

HTTP Alternative Services 介绍

Aug 21, 2016

20 Comments

HTTP Alternative

Services (HTTP 替代服务) 是今年上半年由 IESG 通过的一项与 HTTP 有关的新协议。估计很少有人能从名字上猜

出它是用来干嘛的，本文从解决什么问题、如何使用以及真实场景下的应用三方面来介绍这份协议。

顺便说一下，HTTP 各种协议除了可以在 tools.ietf.org 找到，还可以前往 httpwg.org 查看。后者格式更丰富，阅读体验更好，例如本文介绍的 HTTP Alternative Services 协议也可以通过[这个地址](#)查看。

文章目录

- [解决什么问题](#)
- [如何使用](#)
- [真实案例](#)

解决什么问题

在 Web 系统中，我们经常有把用户导向不同服务器的需求，例如让不同地域的用户访问离自己最近的服务器。记得我刚上网那会儿，很多网站都会提供电信 / 网通等不同二级域名，供不同运营商用户选择，这无疑增加了使用成本。当前，一般网站都使用 DNS 服务来解决这个问题：按地域、运营商等条件，将用户 DNS 请求解析到最合适的 IP。这种方案需要配置合理的 TTL (Time To Live) 时间，太短会造成客户端频繁发起 DNS 查询，影响访问速度；太长则无法让 DNS 修改及时生效。

大型 Web 系统经常会出现某个机房流量过大，需要尽快分流给其它机房这种场景。这时候依靠修改 DNS 解析有点力不从心：一方面由于 DNS 缓存的存在，新的解析不能马上生效；另一方面

Jerry Qu

专注 WEB 端开发

[首页](#)

[专题](#)

[归档](#)

[友链](#)

[关于](#)



由于 HTTP 的 keep-alive 机制，已连接的浏览器还会继续使用之前解析到的 IP。

而 HTTP Alternative Services 可以很好地解决这个问题：服务端可以将自己的替代服务地址以协议规定的方式告诉浏览器，对于支持这个协议的浏览器来说，后续请求都会使用新地址。

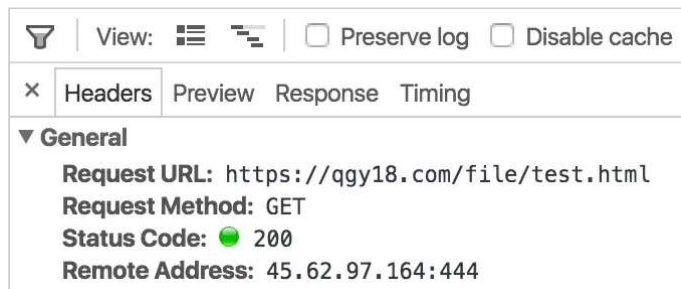
协议规定的替代服务地址由三部分组成：协议、主机名和端口。也就是说一个网站的替代服务，可以部署在不同 IP、不同端口，甚至使用不同协议。

不同于使用 30x 状态码进行重定向分流，**HTTP Alternative Services 只改变浏览器获取资源的网络方式，上层应用不会感觉到任何变化。**以下是两个示例：



(截图一：Firefox 48.0.1)

在截图一中，浏览器通过 TLS 加密通道发起了 HTTP/2 请求，但上层拿到的 Request URL 仍然是 http:// 开头的地址，浏览器地址栏也仍然显示为 http:// 。



(截图二：Chrome 54.0.2835.0 canary)

在截图二中，浏览器将请求发送给了服务器 444 端口，而上层拿到的 Request URL 没有任何变化。

Jerry Qu

专注 WEB 端开发

首页

专题

归档

友链

关于



如何使用

对于 HTTP/1，协议新增了一个响应头部 `Alt-Svc`，用来指定替代服务地址，它的基本格式如下：

```
Alt-Svc: h2="alt.example.com:8000",  
h2=":443"; ma=2592000; persist=1
```

`h2="alt.example.com:8000"` 这部分内容定义了替代服务使用的协议、主机名和端口，其中主机名和端口可选。多个替代服务之间用英文逗号分隔。

`ma` 是 `max-age` 的缩写，单位为秒。显然，它表示浏览器在指定时间内，可以直接使用替代服务地址。

协议还规定，当网络发生变化时（例如从 WIFI 切到 3G），浏览器必须弃用当前所有替代服务，除非定义了 `persist=1`。

对于 HTTP/2，协议新增了一个 `ALTSVC` 帧，具体定义这里略过。

可以看到，对于 HTTP/1 来说，`Alt-Svc` 头部必须依附于首次响应，只有从第二个请求开始浏览器才会使用替代服务地址；而在 HTTP/2 中，`ALTSVC` 帧可以独立发送，浏览器从首次请求开始就能用上新地址。

目前只有 Firefox 完整支持了 HTTP Alternative Services 协议，以下是在 Firefox 中的测试。

首次访问指定地址时，服务端返回了一个 `Alt-Svc` 头部，指定了替代服务地址：

Jerry Qu

专注 WEB 端开发

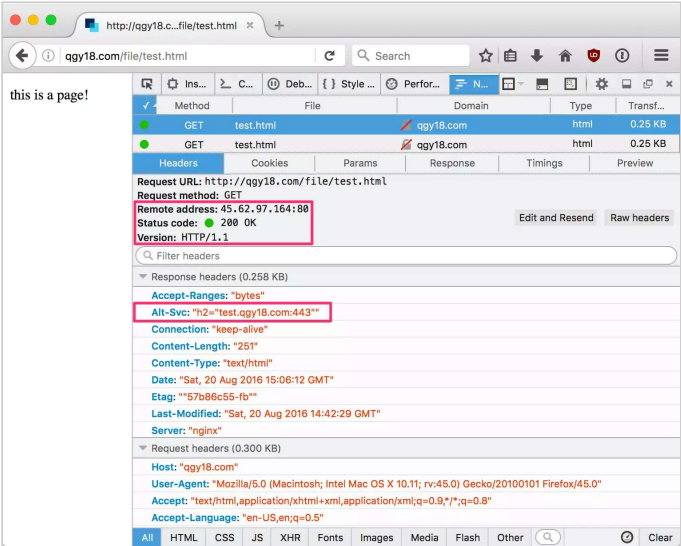
首页

专题

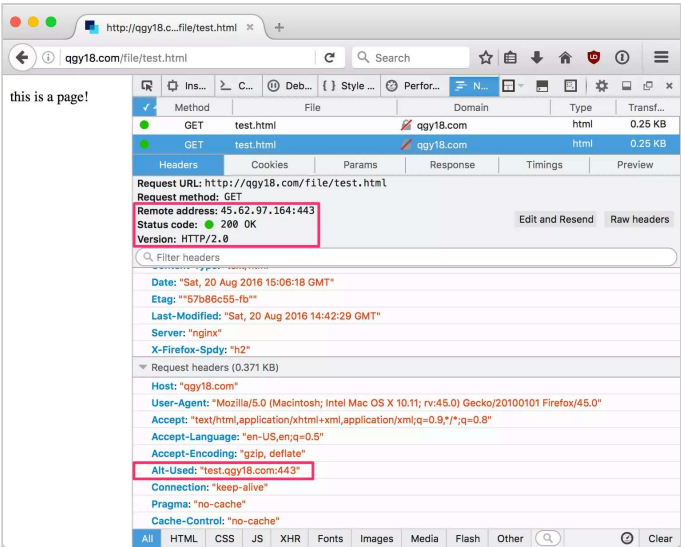
归档

友链

关于



再次访问时，浏览器就会使用替代服务地址中指定的协议、主机名和端口发起请求。这一切对上层应用透明，但发往替代服务的请求头部，会多出一个 Alt-Used 字段：

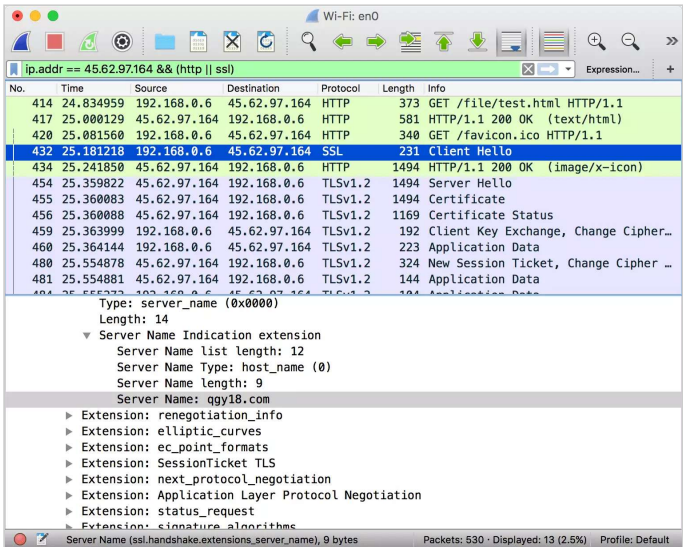


需要注意的是，尽管我使用 test.qgy18.com 做为替代服务主机名，但浏览器在向替代服务发起请求时，仍然会使用当前页面的主机名。以下是 Wireshark 抓到的信息，SNI 依然是

qgy18.com：

Jerry Qu
专注 WEB 端开发

- 首页
- 专题
- 归档
- 友链
- 关于



出于安全考虑，协议提出了两点要求：1）所有替代服务必须基于 TLS 部署；2）原网站为 HTTPS 的情况下，替代服务必须使用原网站证书部署。特别地，在 Chrome 中，只有 HTTPS 原网站才能使用替代服务。

真实案例

Firefox 37 基于 HTTP Alternative Services 协议提出了一个非常有意思的方案：[Opportunistic Encryption](#)（不知道怎么翻译，请读者自己意会，后续简称为 OE），我们一起来看下。

我们知道对于 HTTPS 而言，如果没有证书信任链校验机制，无法抵御 MITM（中间人）攻击。但 Firefox 认为，不校验证书的 TLS 网站怎么也比纯明文传输要强，对于那些短期内无法切换到 HTTPS 的网站来说，OE 提供了一种可以使用 TLS 进行传输加密，但不进行证书校验的折衷方案。

实施这个方案只需以下两步：

- 部署 HTTP/2 over TLS 服务，允许使用自签名证书；
- 给网站响应头部加上：`Alt-Svc: h2=":443"; ma=600`；

Jerry Qu
专注 WEB 端开发

- 首页
- 专题
- 归档
- 友链
- 关于



当用户通过 `http://yourdomain.com` 访问网站时，对于能够识别 `Alt-Svc` 的浏览器来说，后续所有流量都会使用新协议（`HTTP/2 over TLS`）、新端口（`443`）。同时对于上层应用来说，URL 依然是 `http://yourdomain.com`，没有任何变化。也就是说，OE 在提升安全性和性能的同时，无需对 Web 应用代码作出任何修改。

但在 OE 中，用户首次访问还是走的 HTTP，响应很容易就被篡改，从而去掉 `Alt-Svc` 头部；即便是后续使用基于 TLS 部署的替代服务地址，由于浏览器不校证书，还是很容易被攻击。所以，它只能将 HTTP 网站从**极不安全**提升到**不安全**，作用有限。

有趣的是，Firefox 37 推出 OE 之后，很快就被发现存在巨大的安全问题，官方不得不迅速推出 37.0.1 来禁用 OE。当然，产生问题的原因是代码实现上的疏忽，修复 Bug 后，Firefox 又重新启用了它。

Chrome 并不打算支持 Opportunistic Encryption，考虑 Firefox 当前的市场占有率，我个人觉得对于 OE 方案，大家了解下就可以了。

本文链接：<https://imququ.com/post/http-alt-svc.html>，[参与评论](#) »

--EOF--

发表于 2016-08-21 22:27:29，并被添加

「[HTTP](#)、[HTTPS](#)、[协议](#)」标签。[查看本文 Markdown 版本](#) »

本站使用「[署名 4.0 国际](#)」创作共享协议，[相关说明](#) »

专题「HTTP 相关」的其他文章 »

- [关于启用 HTTPS 的一些经验分享](#)
(三) (May 05, 2016)

Jerry Qu

专注 WEB 端开发

[首页](#)

[专题](#)

[归档](#)

[友链](#)

[关于](#)



- [如何压缩 HTTP 请求正文](#) (Apr 18, 2016)
- [HTTP 协议中的 Content-Encoding](#) (Apr 17, 2016)
- [三种解密 HTTPS 流量的方法介绍](#) (Mar 28, 2016)
- [HTTP Public Key Pinning 介绍](#) (Mar 05, 2016)
- [关于启用 HTTPS 的一些经验分享 \(二\)](#) (Dec 22, 2015)
- [关于启用 HTTPS 的一些经验分享 \(一\)](#) (Dec 04, 2015)
- [HTTP 代理原理及实现 \(二\)](#) (Nov 20, 2015)
- [HTTP 代理原理及实现 \(一\)](#) (Nov 20, 2015)
- [Content Security Policy Level 2 介绍](#) (Oct 05, 2015)

[« 谈谈 Nginx 的 HTTP/2 POST Bug](#)
[开始使用 ECC 证书 »](#)

Comments [「切换到评论浏览模式」](#)

Comments 在线社区 1 Login ▾

♥ Recommend ↗ Share 按从新到旧排序 ▾

Join the discussion...



依云 • 2个月前



CloudFlare 默认支持了！不过过期时间好短.....

另外，好像设置代理服务器之后，火狐就不会使用 Alt-Svc 了？

1 ^ | ▾ • Reply • Share ▸



xiaohui lam • 4个月前



屈老板你知道的好多啊~~

^ | ▾ • Reply • Share ▸



lony • 4个月前



这样的话，我可以免备案使用国内的主机

Jerry Qu
专注 WEB 端开发

首页
专题
归档
友链
关于



非80和443端口来做代替服务器，加快网站访问速度，不支持的浏览器就直接是国外的资源。

^ | v • Reply • Share ›



依云 → lony • 3个月前



这个主意好棒～

^ | v • Reply • Share ›



Jerry Qu Mod → lony



• 4个月前

对，替代服务本来就是为就近访问这个场景而设计的。

^ | v • Reply • Share ›



lony → Jerry Qu



• 4个月前

虽然我几乎看不懂英文，但我随便看了一下，好像这个新的主机名就是指 DNS 的 CNAME 主机名

^ | v • Reply • Share ›



lony → Jerry Qu



• 4个月前

你上面所说的，使用用新的域名 test.qgy18.com 做为替代服务主机名，浏览器认为这个域名只是 CNAME 而已吧，并不是用来请求的主机名。

^ | v • Reply • Share ›



Lan Tian • 4个月前



可以拿来做国内主机免备案

^ | v • Reply • Share ›



王琪亮 → Lan Tian • 4个月前



国内某些云的备案白名单防火墙会 http 抢答我会乱说。我在腾讯等都碰过这种壁。

^ | v • Reply • Share ›



Lan Tian → 王琪亮



• 4个月前

这些替代服务都是必须加上 SSL 的

SSL 面前什么白名单都是辣鸡


Jerry Qu
专注 WEB 端开发


- 首页
- 专题
- 归档
- 友链
- 关于




实在不行不要用80和443就行

^ | v • Reply • Share ›

 **王琪亮** → Lan Tian • 4个月前
不排除首先访问80端口的首次访客被你挡外面了。
^ | v • Reply • Share ›


 **Lan Tian** → 王琪亮 • 4个月前
域名解析到海外反代服务器上，反代服务器向客户端发指令将请求转到国内服务器的特定端口
这样即使用户浏览器不支持HTTP替代服务也可以访问网站，只是速度会慢
^ | v • Reply • Share ›

 **liwanglin12** • 4个月前
“考虑 Firefox 当前的市场占有率，我个人觉得对于 OE 方案，大家了解下就可以了。”
这是 Firefox 被黑的最惨的一次 233333
^ | v • Reply • Share ›

 **王琪亮** → liwanglin12 • 4个月前
好歹市占率 >10% 2333333
纠正:大于20%
^ | v • Reply • Share ›

Jerry Qu
专注 WEB 端开发

- 首页
- 专题
- 归档
- 友链
- 关于

 **Jerry Qu** Mod → 王琪亮 • 4个月前
因为在 Chrome 中，只有 HTTPS 原网站才能使用替代服务，也就是说 Chrome 无论如何也不可能支持 OE 方案。
所以与其提供一个只服务于小部分用户且不那么安全的方案，还不如想办法切换到全站 HTTPS。



对于 **Firefox**，我还是有感情的，毕竟从 **Firefox 1.5** 开始用，至少有七年之久。

© 2016 - JerryQu 的小站 - 京 ICP 备 15046275 号

Powered by [ThinkJS](#) & [GreyShade](#)

Jerry Qu
专注 WEB 端开发

- 首页
- 专题
- 归档
- 友链
- 关于