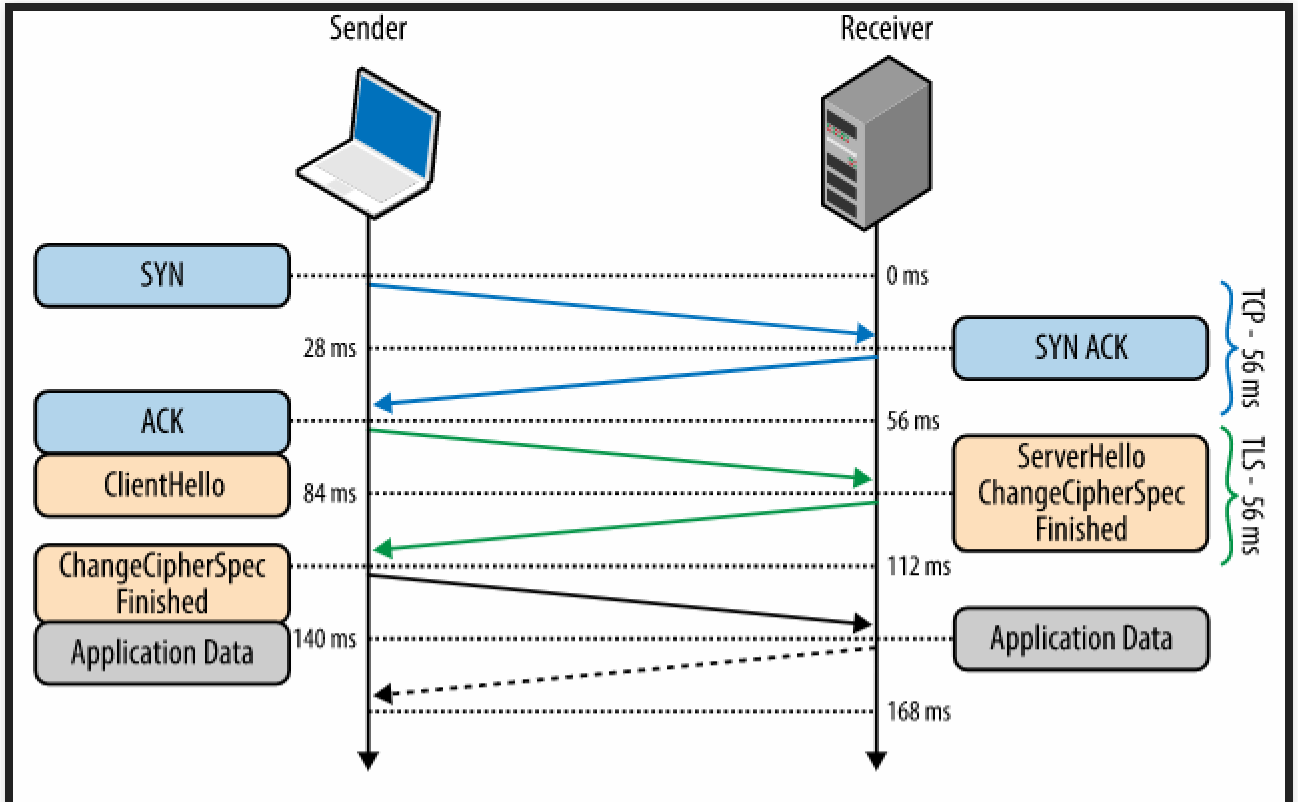


Figure 4-3. Abbreviated TLS handshake protocol

https://hpbn.co/transport-layer-security-tls/#optimizing-for-tls

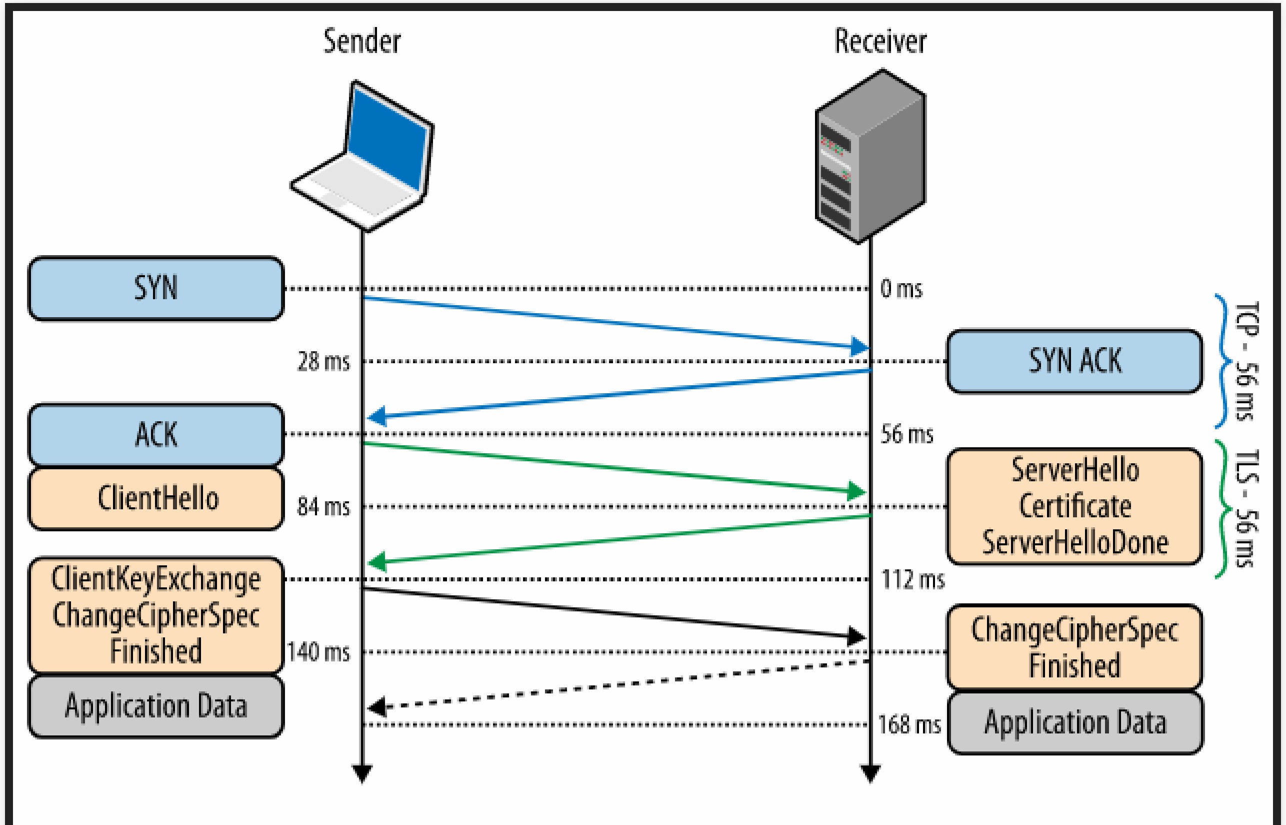
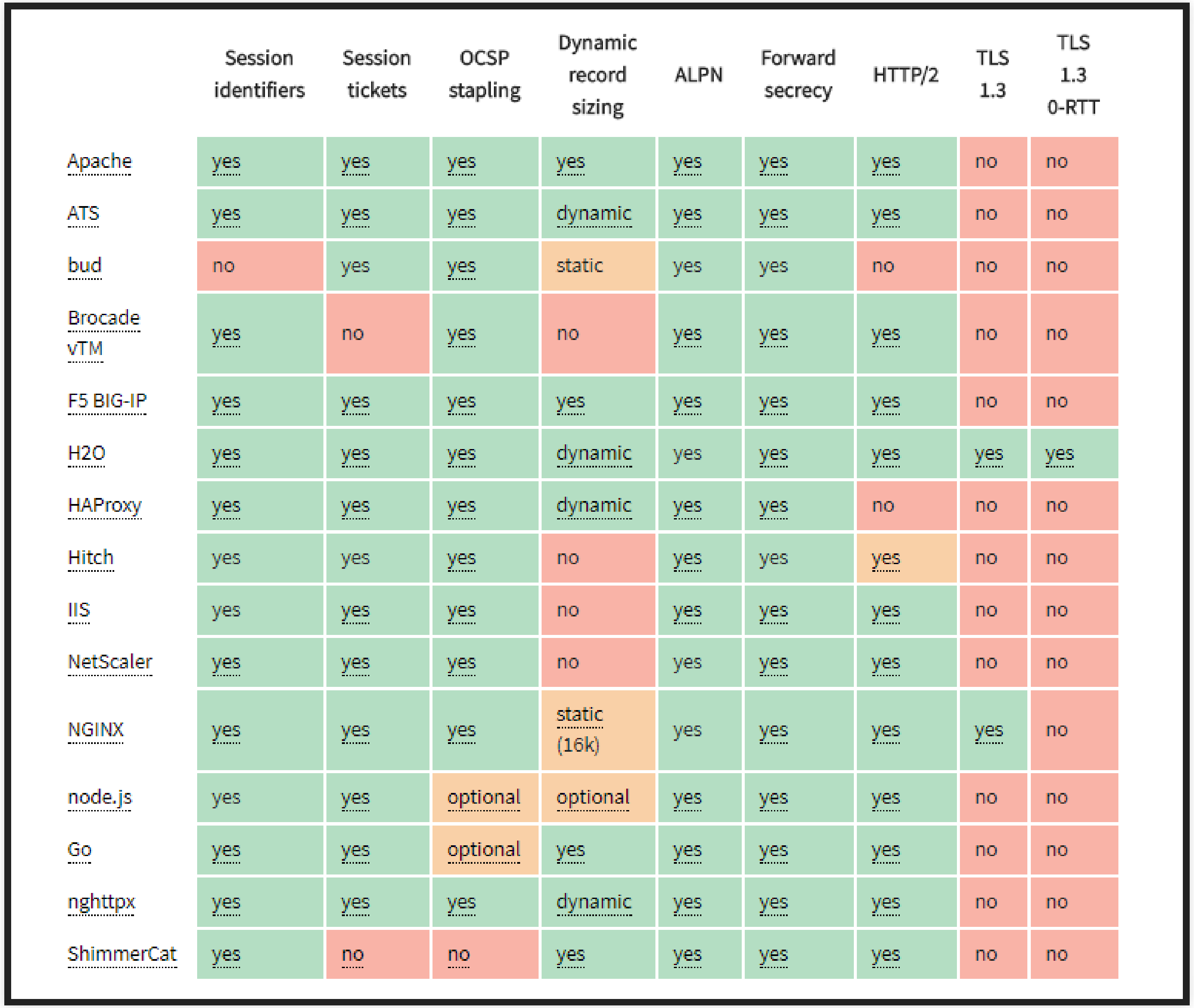


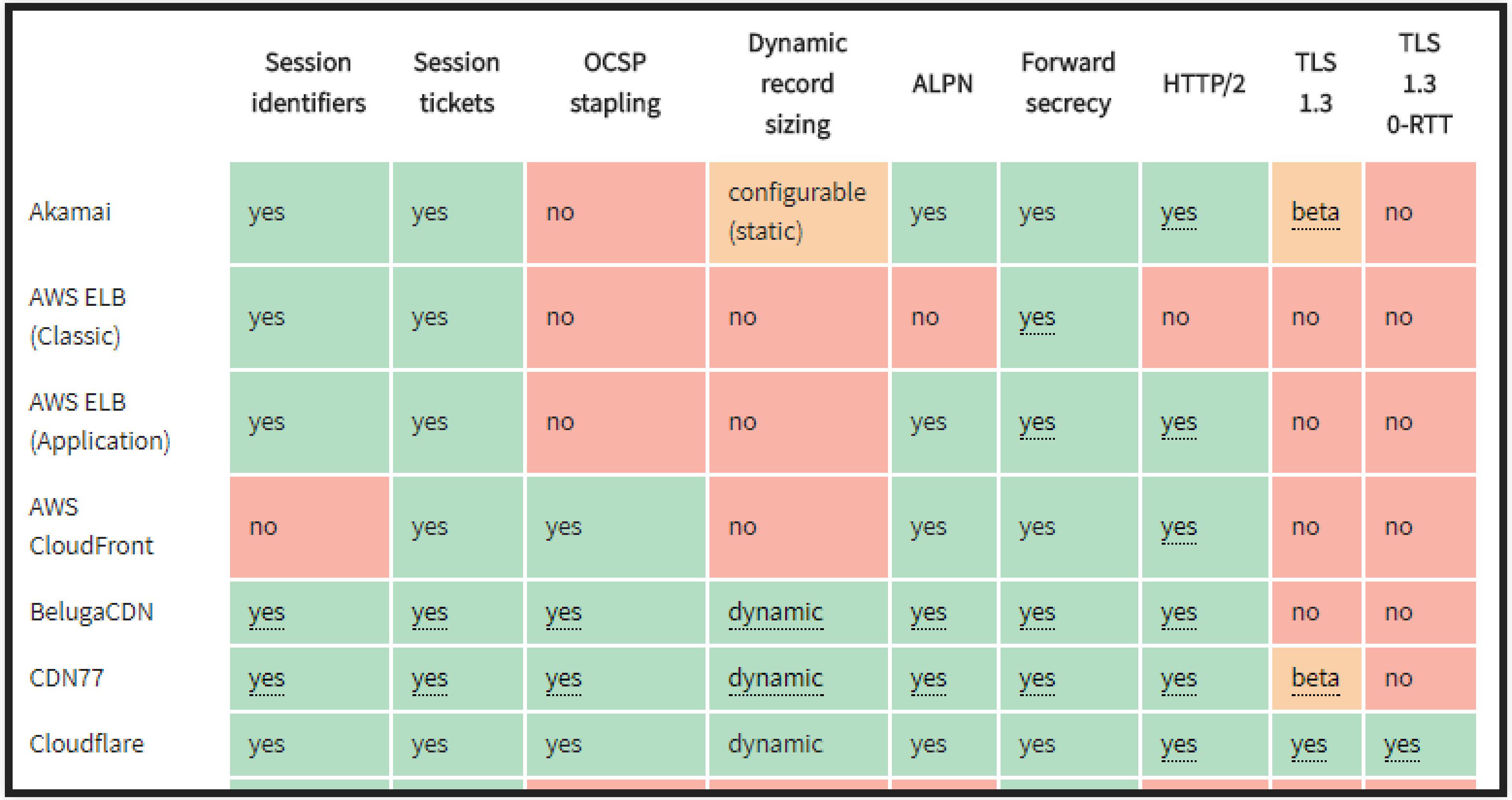
Figure 4-10. TLS handshake with False Start

https://hpbn.co/transport-layer-security-tls/#optimizing-for-tls



	Session identifiers	Session tickets	OCSP stapling	Dynamic record sizing	ALPN	Forward secrecy	HTTP/2	TLS 1.3	TLS 1.3 0-RTT
Apache	yes	yes	yes	yes	yes	yes	yes	no	no
ATS	yes	yes	yes	dynamic	yes	yes	yes	no	no
bud	no	yes	yes	static	yes	yes	no	no	no
Brocade vTM	yes	no	yes	no	yes	yes	yes	no	no
F5 BIG-IP	yes	yes	yes	yes	yes	yes	yes	no	no
H2O	yes	yes	yes	dynamic	yes	yes	yes	yes	yes
HAProxy	yes	yes	yes	dynamic	yes	yes	no	no	no
Hitch	yes	yes	yes	no	yes	yes	yes	no	no
IIS	yes	yes	yes	no	yes	yes	yes	no	no
NetScaler	yes	yes	yes	no	yes	yes	yes	no	no
NGINX	yes	yes	yes	static (16k)	yes	yes	yes	yes	no
node.js	yes	yes	optional	optional	yes	yes	yes	no	no
Go	yes	yes	optional	yes	yes	yes	yes	no	no
nghttpx	yes	yes	yes	dynamic	yes	yes	yes	no	no
ShimmerCat	yes	no	no	yes	yes	yes	yes	no	no

https://istlsfastyet.com/



	Session identifiers	Session tickets	OCSP stapling	Dynamic record sizing	ALPN	Forward secrecy	HTTP/2	TLS 1.3	TLS 1.3 0-RTT
Akamai	yes	yes	no	configurable (static)	yes	yes	yes	beta	no
AWS ELB (Classic)	yes	yes	no	no	no	yes	no	no	no
AWS ELB (Application)	yes	yes	no	no	yes	yes	yes	no	no
AWS CloudFront	no	yes	yes	no	yes	yes	yes	no	no
BelugaCDN	yes	yes	yes	dynamic	yes	yes	yes	no	no
CDN77	yes	yes	yes	dynamic	yes	yes	yes	beta	no
Cloudflare	yes	yes	yes	dynamic	yes	yes	yes	yes	yes

https://istlsfastyet.com/

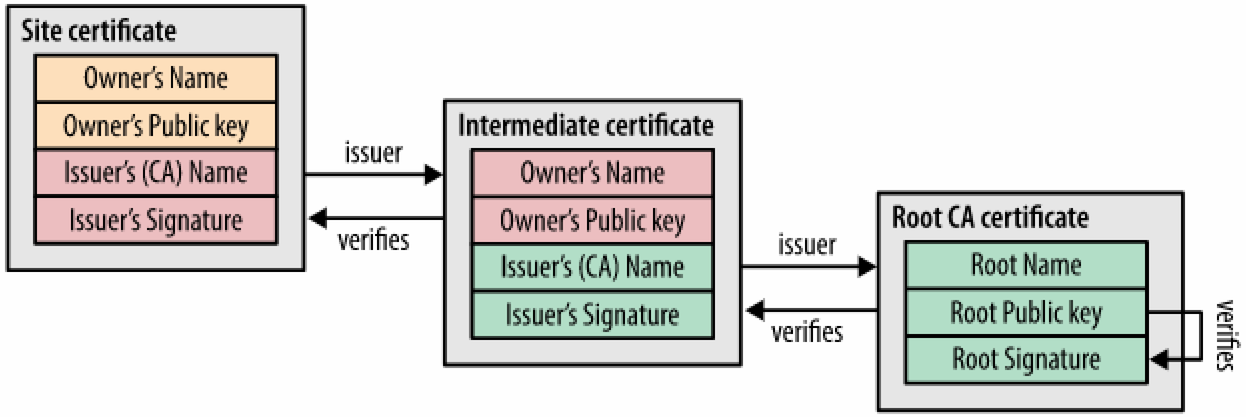
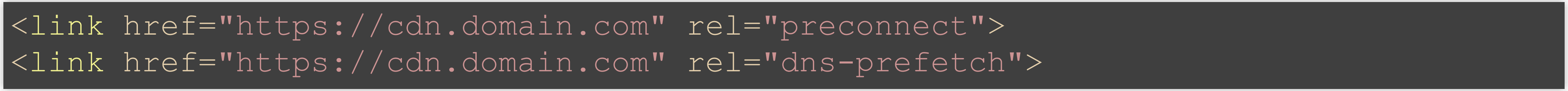


Figure 4-5. CA signing of digital certificates

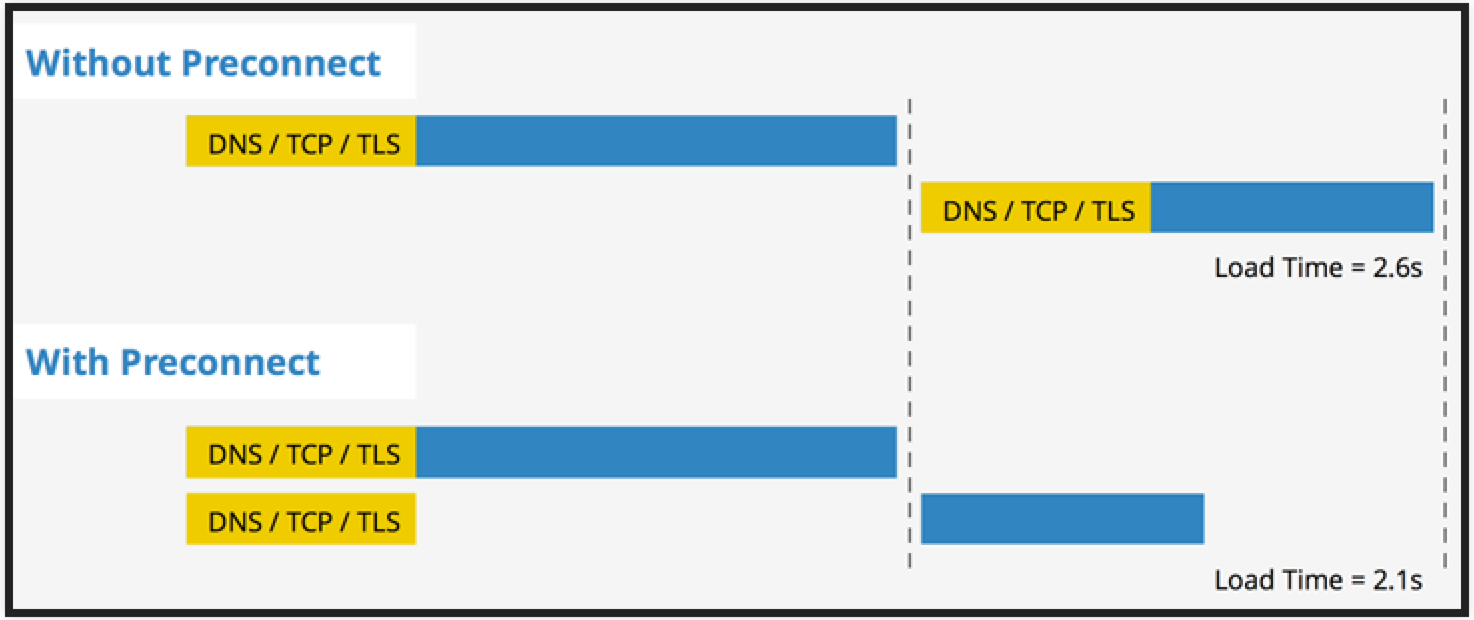
https://hpbn.co/transport-layer-security-tls/#optimizing-for-tls

frontend solutions

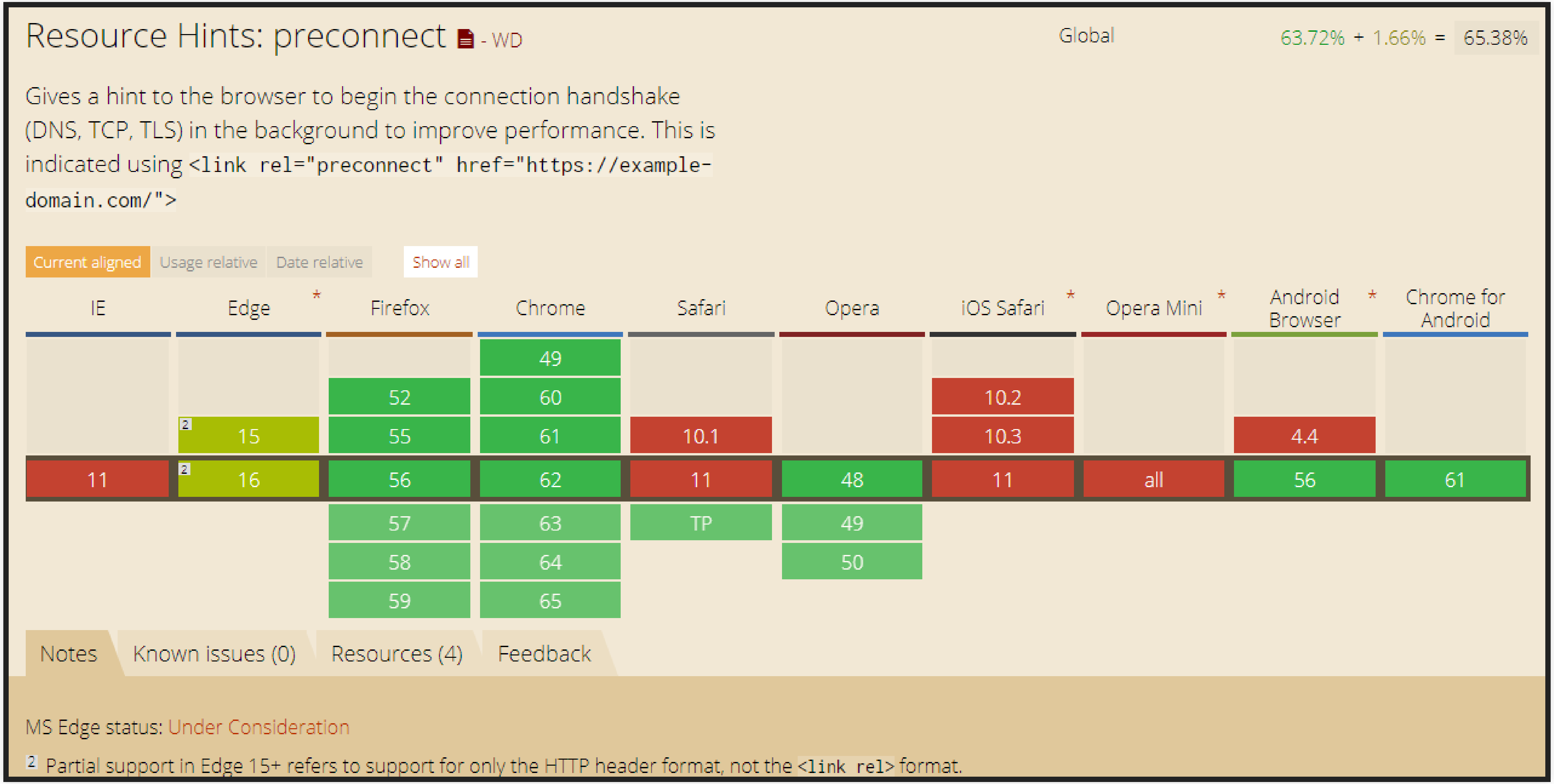
- preconnect
- dns-prefetch



```
<link href="https://cdn.domain.com" rel="preconnect">
<link href="https://cdn.domain.com" rel="dns-prefetch">
```



https://www.keycdn.com/blog/resource-hints/



Resource Hints: preconnect - WD

Global 63.72% + 1.66% = 65.38%

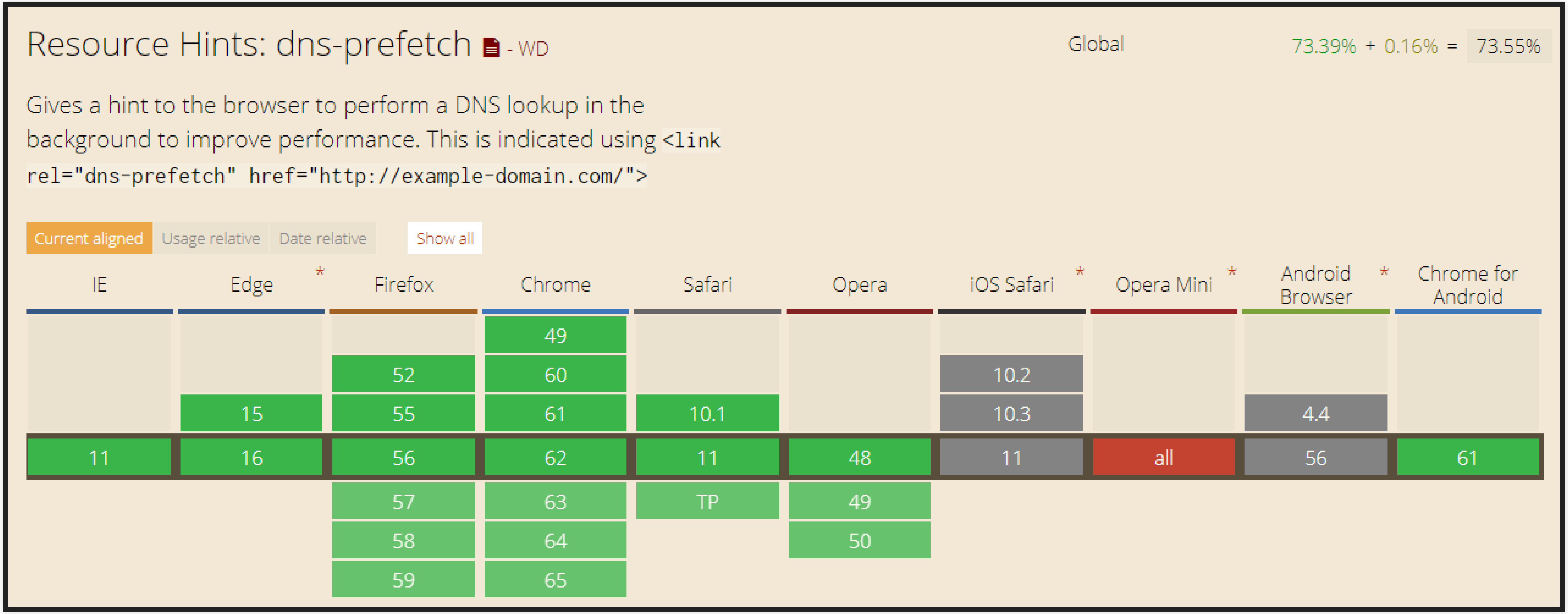
Gives a hint to the browser to begin the connection handshake (DNS, TCP, TLS) in the background to improve performance. This is indicated using `<link rel="preconnect" href="https://example-domain.com/">`

IE	Edge *	Firefox	Chrome	Safari	Opera	iOS Safari *	Opera Mini *	Android Browser *	Chrome for Android
			49						
		52	60			10.2			
	[2] 15	55	61	10.1		10.3		4.4	
11	[2] 16	56	62	11	48	11	all	56	61
		57	63	TP	49				
		58	64		50				
		59	65						

MS Edge status: Under Consideration

[2] Partial support in Edge 15+ refers to support for only the HTTP header format, not the `<link rel>` format.

https://caniuse.com/#feat=link-rel-preconnect



Resource Hints: dns-prefetch - WD

Global 73.39% + 0.16% = 73.55%

Gives a hint to the browser to perform a DNS lookup in the background to improve performance. This is indicated using `<link rel="dns-prefetch" href="http://example-domain.com/">`

IE	Edge *	Firefox	Chrome	Safari	Opera	iOS Safari *	Opera Mini *	Android Browser *	Chrome for Android
			49						
		52	60			10.2			
	15	55	61	10.1		10.3		4.4	
11	16	56	62	11	48	11	all	56	61
		57	63	TP	49				
		58	64		50				
		59	65						

https://caniuse.com/#feat=link-rel-dns-prefetch

https://istlsfastyet.com/

https://hpbn.co/tls

2016