



HTTP/2 објашњен

Позадина, протокол, имплементација и будућност

<http://daniel.haxx.se/HTTP/2/>

by Daniel Stenberg
превео Марко Кажих

Садржај

1. Позадина.....	4
1.1.Аутор.....	4
1.2.Преводац.....	4
1.3.Упомоћ!.....	4
1.4.Лиценца.....	5
1.5.Историја документа.....	5
2. HTTP данас.....	7
2.1.HTTP 1.1 је огроман.....	7
2.2.Цео свемир могућности.....	7
2.3.Неадекватно коришћење TCP-а.....	7
2.4.Величина преноса и бројеви објеката.....	8
2.5.Време одзива убија.....	8
2.6.Блокирање почетка реда.....	9
3. Како да премостите дуго време одзива.....	10
3.1.Талонирање (<i>spriting</i>).....	10
3.2.Inlining.....	10
3.3.Надовезивање.....	10
3.4.Комадање.....	11
4. Надоградња HTTP-а.....	12
4.1.IETF и HTTPbis радна група.....	12
4.1.1.“bis” део имена.....	12
4.2.HTTP/2 је настао од SPDY-а.....	13
5. HTTP/2 концепти.....	14
5.1.HTTP/2 за постојеће URI шеме.....	14
5.2.HTTP/2 за https://.....	15
5.3.HTTP/2 преговори преко TLS.....	15
5.4.HTTP/2 за http://.....	15
6.The HTTP/2 protocol.....	17
6.1.Binary.....	17
6.2.The binary format.....	17
6.3.Multiplexed streams.....	18
6.4.Priorities and dependencies.....	19
6.5.Header compression.....	19
6.5.1.Compression is a tricky subject.....	19
6.6.Reset - change your mind.....	20
6.7.Server push.....	20
6.8.Flow Control.....	20
7.Extensions.....	21
7.1.Alternative Services.....	21
7.1.1.Opportunistic TLS.....	21
7.2.Blocked.....	21
8.A HTTP/2 world.....	23
8.1.How will HTTP/2 affect ordinary humans?.....	23
8.2.How will HTTP/2 affect web development?.....	23
8.3.HTTP/2 implementations.....	24

8.3.1.Missing implementations.....	24
8.4.Common critiques of HTTP/2.....	25
8.4.1.“The protocol is designed or made by Google”.....	25
8.4.2.“The protocol is only useful for browsers”.....	25
8.4.3.“The protocol is only useful for big sites”.....	25
8.4.4.“Its use of TLS makes it slower”.....	25
8.4.5.“Not being ASCII is a deal-breaker”.....	26
8.4.6.“It isn't any faster than HTTP/1.1”.....	26
8.4.7.“It has layering violations”.....	26
8.4.8.“It doesn't fix several HTTP/1.1 shortcomings”.....	27
8.5.Will HTTP/2 become widely deployed?.....	27
9. HTTP/2 у Firefox-у.....	29
9.1.Прво, будите сигурни да је укључен.....	29
9.2.Само TLS.....	29
9.3.Невидљив!.....	29
9.4.Визуализујте коришћење HTTP/2.....	30
10.HTTP/2 у Chromium-у.....	31
10.1.Прво, будите сигурни да је укључен.....	31
10.2.Само TLS.....	31
10.3.Визуализујте коришћење HTTP/2.....	31
11.HTTP/2 у curl-у.....	32
11.1.HTTP 1.x двојник.....	32
11.2.Прост текст није безбедан.....	32
11.3.TLS and what libraries.....	32
11.4.Command line use.....	32
11.5.libcurl options.....	32
12.После HTTP/2.....	33
13. Даље читање.....	34
14. Хвала.....	35

1. Позадина

Овај документ описује HTTP/2 на техничком и протоколарном нивоу. Започет је као презентација коју сам држао у Стокхолму у априлу 2014. године, а касније је конвертован и проширен у пун документ са свим детаљима и ваљаним објашњењима.

Финална HTTP/2 спецификације је завршена и одобрена од стране IESG-а 18. фебруара 2015. године. Тренутна верзија је нацрт-17¹ и тај формат протокола постаће завршни 33К. Све грешке у документу су моје и резултати мојих недостатака. Молим Вас да ми их покажете како бих могао да ажурирам документ и отклоним их.

Верзија овог документа је 1.12, објављена 18.априла 2015. године.

1.1. Аутор

Моје име је Даниел Стенберг и радим у Мозили. Радио сам на пројектима отвореног кода и мрежења протеклих двадесетак година. Вероватно сам најпознатији по томе што предводим развој *curl* и *libcurl*-а. Укључен сам и у IETF HTTPbis радну групу протеклих неколико година и тамо сам био у току са ажурирањима на HTTP 1.1 као и на развоју HTTP/2 стандарда.

Е-пошта: daniel@haxx.se

Twitter: [@bagder](https://twitter.com/bagder)

Веб: daniel.haxx.se

Блог: daniel.haxx.se/blog

1.2. Преводацац

Зовем се Марко Кажич. Радим као веб програмер, евангелиста веб технологија и локализатор. Радио сам на пројектима отвореног кода за локализацију и веб.

Е-пошта: marko.kazic@zamphyr.com

Twitter: [@marxo](https://twitter.com/marxo)

Веб: marxo.me

Github: [@marxo](https://github.com/marxo)

1.3. Упомоћ!

Ако наиђете на грешке, омашке, или блатантне лажи, пошаљите ми поправљену верзију параграфа који треба изменити и ја ћу га изменити.

Поменућу све који буду помогли! Надам се да ће овај документ бити бољи како време пролази.

¹ <http://tools.ietf.org/html/draft-ietf-httpbis-HTTP/2-17>

Овај документ је изворно доступан на енглеском језику на адреси:
<http://daniel.haxx.se/HTTP/2>

1.4. Лиценца

Овај документ је лиценциран под Creative Commons Attribution 4.0 лиценцом: <http://creativecommons.org/licenses/by/4.0/>



1.5. Историја документа

Прва верзија овог документа је објављена 25. априла 2014. године. Следи листа највећих промена кроз верзије документа.

Верзија 1.12:

- **9.1:** mention the Firefox 36+ config switch for HTTP/2

Верзија 1.11:

- Lots of language improvements mostly pointed out by friendly contributors
- **8.3.1:** mention nginx and Apache httpd specific activities

Верзија 1.10:

- 1: the protocol has been "okayed"
- 4.1: refreshed the wording since 2014 is last year
- front: added image and call it "HTTP/2 explained" there, fixed link
- 1.4: added document history section
- many spelling and grammar mistakes corrected
- 14: added thanks to bug reporters
- 2.4: (better) labels for the HTTP growth graph
- 6.3: corrected the wagon order in the multiplexed train
- 6.5.1: HPACK draft-12

Верзија 1.9: February 11, 2015

- Updated to HTTP/2 draft-17 and HPACK draft-11
- Added section "10. HTTP/2 in Chromium" (== one page longer now)
- Lots of spell fixes
- At 30 implementations now
- 8.5: added some current usage numbers
- 8.3: mention internet explorer too
- 8.3.1 "missing implementations" added
- 8.4.3: mention that TLS also increases success rate

Верзија 1.8: January 15th, 2015

- Compressed the images better, leading to a *much* smaller PDF
- Updated to draft-16 and hpack-10
- Replaced several images

- Linkified many URLs
- Added a few questions in 8.4
- Mentions IETF Last Call

2. HTTP данас

HTTP 1.1 се претворио у протокол који се користи буквално за све на интернету. Велика улагања су направљена у протоколе и инфраструктуре да би се искористила предност HTTP-а. Та улагања довела су до тога да је данас лакше направити нешто што ради преко HTTP-а, него писати свој протокол који ради независно.

2.1. HTTP 1.1 је огроман

Када је HTTP створен и пуштен у свет, на њега је гледано као један крајње једноставан протокол, али је време показало да ти није тако. HTTP 1.0 у ЗК 1945 је спецификација од 60 страна објављена 1996. године. ЗК 2616 који описује HTTP 1.1 објављен је само три године касније, 1999. године и проширен је значајно; на 176 страна. Ипак, када смо ми унутар IETF-а радили на ажурирању те спецификације, поделили смо је и претворили у *шест* докумената, који су имали далеко више страна спојени (што је довело до ЗК 7230 и сродних ЗК-а). По свим бројкама, HTTP 1.1 је огроман и укључује плејаду детаља, финеса и велики број изборних делова.

2.2. Цео свемир могућности

Природа HTTP 1.1 да има много детаља и опција доступних за касније проширење, произвела је екосистем где скоро ниједна имплементација нема имплементирано све – јер „све“ и није могуће дефинисати и рећи шта је то „све“. То је довело до ситуације да могућности које су мало кориштене нису имале велики број имплементација, а они који су их имплементирали нису имали много користи од истих.

То је касније проузроковало проблем са интероперабилношћу, када су клијенти или сервери почели чешће да користе те могућности.

2.3. Неадекватно коришћење TCP-а

Користећи HTTP 1.1 веома је тешко искористити све предности и пуну моћ перформанаса које пружа TCP. HTTP клијенти и прегледачи морају да буду веома креативни када налазе решења да смање време учитавања стране.

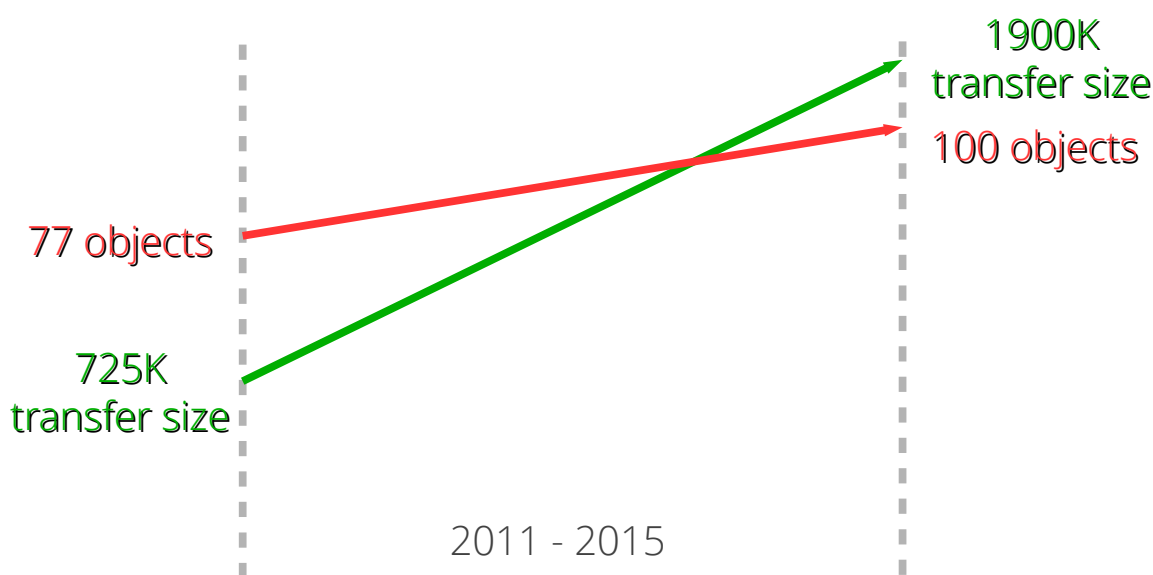
Други покушаји који су кроз године постојали, показали су да TCP није лако заменити и ми смо наставили да побољшавамо TCP и протоколе изнад њега.

Просто речено, TCP се може боље искористити да се избегну паузе или моменти у времену који се могу користити да се подаци примају или шаљу. Одељак који следи ће нагласити неке од недостатака.

2.4. Величина преноса и бројеви објеката

Када погледамо неке од највећих веб сајтова и колико података треба да преузмемо за њихове почетне стране, шаблон је јасан. Током година, количина података која се мора преузети се постепено попела на 1.9МБ. Оно што је важније у овом контексту је то да је у просеку преко стотину засебних ресурса потребно да би се једна страна приказала.

Како график испод приказује, тренд није нов и нема назнаке да ће се променити у скорије време. Показује раст укупног преноса података (зелено) и број укупних захтева – у просеку (црвено), и како су се они мењали у протекле четири године.

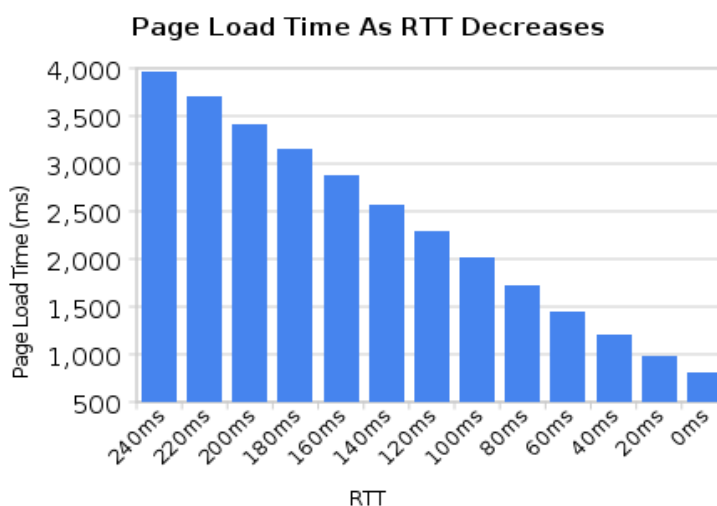


data from [httparchive.org](http://archive.org)

2.5. Време одзива убија

HTTP 1.1 је веома осетљив на време одзива, делом и јер HTTP Pipelining и даље муче проблеми, што је довољно да исти буде искључен за већину корисника.

Иако смо видели велики пораст у доступном протоку у последњих неколико године, нисмо видели побољшање у смањивању времена одзива. Високо време одзива, као и многе мобилне технологије онемогућава вам да добијете добро и брзо веб искуство чак и са везом високог



Drawing 1: RTT, Round Trip Time affects Page Load Time

протока.

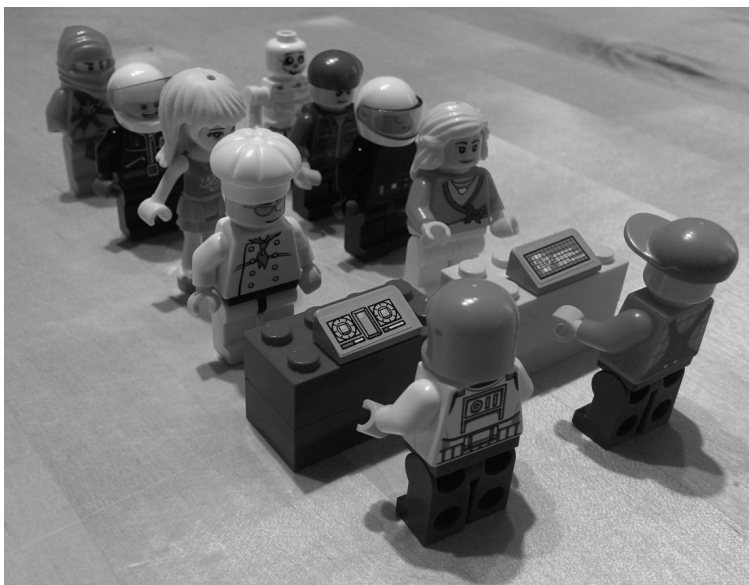
Још један пример где би кратко време одзива било потребно је видео конференција, играње и случно, технологије у којима се не шаље унапред спремљен поток.

2.6. Блокирање почетка реда

HTTP Pipelining је начин да пошаљете још један захтев док чекате одговор на прошли захтев. То је веома слично реду у продавници или у банци. Ви не знате да ли ће особа испред вас пазарити брзо или ће писати чек пола сата.

Можете бити пажљиви у погледу тога који ред бирате, и да изаберете онај за који мислите да је најбржи, некад можете почети нови ред, али не можете избећи доношење одлуке и то да када једном одаберете не можете променити ред.

Прављење новог реда се често доводи у везу са перформансама и казнама у ресурсима, па се не препоручује преко малог броја редова. Једноставно, нема савршеног решења за овај проблем.



Чак и данас, 2015. године, већина веб прегледача долази са искљученим HTTP pipelining-ом.

Више о овом проблему можете прочитати на багзила уносу бр. 264354².

2 https://bugzilla.mozilla.org/show_bug.cgi?id=264354

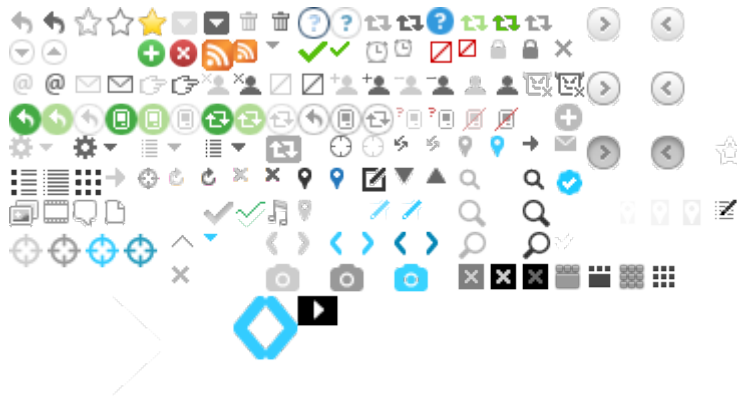
3. Како да премостите дуго време одзива

Као и увек када су суочени са проблемима, људи нађу решење. Нека од ових решења су лукава и корисна, а нека су просто ужасна.

3.1. Талонирање (*spriting*)

Талонирање је термин којим се описује техника комбиновања више малих слика у једну велику слику. Касније користите JavaScript и CSS да „исечете“ посебне делове како би приказали посебне мање слике.

Сајт користи овај трик ради брзине. Преузимање једне велике датотеке је далеко брже у HTTP 1.1 него преузимање 100 посебних мањих.



Наравно, ова техника има своје мане за стране које желе да прикажу једну или две мање слике и слично. Ово такође значи да ће слике бити избачене из кеша у исто време, док би боље решење било да оне чешће кориштене остану у кешу.

3.2. *Inlining*

Inlining је један од трикова који се користе како би избегли слање засебних слика, а постиже се коришћењем `data: URL`а убачених у CSS. Ова техника има сличне предности и мане као и талонирање.

```
.icon1 {  
    background: url(data:image/png;base64,<data>) no-repeat;  
}  
  
.icon2 {  
    background: url(data:image/png;base64,<data>) no-repeat;  
}
```

3.3. Надовезивање

Велики сајт или апликација углавном користе много JavaScript датотека. Фронтенд алати помажу програмерима да споје све у те датотеке у једну велику грудву како би прегледачи преузимали један велики уместо много малих датотека. Превише података се шаље иако је мало неопходно. Превише података се поново преузима када је мало потребно. Ова пракса је углавном лоша за програмере који је користе.

3.4. Комадање

Последњи трик за перформансе који ћу поменути се често назива „комадање“. Суштински, техника се своди на сервирање различитих аспеката са што више домаћина. На први поглед то може бити чудно али постоји врло разумно објашњење за то.

У почетку HTTP 1.1 спецификација је наводила да је клијент ограничен на највише две TCP конекције на сваког домаћина. Дакле, како се не би огрешили о спецификацију, сајтови су једноставно додали нову адресу домаћина и могли су користити више веза ка сервер и смањити време учитавања.

Како је време пролазило, ограничење је укинато и данас клијенти могу да користе 6-8 веза по домаћину, али и даље имају ограничење, па сајтови настављају да користе ову технику како би повећали број веза. Како се број објеката повећава увек – као што смо видели раније – велики број веза се користи како бисмо били сигурни да HTTP ради довољно брзо. Није неуобичајено да сајтови користе више од 50, па чак и преко 100 веза ка једном серверу, користећи ову технику. Скорашња статистика сајта <httparchive.org> показује да првих 300 хиљада линкова на свету треба у просеку 38(!) TCP веза како би показали сајт, а тенденција је да се тај број увећава полако.

Још један разлог да преместите статички садржај као што су слике на друго име домаћина је што такви линкови не користе колачиће, а величина колачића ових дана може бити веома значајна. Коришћењем домаћина без колачића, можете повећати перформансе једноставно тако што ћете имати HTTP захтеве мање величине.

Слика испод показује траг пакета сурфовања по једном од највећих шведских сајтова и како су захтеви подељени на више имена домаћина.

GET	/	www.aftonbladet.se	html	205.71 KB	→ 32 ms
GET	general.css?57785785	www.aftonbladet.se	css	193.22 KB	→ 10 ms
GET	d-head.js?57785785	www.aftonbladet.se	js	190.40 KB	→ 20 ms
GET	aftonbladet.gif	gfx.aftonbladet-cdn.se	gif	6.33 KB	→ 44 ms
GET	sanna_lundell_white.jpg	gfx.aftonbladet-cdn.se	jpeg	3.01 KB	→ 44 ms
GET	pappa01.jpg	gfx2.aftonbladet-cdn.se	jpeg	18.66 KB	→ 228 ms
GET	forskare.jpg	gfx.aftonbladet-cdn.se	jpeg	6.88 KB	→ 44 ms
GET	story26jan.jpg	gfx.aftonbladet-cdn.se	jpeg	2.66 KB	→ 45 ms
GET	osbalk.jpg	gfx2.aftonbladet-cdn.se	jpeg	4.11 KB	→ 238 ms
GET	Bank.jpg	gfx2.aftonbladet-cdn.se	jpeg	16.09 KB	→ 247 ms
GET	Tatu.JPG	gfx.aftonbladet-cdn.se	jpeg	7.38 KB	→ 44 ms
GET	sve8.jpg	gfx.aftonbladet-cdn.se	jpeg	7.39 KB	→ 45 ms
GET	otto-tvaa.jpg	gfx.aftonbladet-cdn.se	jpeg	6.71 KB	→ 46 ms
GET	ASTridTT.JPG	gfx.aftonbladet-cdn.se	jpeg	6.52 KB	→ 66 ms
GET	nimoy.jpg	gfx.aftonbladet-cdn.se	jpeg	7.87 KB	→ 67 ms
GET	PSYK0\$.jpg	gfx2.aftonbladet-cdn.se	jpeg	18.28 KB	→ 257 ms
GET	parislgh.jpg	gfx2.aftonbladet-cdn.se	jpeg	21.89 KB	→ 267 ms
GET	ProjectRunwayvinnare.jpg	gfx2.aftonbladet-cdn.se	jpeg	7.83 KB	→ 276 ms
GET	par_strand-opt.jpg	gfx2.aftonbladet-cdn.se	jpeg	5.72 KB	→ 286 ms
GET	mack.jpg	gfx2.aftonbladet-cdn.se	jpeg	16.27 KB	→ 299 ms
GET	skildaVpuffmitt.jpg	gfx1.aftonbladet-cdn.se	jpeg	4.49 KB	→ 144 ms
GET	socket_ny.jpg	gfx1.aftonbladet-cdn.se	jpeg	3.79 KB	→ 153 ms
GET	andreetta.jpg	gfx1.aftonbladet-cdn.se	jpeg	5.53 KB	→ 163 ms
GET	skidor_50.gif	gfx.aftonbladet-cdn.se	gif	3.20 KB	→ 70 ms

4. Надоградња HTTP-а

Зар не би било лепо када би направили надограђен протокол? Он би био...

1. Протокол мање осетљив на време одзива
2. Протокол без проблема са пајплајнигом и блокирањем почетка реда
3. Протокол који не захтева повећавање број бежа ка домаћину
4. Протокол који задржава постојеће интерфејсе, сав садржај, формате и шеме
5. Протокол који је направљен унутар IETF HTTPbis радне групе

4.1. IETF и HTTPbis радна група

Internet Engineering Task Force (IETF) је организација која развија и промовише интернет стандарде, углавном на протоколарном нивоу. Они су чувени по серији 33К докумената који документују све од TCP-а, DNS-а, FTP-а до најбољих пракси, HTTP-а и бројних варијанти протокола који никад нису објављени или заживели.

Унутар IETF-а “радне групе” се формирају са ограниченим опсегом рада како би радили на остварењу специфичног циља. They establish a “charter” with some set guidelines and limitations for what they should produce. Everyone and anyone is allowed to join in the discussions and development. Everyone who attends and says something has the same weight and chance to affect the outcome and everyone is counted as humans and individuals, little care is given to which companies the individuals work for.

The HTTPbis working group (see later for an explanation of the name) was formed during the summer of 2007 and tasked with creating an update of the HTTP 1.1 specification. Within this group the discussions about a next-version HTTP really started during late 2012. The HTTP 1.1 updating work was completed early 2014 and resulted in the RFC 7320 series.

The supposedly final inter-op meeting for the HTTPbis WG was held in New York City in the beginning of June 2014. The remaining discussions and the IETF procedures to actually get an official RFC out would prove to continue over into the following year.

Some of the bigger players in the HTTP field have been missing from the working group discussions and meetings. I don't want to mention any particular company or product names here, but clearly some actors on the Internet today seem to be confident that IETF will do good without these companies being involved...

4.1.1. “bis” део имена

Група се зове HTTPbis где “bis” долази од латинског прилог за „два”. „Bis” се често користи као наставак или део имена унутар IETF-а за надоградње или друге инстанце спецификација, као што је био случај са HTTP 1.1.

4.2. HTTP/2 је настао од SPDY-а

SPDY³ је протокол који је развио и предводио Google. Они су протокол развили отворено и позвали све да учествују, али је било очигледно да они профитирају имајући контролу над популарном имплементацијом у прегледачу и значајном серверском популацијом са добро уходаним сервисима.

Када је HTTPbis група одлучила да је време да се ради на HTTP/2, SPDY је већ доказао да је концептуално исправан. Показао је да је могуће развити га на Интернет и већ је постојао одређени број публикација о томе како добре перформансе нуди. HTTP/2 је стога заснован на SPDY/3 нацрту, који је фактички преименован у HTTP/2 нацрт-00 коришћењем претраге и замене.

3 <http://en.wikipedia.org/wiki/SPDY>

5. HTTP/2 концепти

Шта тачно HTTP/2 постиже? Где су границе онога што је HTTPbis група зацртала?

Граница је у ствару веома строга и ставила је

- ✓ Протокол мора да задржи HTTP парадигме. И даље је протокол где клијент шаље серверу захтев преко TCP-а.
- ✓ http:// и https:// URLи се не могу мењати. Не може бити нове шеме за линкове. Количина садржаја са таквим линковима је превелика да би их мењали.
- ✓ HTTP1 сервери и клијенти ће бити ту још деценијама, морамо да омогућимо да се преусмере на HTTP/2 сервере.
- ✓ Затим, проксији морају бити у могућности да мапирају HTTP/2 могућности на HTTP 1.1 клијенте 1:1.
- ✓ Уклањање или смањивање изборних делова протокола. Ово није био прави захтев колико мантра, преузета до SPDY-а и Google-овог тима. Чинећи све могућности обавезним, смањујемо могућност да ће могућности касније остати неимплементирани.
- ✓ Нема више минорних верзија. Одлучено је да су клијенти и сервер или компатибилни са HTTP/2 или нису. Ако дође до ситуације да се протокол мења то ће бити HTTP/3. Неће бити малих ревизија у HTTP/2.



5.1. HTTP/2 за постојеће URI шеме

Као што смо раније поменули, постојеће URI шеме не могу се мењати за HTTP/2. Пошто се оне користе за HTTP 1.x данас, очигледно морамо да нађемо начин да надоградимо протокол на HTTP/2 или некако другачије захтевамо од сервера да користи HTTP/2 уместо старих протокола.

HTTP 1.1 је дефинисао начин да то уради; Upgrade: заглавље које омогућава серверу да одговори користећи нови протокол када се такав захтев пошаље користећи стари протокол. По цени кружења.

Казна у виду кружења је нешто што тим који је развијао SPDY није хтео да прихвати и како су имплементирали SPDY само преко TLS-а, они су развили додатак који се користи за преговарање и знатно га скраћује. Користећи овај додатак који се зове NPN (Next Protocol Negotiation), сервер говори клијенту који протокол зна, а клијент потом користи преферирани протокол из те листе.

5.2. HTTP/2 за https://

A lot of focus of HTTP/2 has been to make it behave properly over TLS. SPDY is only done over TLS and there's been a strong push for making TLS mandatory for HTTP/2 but it didn't get consensus and HTTP/2 will ship with TLS as optional. However, two prominent implementers have stated clearly that they will only implement HTTP/2 over TLS: the Mozilla Firefox lead and the Google Chrome lead. Two of the leading web browsers of today.

Reasons for choosing TLS-only include respect for user's privacy and early measurements showing that new protocols have a higher success rate when done with TLS. This because of the widespread assumption that anything that goes over port 80 is HTTP 1.1 makes some middle-boxes interfere and destroy traffic when instead other protocols are communicated there.

The subject about mandatory TLS has caused much hand-waving and agitated voices in mailing lists and meetings – is it good or is it evil? It is an infected subject – be aware of this when you throw this question in the face of a HTTPbis participant!



Similarly, there's been a fierce and long-going debate on whether HTTP/2 should dictate a list of ciphers that should be mandatory when using TLS, or if it perhaps should blacklist a set or if it shouldn't require anything at all from the TLS "layer" but leave that to the TLS WG.

5.3. HTTP/2 преговори преко TLS

Next Protocol Negotiation (NPN), is the protocol used to negotiate SPDY with TLS servers. As it wasn't a proper standard, it was taken through the IETF and ALPN came out of that: *Application Layer Protocol Negotiation*. ALPN is what is being promoted to be used for HTTP/2, while SPDY clients and servers still use NPN.

The fact that NPN existed first and ALPN has taken a while to go through standardization has lead to many early HTTP/2 clients and HTTP/2 servers implementing and using both these extensions when negotiating HTTP/2. Also, as NPN is what's used for SPDY and many servers offer both SPDY and HTTP/2 so supporting both NPN and ALPN on those servers make perfect sense.

ALPN primarily differs from NPN in who decides what protocol to speak. With ALPN the client tells the server a list of protocols in its order of preference and the server picks the one it wants, while with NPN the client makes that final choice.

5.4. HTTP/2 за http://

As mentioned briefly previously, for plain-text HTTP 1.1 the way to negotiate HTTP/2 is by asking the server with an **Upgrade:** header. If the server speaks HTTP/2 it responds with a "101 Switching" status and from then on it speaks HTTP/2 on that connection. You of

course realize that this upgrade procedure costs a full network round-trip, but the upside is that a HTTP/2 connection should be possible to keep alive and re-use to a larger extent than HTTP1 connections generally are.

While some browsers' spokespersons have stated they will not implement this means of speaking HTTP/2, the Internet Explorer team has expressed that they will, and curl already supports this.

6.The HTTP/2 protocol

Enough about the background, the history and politics behind what took us here. Let's dive into the specifics of the protocol. The bits and the concepts that create HTTP/2.

6.1. Binary

HTTP/2 is a binary protocol.

Just let that sink in for a minute. If you're a person who has been involved in internet protocols before, chances are that you will now be instinctively reacting against this choice and marshaling your arguments that spell out how protocols that are made based on text/ascii are superior because humans can handcraft request over telnet and so on..

HTTP/2 is binary to make the framing much easier. Figuring out the start and the end of frames is one of the really complicated things in HTTP 1.1 and actually in text based protocols in general. By moving away from optional white spaces and different ways to write the same thing, implementations become simpler.

Also, it makes it much easier to separate the actual protocol parts from the framing - which in HTTP1 is confusingly intermixed.

The facts that the protocol features compression and often will run over TLS also diminish the value of text since you won't see text over the wire anyway. We simply have to get used to the idea to use a Wireshark inspector or similar to figure out exactly what's going on at protocol level in HTTP/2.

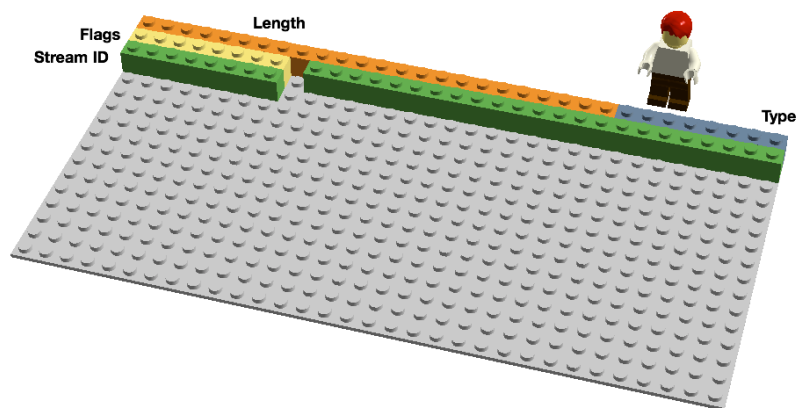
Debugging of this protocol will instead probably have to be done with tools like curl or by analyzing the network stream with Wireshark's HTTP/2 dissector and similar.

6.2. The binary format

HTTP/2 sends binary frames. There are different frame types that can be sent and they all have the same setup:

Type, Length, Flags, Stream Identifier and frame payload.

There are ten different frames defined in the HTTP/2 spec and the two perhaps most fundamental ones that map HTTP 1.1 features are DATA and HEADERS. I'll describe some of the frames in closer detail further on.



6.3. Multiplexed streams

The Stream Identifier mentioned in the previous section describing the binary frame format, makes each frame sent over HTTP/2 get associated with a “stream”. A stream is a logical association. An independent, bi-directional sequence of frames exchanged between the client and server within an HTTP/2 connection.

A single HTTP/2 connection can contain multiple concurrently open streams, with either endpoint interleaving frames from multiple streams. Streams can be established and used unilaterally or shared by either the client or server and they can be closed by either endpoint. The order in which frames are sent within a stream is significant. Recipients process frames in the order they are received.

Multiplexing the streams means that packages from many streams are mixed over the same connection. Two (or more) individual trains of data are made into a single one and then split up again on the other side. Here are two trains:



So they're crammed into and over the same connection in a multiplexed manner:



In HTTP/2 we will see tens and hundreds of simultaneous streams. The cost of creating a new one is very low.

6.4. Priorities and dependencies

Each stream also has a priority, which is used to tell the peer which streams to consider most important.

The exact details on how priorities work in the protocols have changed several times and are still being debated. The point is however that a client can specify which streams that are most important and there's a dependency parameter so that one stream can be made dependent on another.

The priorities can be changed dynamically in run-time, which should enable browsers to make sure that when users scroll down a page full of images it can specify which images that are most important, or if you switch tabs it can prioritize a new set of streams then suddenly come into focus.

6.5. Header compression

HTTP is a state-less protocol. In short that means that every request needs to bring with it as much details as the server needs to serve that request, without the server having to store a lot of info and meta-data from previous requests. Since HTTP/2 doesn't change any such paradigms, it too has to do this.

This makes HTTP repetitive. When a client asks for many resources from the same server, like images from a web page, there will be a large series of requests that all look almost identical. A series of almost identical something begs for compression.

While the number of objects per web page increases as I've mentioned earlier, the use of cookies and the size of the requests have also kept growing over time. Cookies also need to be included in all requests, mostly the same over many requests.

The HTTP 1.1 request sizes have actually gotten so large over time so they sometimes even end up larger than the initial TCP window, which makes them very slow to send as they need a full round-trip to get an ACK back from the server before the full request has been sent. Another argument for compression.



6.5.1. Compression is a tricky subject

HTTPS and SPDY compressions were found to be vulnerable to the BREACH⁴ and CRIME⁵ attacks. By inserting known text into the stream and figuring out how that changes the output, an attacker can figure out what's being sent.

Doing compression on dynamic content for a protocol without then becoming vulnerable for one of these attacks requires some thoughts and careful considerations. This is what

4 http://en.wikipedia.org/wiki/BREACH_%28security_exploit%29

5 <http://en.wikipedia.org/wiki/CRIME>

the HTTPbis team tries to do.

Enter HPACK⁶, *Header Compression for HTTP/2*, which – as the name suitably suggests - is a compression format especially crafted for HTTP/2 headers and it is strictly speaking being specified in a separate internet draft. The new format, together with other counter-measures such as a bit that asks intermediaries to not compress a specific header and optional padding of frames should make it harder to exploit this compression.

In the words of Roberto Peon (one of the creators of HPACK) “HPACK was designed to make it difficult for a conforming implementation to leak information, to make encoding and decoding very fast/cheap, to provide for receiver control over compression context size, to allow for proxy re-indexing (i.e. shared state between frontend and backend within a proxy), and for quick comparisons of huffman-encoded strings”.

6.6. Reset - change your mind

One of the drawbacks with HTTP 1.1 is that when a HTTP message has been sent off with a Content-Length of a certain size, you can't easily just stop it. Sure you can often (but not always) disconnect the TCP connection but that then comes as the price of having to negotiate a new TCP handshake again.

A better solution would be to just stop the message and start anew. This can be done with HTTP/2's RST_STREAM frame which will help in preventing wasted bandwidth and avoid having to tear down any connection.

6.7. Server push

This is the feature also known as “cache push”. The idea here is that if the client asks for resource X the server may know that the client then also most likely want resource Z and sends that to the client without it asking for it. It helps the client to put Z into its cache so that it'll be there when it wants it.

Server push is something a client explicitly must allow the server to do and even if a client does that, it can at its own choice swiftly terminate a pushed stream with RST_STREAM should it not want a particular one.

6.8. Flow Control

Each individual stream over HTTP/2 has its own advertised flow window that the other end is allowed to send data for. If you happen to know how SSH works, this is very similar in style and spirit.

For every stream both ends have to tell the peer that it has more room to fit incoming data in, and the other end is only allowed to send that much data until the window is extended. Only DATA frames are flow controlled.

6 <http://tools.ietf.org/html/draft-ietf-httpbis-header-compression-12>

7. Extensions

The protocol mandates that a receiver must read and ignore all unknown frames using unknown frame types. Two parties can thus negotiate use of new frame types on a hop-by-hop basis, and those frames aren't allowed to change state and they will not be flow controlled.

The subject of whether HTTP/2 should allow extensions at all was debated at length during the time the protocol was developed with opinions swinging for and against. After draft-12 the pendulum swept back one last time and extensions were allowed again.

Extensions are then not part of the actual protocol but will be documented outside of the core protocol spec. Already at this point, there are two frame types that have been discussed for inclusion in the protocol that probably will be the first frames sent as extensions. I'll still describe them here just because of their popularity and previous state as "native" frames:

7.1. Alternative Services

With HTTP/2 getting adopted, there are reasons to suspect that TCP connections will be much lengthier and be kept alive much longer than HTTP 1.x connections have been. A client should be able to do a lot of what it wants with a single connection to each host/site and that single one could then potentially be open for quite some time.

This will affect how HTTP load balancers work and there may come situations when a site wants to advertise and suggest that the client connects to another host. It could be for performance reasons but also if a site is being taken down for maintenance and similar.

The server will then send the Alt-Svc: header⁷ (or ALTSVC frame with HTTP/2) telling the client about an alternative service. Another route to the same content, using another service, host and port number.

A client is then meant to attempt to connect to that service asynchronously and only use the alternative if that works fine.

7.1.1. Opportunistic TLS

The Alt-Svc header allows a server that provides content over http://, to inform the client that the same content is also available over a TLS connection.

This is a somewhat debated feature. Such a connection would do unauthenticated TLS and wouldn't be advertised as "secure" anywhere, wouldn't use any padlock in the UI or in fact in no way tell the user that it isn't plain old HTTP, but this is still opportunistic TLS and some people are very firmly against this concept.

7.2. Blocked

A frame of this type is meant to be sent *exactly once* by a HTTP/2 party when it has data to

⁷ <http://tools.ietf.org/html/draft-ietf-httpbis-alt-svc-01>

send off but flow control forbids it to send any data. The idea being that if your implementation receives this frame you know your implementation has messed up something and/or you're getting less than perfect transfer speeds because of this.

A quote from draft-12, before this frame was moved out to become an extension:

"The BLOCKED frame is included in this draft version to facilitate experimentation. If the results of the experiment do not provide positive feedback, it could be removed"

8.A HTTP/2 world

So what will things look like when HTTP/2 gets adopted? Will it get adopted?

8.1. How will HTTP/2 affect ordinary humans?

HTTP/2 is not yet widely deployed nor used. We can't tell for sure exactly how things will turn out. We have seen how SPDY has been used and we can make some guesses and calculations based on that and other past and current experiments.

HTTP/2 reduces the number of necessary network round-trips and it avoids the head of line blocking dilemma completely with multiplexing and fast discarding of unwanted streams.

It allows a large amount of parallel streams that go way over even the most sharding sites of today.

With priorities used properly on the streams, chances are much better that clients will actually get the important data before the less important data.



All this taken together, I'd say that the chances are very good that this will lead to faster page loads and to more responsive web sites. Shortly put: a better web experience.

How much faster and how much improvements we will see, I don't think we can say yet. First, the technology is still very early and then we haven't even started to see clients and servers trim implementations to really take advantage of all the powers this new protocol offers.

8.2. How will HTTP/2 affect web development?

Over the years web developers and web development environments have gathered a full toolbox of tricks and tools to work around problems with HTTP 1.1, recall that I outlined some of them in the beginning of this document as a justification for HTTP/2.

Lots of those workarounds that tools and developers now use by default and without thinking, will probably hurt HTTP/2 performance or at least not really take advantage of HTTP/2's new super powers. Spriting and inlining should most likely not be done with HTTP/2. Sharding will probably be detrimental to HTTP/2 as it will probably benefit from using less connections.

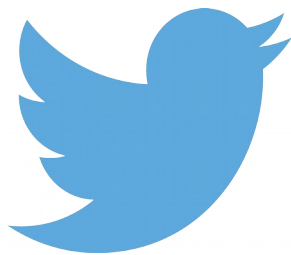
A problem here is of course that web sites and web developers need to develop and deploy for a world that in the short term at least, will have both HTTP1.1 and HTTP/2 clients as users and to get maximum performance for all users can be challenging

without having to offer two different front-ends.

For these reasons alone, I suspect there will be some time before we will see the full potential of HTTP/2 being reached.

8.3. HTTP/2 implementations

Trying to document specific implementations in a document such as this is of course completely futile and doomed to fail and only feel outdated within a really short period of time. Instead I'll explain the situation in broader terms and refer readers to the list of implementations⁸ on the HTTP/2 web site.



There was a large amount of implementations already early on, and the amount has increased over time during the HTTP/2 work. At the time of writing this there are over 30 implementations listed, and most of them implement the latest drafts.



Firefox has been the browser that's been on top of the bleeding edge drafts, Twitter has kept up and offered its services over HTTP/2. Google started during April 2014 to offer HTTP/2 support on a few test servers running their services and since May 2014 they offer HTTP/2 support in their development versions of Chrome. Microsoft has shown a tech preview with HTTP/2 support for their next Internet Explorer version.

curl and libcurl support insecure HTTP/2 as well as the TLS based using on one out of several different TLS libraries.



While draft-17 is the current draft version, it is binary compatible back to draft-14 and the -14 version is the last one that is marked as an implementation / interop draft.

But while binary compatible over the wire, the language in the spec drafts have changed somewhat so they are not identical behavior wise.

8.3.1. Missing implementations

The list of existing implementations still lacks some reputable brands. We have not heard anything official from Apple about support for HTTP/2 in Safari. The two immensely popular servers Apache HTTPD and Nginx both offer SPDY support but none of them have yet shown official HTTP/2 support.

Nginx says "we plan to release versions of nginx and NGINX Plus by the end of 2015 that will include support for HTTP/2"⁹. There's an early version of a HTTP/2 module for Apache called mod_h2¹⁰ claimed to be "Very alpha"

⁸ <https://github.com/HTTP2/HTTP2-spec/wiki/Implementations>

⁹ <http://nginx.com/blog/how-nginx-plans-to-support-HTTP/2/>

¹⁰ https://icing.github.io/mod_h2/

8.4. Common critiques of HTTP/2

During the development of this protocol the debate has been going back and forth and of course there is a certain amount of people who believe this protocol ended up completely wrong. I wanted to mention a few of the more common complaints and mention the arguments against them:

8.4.1. “The protocol is designed or made by Google”

It also has variations implying that the world gets even further dependent or controlled by Google by this. This isn't true. The protocol was developed within the IETF in the same manner that protocols have been developed for over 30 years. However, we all recognize and acknowledge Google's impressive work with SPDY that not only proved that it is possible to deploy a new protocol this way but also provided numbers illustrating what gains could be made.

Google has publicly announced¹¹ that they will remove support for SPDY and NPN in Chrome in 2016 and they urge servers to migrate to HTTP/2 instead.

8.4.2. “The protocol is only useful for browsers”

This is sort of true. One of the primary drivers behind the HTTP/2 development is the fixing of HTTP pipelining. If your use case originally didn't have any need for pipelining then chances are HTTP/2 won't do a lot of good for you. It certainly isn't the only improvement in the protocol but a big one.

As soon as services start realizing the full power and abilities the multiplexed streams over a single connection brings, I suspect we will see more application use of HTTP/2.

Small REST APIs and simpler programmatic uses of HTTP 1.x may not find the step to HTTP/2 to offer very big benefits. But also, there should be very few downsides with HTTP/2 for most users.

8.4.3. “The protocol is only useful for big sites”

Not at all. The multiplexing capabilities will greatly help to improve the experience for high latency connections that smaller sites without wide geographical distributions often offer. Large sites are already very often faster and more distributed with shorter round-trip times to users.

8.4.4. “Its use of TLS makes it slower”

This can be true to some extent. The TLS handshake does add a little extra, but there are existing and ongoing efforts on reducing the necessary round-trips even more for TLS. The overhead for doing TLS over the wire instead of plain-text is not insignificant and clearly notable so more CPU and power will be spent on the same traffic pattern as a non-secure protocol. How much and what impact it will have is a subject of opinions and

11 http://blog.chromium.org/2015/02/hello-HTTP/2-goodbye-spdy-http-is_9.html

measurements. See for example istlsfastyet.com for one source of info.

Telecom and other network operators, for example in the *ATIS Open Web Alliance*, say that they need unencrypted traffic¹² to offer caching, compression and other techniques necessary to provide a fast web experience over satellite, in airplanes and similar.

HTTP/2 does not make TLS use mandatory so we shouldn't conflate the terms.

Many Internet users have expressed a preference for TLS to be used more widely and we should help to protect users' privacy.

Experiments have also shown that by using TLS, there is a higher degree of success than when implementing new plain-text protocols over port 80 as there are just too many middle boxes out in the world that interfere with what they would think is HTTP 1.1 if it goes over port 80 and might look like HTTP at times.

Finally, thanks to HTTP/2's multiplexed streams over a single connection, normal browser use cases still could end up doing substantially fewer TLS handshakes and thus perform faster than HTTPS would when still using HTTP 1.1.

8.4.5. “Not being ASCII is a deal-breaker”

Yes, we like being able to see protocols in the clear since it makes debugging and tracing easier. But text based protocols are also more error prone and open up for much more parsing and parsing problems.

If you really can't take a binary protocol, then you couldn't handle TLS and compression in HTTP 1.x either and its been there and used for a very long time.

8.4.6. “It isn't any faster than HTTP/1.1”

This is of course subject to debate and discussions on how to measure what faster means, but already in the SPDY days many tests were made that proved faster browser page loads (like “How Speedy is SPDY?”¹³ by people at University of Washington and “Evaluating the Performance of SPDY-enabled Web Servers”¹⁴ by Hervé Servy) and such experiments have been repeated with HTTP/2 as well. I'm looking forward to seeing more such tests and experiments getting published. A basic first test made by httpwatch.com¹⁵ might imply that HTTP/2 holds its promises.

HTTP/2 is demonstrably faster in some scenarios, especially with high latency connections involving many objects and as shown in previous sections, the trend is heading towards even more objects and more data per site.

8.4.7. “It has layering violations”

Seriously, that's your argument? Layers are not holy untouchable pillars of a global

12 <http://www.atis.org/openweballiance/docs/OWAKickoffSlides051414.pdf> (page 26)

13 https://www.usenix.org/system/files/conference/nsdi14/nsdi14-paper-wang_xiao_sophia.pdf and https://www.usenix.org/sites/default/files/conference/protected-files/nsdi14_slides_wang.pdf

14 <http://www.neotys.com/blog/performance-of-spdy-enabled-web-servers/>

15 <http://blog.httpwatch.com/2015/01/16/a-simple-performance-comparison-of-https-spdy-and-http/2/>

religion and if we've crossed into a few gray areas when making HTTP/2 it has been in the interest of making a good and effective protocol within the given constraints.

8.4.8. "It doesn't fix several HTTP/1.1 shortcomings"

That's true. With the specific goal of maintaining HTTP/1.1 paradigms there were several old HTTP features that had to remain. Such as the common headers that also include the often dreaded cookies, authorization headers and more. But by the upside of maintaining these paradigms is that we got a protocol that is possible to deploy without an inconceivable amount of upgrade work that requires fundamental parts to be completely replaced or rewritten. HTTP/2 is basically just a new framing layer.

8.5. Will HTTP/2 become widely deployed?

It is too early to tell for sure, but I can still guess and estimate and that's what I'll do here.

The naysayers will say "look at how good IPv6 has done" as an example of a new protocol that's taken decades to just start to get widely deployed. HTTP/2 is not an IPv6 though. This is a protocol on top of TCP using the ordinary HTTP update mechanisms and port numbers and TLS etc. It will not require most routers or firewalls to change at all.

Google proved to the world with their SPDY work that a new protocol like this can be deployed and used by browsers and services with multiple implementations in a fairly short amount of time. While the amount of servers on the Internet that offer SPDY today is in the 1% range, the amount of data those servers deal with is much larger. Some of the absolutely most popular web sites today offer SPDY.

HTTP/2, based on the same basic paradigms as SPDY, I would say is likely to be deployed even more since it is an IETF protocol. SPDY deployment was always held back a bit by the "it is a Google protocol" stigma.

There are several big browsers behind the roll-out. Representatives from Firefox, Chrome and Internet Explorer have expressed they will ship HTTP/2 capable browsers and they have shown working implementations.

There are several big server operators that are likely to offer HTTP/2 soon, including Google, Twitter and Facebook and we hope to see HTTP/2 support soon get added to popular server implementations such as the Apache HTTP Server and nginx. H2o¹⁶ is a new blazingly fast HTTP server with HTTP/2 support that shows potential.

Some of the biggest proxy vendors, including HAProxy, Squid and Varnish have expressed their intentions to support HTTP/2.

I think there is likely to be even more implementations popping up once the spec becomes a ratified RFC.

In late January 2015, after Firefox 35 had shipped with HTTP/2 enabled by default and Chrome 40 had it enabled for 2% of its users, Google reported early and not statistically

16 <https://github.com/h2o/h2o>

safe numbers to me. They then saw HTTP/2 in roughly 5% of their global traffic. At the same time, Firefox 35 responses recorded HTTP/2 in about 9% of all responses.

9. HTTP/2 у Firefox-у

Firefox прати нацрте веома помно и пружа пробне имплементације HTTP/2 неколико месеци. Током развоја HTTP/2 протокола, клијенти и сервери морају да се договоре који нацрт ће користити што чини покретање тестова напорним. Имајте то на уму како би се ваш клијент и сервер сложили око нацрта који имплементирају.

9.1. Прво, будите сигурни да је укључен

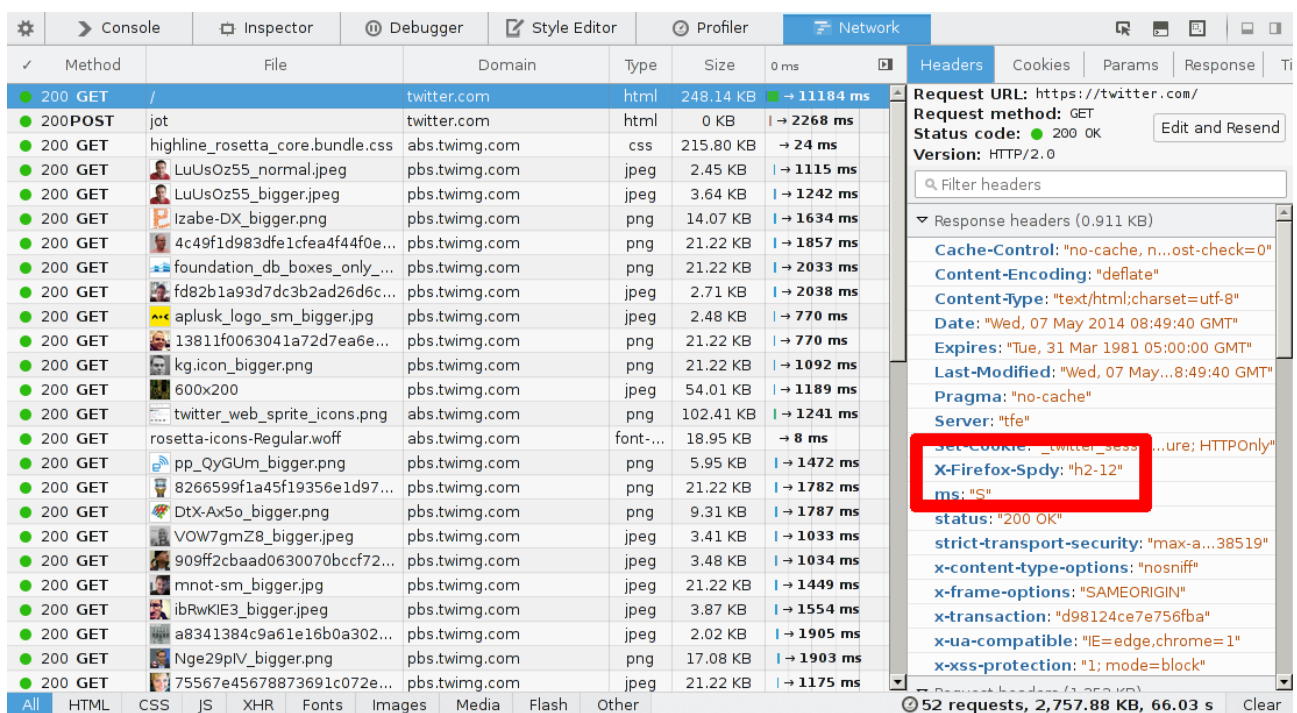
У свим верзијама Firefox-а од верзије 35, објављене 13. јануара 2015. године, HTTP/2 подршка је подразумевано укључена.

Унесите 'about:config' у вашу адресницу и потражите опцију "network.http.spdy.enabled.HTTP/2draft". Измените на **true**. Firefox 36 је додао још једну опцију "network.http.spdy.enabled.HTTP/2" која је подразумевано стављена на **true**. Друга контролише „обичну“ (нешифровану) верзију HTTP/2, док друга укључује или искључује преговоре између нацрта протокола. Обе су подразумевано **true** од Firefox верзије 36.

9.2. Само TLS

Запамтите да Firefox имплементира HTTP/2 само преко TLS-а. Видећете HTTP/2 у акцији само ако посетите <https://> сајтове са HTTP/2 подршком.

9.3. Невидљив!



The screenshot displays the Firefox Network Monitor interface. The 'Network' tab is active, showing a list of requests. The first request is a 200 GET to 'twitter.com' with a size of 248.14 KB and a time of 11184 ms. The 'Headers' panel on the right shows the response headers for this request. The 'X-Firefox-Spdy' header is highlighted with a red box, indicating the use of HTTP/2. Other headers include 'Cache-Control', 'Content-Encoding', 'Content-Type', 'Date', 'Expires', 'Last-Modified', 'Pragma', 'Server', 'Set-Cookie', 'strict-transport-security', 'x-content-type-options', 'x-frame-options', 'x-transaction', 'x-ua-compatible', and 'x-xss-protection'.

Method	File	Domain	Type	Size	0 ms
200 GET	/	twitter.com	html	248.14 KB	→ 11184 ms
200 POST	jot	twitter.com	html	0 KB	→ 2268 ms
200 GET	highline_rosetta_core.bundle.css	abs.twimg.com	css	215.80 KB	→ 24 ms
200 GET	LuUsOz55_normal.jpeg	pbs.twimg.com	jpeg	2.45 KB	→ 1115 ms
200 GET	LuUsOz55_bigger.jpeg	pbs.twimg.com	jpeg	3.64 KB	→ 1242 ms
200 GET	Izabe-DX_bigger.png	pbs.twimg.com	png	14.07 KB	→ 1634 ms
200 GET	4c49f1d983dfe1cfea4f44f0e...	pbs.twimg.com	png	21.22 KB	→ 1857 ms
200 GET	foundation_db_boxes_only_...	pbs.twimg.com	png	21.22 KB	→ 2033 ms
200 GET	fd82b1a93d7dc3b2ad26d6c...	pbs.twimg.com	jpeg	2.71 KB	→ 2038 ms
200 GET	aplusk_logo_sm_bigger.jpg	pbs.twimg.com	jpeg	2.48 KB	→ 770 ms
200 GET	13811f063041a72d7ea6e...	pbs.twimg.com	png	21.22 KB	→ 770 ms
200 GET	kg.icon_bigger.png	pbs.twimg.com	png	21.22 KB	→ 1092 ms
200 GET	600x200	pbs.twimg.com	jpeg	54.01 KB	→ 1189 ms
200 GET	twitter_web_sprite_icons.png	abs.twimg.com	png	102.41 KB	→ 1241 ms
200 GET	rosetta-icons-Regular.woff	abs.twimg.com	font-...	18.95 KB	→ 8 ms
200 GET	pp_QyGUm_bigger.png	pbs.twimg.com	png	5.95 KB	→ 1472 ms
200 GET	8266599f1a45f19356e1d97...	pbs.twimg.com	png	21.22 KB	→ 1782 ms
200 GET	DtX-Ax5o_bigger.png	pbs.twimg.com	png	9.31 KB	→ 1787 ms
200 GET	VOW7gmZ8_bigger.jpeg	pbs.twimg.com	jpeg	3.41 KB	→ 1033 ms
200 GET	909ff2cbaad0630070bccf72...	pbs.twimg.com	jpeg	3.48 KB	→ 1034 ms
200 GET	mnnot-sm_bigger.jpg	pbs.twimg.com	jpeg	21.22 KB	→ 1449 ms
200 GET	ibRwKIE3_bigger.jpeg	pbs.twimg.com	jpeg	3.87 KB	→ 1554 ms
200 GET	a8341384c9a61e16b0a302...	pbs.twimg.com	jpeg	2.02 KB	→ 1905 ms
200 GET	Nge29pIV_bigger.png	pbs.twimg.com	png	17.08 KB	→ 1903 ms
200 GET	75567e45678873691c072e...	pbs.twimg.com	jpeg	21.22 KB	→ 1175 ms

Илустрација 1: Снимак екрана који приказује HTTP/2 нацрт-12 у Firefox-у

Нема елемената у графичком интерфејсу који вам показују да користите HTTP/2. Не

можете да одредите тако лако. Један од начина да видите је да приступите “Web developer->Network” и проверите заглавља одговора и видите шта сте добили од сервера. Одговор је онда “HTTP/2.0” и Firefox ће додати своје заглавље са именом “X-Firefox-Spdy:” као што је показано на снимку екрана горе.

Заглавља која видите у алату „Мрежа“ када причате са HTTP/2 сајтом конвертују се из HTTP/2 бинарног формата у формат који личи на HTTP 1.x заглавља ради читљивости.

9.4. Визуализујте коришћење HTTP/2

Постоје Firefox додаци који помажу да видите да ли сајт користи HTTP/2. Један од њих се зове “SPDY Indicator”¹⁷.

¹⁷ <https://addons.mozilla.org/en-US/firefox/addon/spdy-indicator/>

10. HTTP/2 у Chromium-у

Chromium тим имплементирао је HTTP/2 и пружио је подршку за њега у развојним и бета каналима већ дуже време. Почевши од Chrome 40, објављеног 27. јануара 2015, HTTP/2 је подразумевано укључен за одређени број корисника. Тачан број корисника је почео од мале групе и увећавао се постепено како је време одмицало.

SPDY подршка ће бити уклоњена. У блог чланку, пројекат је објавио следеће фебруара 2015.¹⁸ године:

“Chrome је подржавао SPDY од Chrome верзије 6, али како су све предности присутне у HTTP/2, време је да се опростимо. Ми планирамо да уклонимо подршку за SPDY почетком 2016. године.”

10.1. Прво, будите сигурни да је укључен

Унесите “chrome://flags/#enable-spdy4” у адресницу вашег прегледача и кликните „укључи“ ако подешавање није већ укључено.

10.2. Само TLS

Запамтите да Chrome имплементира HTTP/2 само преко TLS-а. Ви ћете видети HTTP/2 у акцији у Chrome-у када идете на https:// сајтове који нуде HTTP/2 подршку.

10.3. Визуализујте коришћење HTTP/2

Постоје Chrome додаци који помажу да видите да ли сајт користи HTTP/2. Један од њих је “SPDY Indicator”¹⁹.

18 <http://blog.chromium.org/2015/02/hello-HTTP/2-goodbye-spdy-http-is-9.html>

19 <https://chrome.google.com/webstore/detail/spdy-indicator/mpbpobfflnpcgagijjhmgnchggcjblin>

11. HTTP/2 у curl-у

Curl пројекат нуди експерименталну подршку за HTTP/2 од септембра 2013.

У духу curl-а, ми намеравамо да подржимо отприлике сваки аспект HTTP/2 који можемо. Curl се често користи као алат за тестирање и чачкање по веб сајтовима и ми намеравамо да тако остане и за HTTP/2.

curl користи експерименталну библиотеку ngHTTP/2²⁰ за HTTP/2 frame слој функционалност.

11.1. HTTP 1.x двојник

Интернет, curl конвертује долазна HTTP/2 заглавља у HTTP 1.x заглавља и приказује их кориснику како би изгледали слично постојећем формату HTTP-а. То помаже лакшој транзицији за све што користи curl и HTTP данас. Слично томе curl конвертује одлазна заглавља. Проследите их у curl у HTTP 1.x стилу и он ће их конвертовати у лету када прича са HTTP/2 серверима. То такође помаже корисницима који не желе да се муче или не желе да размишљају која се верзија HTTP-а користи у преносу.

11.2. Прост текст није безбедан

curl подржава HTTP/2 преко стандардног TCP-а преко Upgrade: заглавља. Ако направите HTTP захтев и тражите HTTP/2, curl ће тражити од сервера да надогради везу на HTTP/2 ако је то могуће.

11.3. TLS and what libraries

curl supports a wide range of different TLS libraries for its TLS back-end, and that is still valid for HTTP/2 support. The challenge with TLS for HTTP/2's sake is the ALPN support and to some extent NPN support.

Build curl against modern versions of OpenSSL or NSS to get both ALPN and NPN support. Using GnuTLS or PolarSSL you will get ALPN support but not NPN.

11.4. Command line use

To tell curl to use HTTP/2, either plain text or over TLS, you use the **--HTTP/2** option (that is "dash dash HTTP/2"). curl still defaults to HTTP/1.1 so the extra option is necessary when you want HTTP/2.

11.5. libcurl options

Your application would use https:// or http:// URLs like normal, but you set curl_easy_setopt's CURLOPT_HTTP_VERSION option to CURL_HTTP_VERSION_2 to make libcurl attempt to use HTTP/2. It will then do a best effort and do HTTP/2 if it can, but otherwise continue to operate with HTTP 1.1.

²⁰ <https://nghttp2.org/>

12. После HTTP/2

Много тешких одлука и компромиса је направљено за HTTP/2.

A lot of tough decisions and compromises have been made for HTTP/2. With HTTP/2 getting deployed there is an established way to upgrade into other protocol versions that work which lays the foundation for doing more protocol revisions ahead. It also brings a notion and an infrastructure that can handle multiple different versions in parallel. Maybe we don't need to phase out the old entirely when we introduce new?

HTTP/2 still has a lot of HTTP 1 “legacy” brought with it into the future because of the desire to keep it possible to proxy traffic back and forth between HTTP 1 and HTTP/2. Some of that legacy hampers further development and inventions. Perhaps http3 can drop some of them?

What do you think is still lacking in http?

13. Даље читање

Ако вам се овај документ чини лаким и као да мањка техничких детаља, ево неколико додатних ресурса да утоле вашу радозналост:

- HTTPbis дописна лист и архива: <http://lists.w3.org/Archives/Public/ietf-http-wg/>
- HTTP/2 спецификација и нацрти; додатни документи од HTTPbis групе: <http://datatracker.ietf.org/wg/httpbis/>
- Firefox HTTP/2 мрежни детаљи: <https://wiki.mozilla.org/Networking/HTTP/2>
- curl HTTP/2 детаљи имплементације: <http://curl.haxx.se/dev/readme-HTTP/2.html>
- HTTP/2 сајт: <http://HTTP/2.github.io/> или прецизније ЧПП: <http://HTTP/2.github.io/faq/>

14. Хвала

Инспирација и Lego слика формата пакета од Marka Nottinghama.

HTTP статистика и тенденције <http://httparchive.org>.

The RTT graph comes from presentations done by Mike Belshe.

My kids Agnes and Rex for letting me borrow their Lego figures for the head of line picture.

Thanks to the following friends for reviews and feedback: Kjell Ericson, Bjorn Reese, Linus Swälas and Anthony Bryan. Your help is greatly appreciated and has really improved the document!

During the various iterations, the following friendly people have provided bug reports and improvements to the document: Mikael Olsson, Remi Gacogne, Benjamin Kircher, saivlis, florin-andrei-tp, Brett Anthoine, Nick Parlante, Matthew King, Nicolas Peels, Jon Forrest, sbrickey, Marcin Olak, Gary Rowe, Ben Frain, Mats Linander, Raul Siles