HTTP Header简介

HTTP

超文本传输协议（HTTP，HyperText Transfer Protocol)是互联网上应用最为广泛的一种网络协议。所有的WWW文件都必须遵守这个标准。HTTP协议采用了请求/响应模 型，浏览器或其他客户端发出请求，服务器给与响应。就整个网络资源传输而言，包括message-header和message-body两部分。首先传 递message-header，即**http header**消息。http header 消息通常被分为4个部分：general header, request header, response header, entity header。但是这种分法就理解而言，感觉界限不太明确。根据维基百科对http header内容的组织形式，大体分为Request和Response两部分。

HTTP Header

协议头的字段(Header)，是在请求（request）或回复（response）那一行（这是一条消息的第一行内容）内容之后传输的。协议头的字段，是以明文的格式传输的，以冒号分隔的键名/值对，最后以回车(CR)和换行(LF)符序列结尾。协议头部分的结束，是以一个空白的字段来标识的，结果就是，会传输两个连续的回车换行符对。 在标准的网络请求中没有针对每个协议头字段的名字和值的尺寸设置任何限制， 也没有限制字段的个数。然而 ， 出于实际场景及安全性的考虑，大部分的服务器、客户端和代理软件都会实施一些限制。例如， 阿帕奇（Apache）2.3 服务器， 在默认情况下， 会限制每个字段的尺寸不超过 8190字节 ， 同时，单个请求中最多可以有 100 个协议头字段。

请求字段(Request)

协议头字段(Header)	说明	示例
Accept	能够接受的回应内容类型（Content-Types）。	Accept: text/plain
Accept-Charset	能够接受的字符集	Accept-Charset: utf-8
Accept-Encoding	能够接受的编码方式列表。	Accept-Encoding:gzip, deflate
Accept-Language	能够接受的回应内容的自然语言列表。	Accept-Language: en-US
Accept-Datetime	能够接受的按照时间来表示的版本	Accept-Datetime: Thu, 31 May 2007 20:35:00 GMT
Authorization	用于超文本传输协议的认证的认证信息	Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
Cache-Control	用来指定在这次的请求/回复链中的所有缓存机制 都必须 遵守的指令	Cache-Control: no-cache
Connection	该浏览器想要优先使用的连接类型	Connection: keep-alive Connection: Upgrade
Cookie	之前由服务器通过 Set- Cookie	Cookie: $Version=1; Skin=new;
Content-Length	以 八位字节数组 （8位的字节）表示的请求体的长度	Content-Length: 348
Content-MD5	请求体的内容的二进制 MD5 散列值，以 Base64 编码的结果	Content-MD5: Q2hlY2sgSW50ZWdyaXR5IQ==
Content-Type	请求体的 多媒体类型 （用于POST和PUT请求中）	Content-Type: application/x-www-form-urlencoded
Date	发送该消息的日期和时间(按照 RFC 7231 中定义的"超文本传输协议日期"格式来发送)	Date: Tue, 15 Nov 1994 08:12:31 GMT
Expect	表明客户端要求服务器做出特定的行为	Expect: 100-continue
From	发起此请求的用户的邮件地址	From: user@example.com

协议头字段(Header)	说明	示例
Host	服务器的域名(用于虚拟主机），以及服务器所监听的传输控制协议端口号。如果所请求的端口是对应的服务的标准端口，则端口号可被省略。 自超文件传输协议版本1.1（HTTP/1.1）开始便是必需字段。	Host:en.wikipedia.org:80 Host: en.wikipedia.org
If-Match	仅当客户端提供的实体与服务器上对应的实体相匹配时，才进行对应的操作。主要作用时，用作像 PUT 这样的方法中，仅当从用户上次更新某个资源以来，该资源未被修改的情况下，才更新该资源。	If-Match: "737060cd8c284d8af7ad3082f209582d"
If-Modified-Since	允许在对应的内容未被修改的情况下返回304 未修改（ 304 Not Modified ）	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
If-None-Match	允许在对应的内容未被修改的情况下返回304 未修改（ 304 Not Modified ），参考 超文本传输协议 的实体标记	If-None-Match: "737060cd8c284d8af7ad3082f209582d"
If-Range	如果该实体未被修改过，则向我发送我所缺少的那一个或多个部分；否则，发送整个新的实体	If-Range: "737060cd8c284d8af7ad3082f209582d"
If-Unmodified-Since	仅当该实体自某个特定时间已来未被修改的情况下，才发送回应。	If-Unmodified-Since: Sat, 29 Oct 1994 19:43:31 GMT
Max-Forwards	限制该消息可被代理及网关转发的次数。	Max-Forwards: 10
Origin	发起一个针对 跨来源资源共享 的请求（要求服务器在回应中加入一个‘访问控制-允许来源’（'Access-Control-Allow-Origin'）字段）。	Origin: http://www.example-social-network.com
Pragma	与具体的实现相关，这些字段可能在请求/回应链中的任何时候产生 多种效果。	Pragma: no-cache
Proxy-Authorization	用来向代理进行认证的认证信息。	Proxy-Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==

协议头字段 (Header)	说明	示例
Range	仅请求某个实体的一部分。字节偏移以0开始。参考 字节服务 。	Range: bytes=500-999
Referer [*sic*]	表示浏览器所访问的前一个页面，正是那个页面上的某个链接将浏览器带到了当前所请求的这个页面。(“引导者”（“referrer”）这个单词，在RFC 中被拼错了，因此在大部分的软件实现中也拼错了，以至于，错误的拼法成为了标准的用法，还被当成了正确的术语)	Referer: http://en.wikipedia.org/wiki/Main_Page
TE	浏览器预期接受的传输编码方式：可使用回应协议头Transfer-Encoding 字段中的那些值，另外还有一个值可用，"trailers"（与" 分块 "传输方式相关），用来表明，浏览器希望在最后一个尺寸为0的块之后还接收到一些额外的字段。	TE: trailers, deflate
User-Agent	浏览器的身份标识字符串	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:12.0) Gecko/20100101 Firefox/21.0
Upgrade	要求服务器升级到另一个协议。	Upgrade: HTTP/2.0, SHTTP/1.3, IRC/6.9, RTA/x11
Via	向服务器告知，这个请求是由哪些代理发出的。	Via: 1.0 fred, 1.1 example.com (Apache/1.1)
Warning	一个一般性的警告，告知，在实体内容体中可能存在错误。	Warning: 199 Miscellaneous warning

常见的非标准请求字段

字段名	说明	示例
X-Requested-With	主要用于标识 Ajax 及可扩展标记语言 请求。大部分的JavaScript框架会发送这个字段，且将其值设置为XMLHttpRequest	X-Requested-With: XMLHttpRequest
DNT	请求某个网页应用程序停止跟踪某个用户。在火狐浏览器中，相当于X-Do-Not-Track协议头字段(自 火狐4.0 测试（Beta） 11版开始支持)。 Safari 和 Internet Explorer 9 也支持这个字段。在2011 年三月7 日，有人向互联网工程任务组提交了一个草案。万维网协会 的跟踪保护工作组正在就此制作一项规范。	DNT: 1 (Do Not Track Enabled) DNT: 0 (Do Not Track Disabled)
X-Forwarded-For	一个事实标准 ，用于标识某个通过超文本传输协议代理或负载均衡连接到某个网页服务器的客户端的原始互联网地址	X-Forwarded-For: client1, proxy1, proxy2 X-Forwarded-For: 129.78.138.66, 129.78.64.103
X-Forwarded-Host	a *de facto* standard for identifying the original host requested by the client in the HostHTTP request header, since the host name and/or port of the reverse proxy (load balancer) may differ from the origin server handling the request.	X-Forwarded-Host: en.wikipedia.org:80 X-Forwarded-Host: en.wikipedia.org
X-Forwarded-Proto	一个事实标准 用于标识某个超文本传输协议请求最初所使用的协议，因为，在反向代理(负载均衡)上，即使最初发往该反向代理的请求类型是安全的超文本传输协议（HTTPS），该反向代理也仍然可能会使用超文本传输协议（HTTP）来与网页服务器通信。谷歌客户端在与谷歌服务器通信时会使用该协议头的一个替代形式（X-ProxyUser-Ip）。	X-Forwarded-Proto: https
Front-End-Https	Non-standard header field used by Microsoft applications and load-balancers	Front-End-Https: on
X-Http-Method-Override	请求某个网页应用程序使用该协议头字段中指定的方法（一般是PUT或DELETE）来覆盖掉在请求中所指定的方法（一般是POST）。当某个浏览器或防火墙阻止直接发送PUT 或DELETE 方法时（注意，这可能是因为软件中的某个漏洞，因而需要修复，也可能是因为某个配置选项就是如此要求的，因而不应当设法绕过），可使用这种方式。	X-HTTP-Method-Override: DELETE

字段名	说明	示例
X-ATT-DeviceId	Allows easier parsing of the MakeModel/Firmware that is usually found in the User-Agent String of AT&T Devices	X-Att-Deviceid: GT-P7320/P7320XXLPG
X-Wap-Profile	Links to an XML file on the Internet with a full description and details about the device currently connecting. In the example to the right is an XML file for an AT&T Samsung Galaxy S2.	x-wap-profile**http://wap.samsungmobile.com/uaprof/SGH-I777.xml**
Proxy-Connection	因为对超文本传输协议规范的误解而实现的一个协议头。因为早期超文本传输协议版本实现中的错误而出现。与标准的连接（Connection）字段的功能完全相同。	Proxy-Connection: keep-alive
X-UIDH	Server-side deep packet insertion of a unique ID identifying customers ofVerizon Wireless; also known as "perma-cookie" or "supercookie"	X-UIDH: ...
X-Csrf-Token	Used to prevent cross-site request forgery. Alternative header names are:X-CSRFTokenand X-XSRF-TOKEN	X-Csrf-Token: i8XNjC4b8KVok4uw5RftR38Wgp2BFwql

回应字段(Response)

回应头字段(Header)	说明	示例
Access-Control-Allow-Origin	指定哪些网站可参与到 跨来源资源共享 过程中	Access-Control-Allow-Origin: *
Accept-Patch	Specifies which patch document formats this server supports	Accept-Patch: text/example;charset=utf-8
Accept-Ranges	这个服务器支持哪些种类的部分内容范围	Accept-Ranges: bytes
Age	这个对象在 代理缓存 中存在的时间，以秒为单位	Age: 12
Allow	对于特定资源有效的动作。针对405不允许该方法（405 Method not allowed）而使用	Allow: GET, HEAD
Cache-Control	向从服务器直到客户端在内的所有缓存机制告知，它们是否可以缓存这个对象。其单位为秒	Cache-Control: max-age=3600
Connection	针对该连接所预期的选项	Connection: close
Content-Disposition	An opportunity to raise a "File Download" dialogue box for a known MIME type with binary format or suggest a filename for dynamic content. Quotes are necessary with special characters.	Content-Disposition: attachment; filename="fname.ext"
Content-Encoding	在数据上使用的编码类型。参考 超文本传输协议压缩 。	Content-Encoding: gzip
Content-Language	内容所使用的语言	Content-Language: da
Content-Length	回应消息体的长度，以 字节 （8位为一字节）为单位	Content-Length: 348
Content-Location	所返回的数据的一个候选位置	Content-Location: /index.htm
Content-MD5	回应内容的二进制 MD5 散列，以 Base64 方式编码	Content-MD5: Q2hlY2sgSW50ZWdyaXR5IQ==
Content-Range	这条部分消息是属于某条完整消息的哪个部分	Content-Range: bytes 21010-47021/47022
Content-Type	当前内容的MIME类型	Content-Type: text/html; charset=utf-8
Date	此条消息被发送时的日期和时间(按照 RFC 7231 中定义的“超文本传输协议日期”格式来表示)	Date: Tue, 15 Nov 1994 08:12:31 GMT

回应头字段(Header)	说明	示例
ETag	对于某个资源的某个特定版本的一个标识符，通常是一个 消息散列	ETag: "737060cd8c284d8af7ad3082f209582d"
Expires	指定一个日期/时间，超过该时间则认为此回应已经过期	Expires: Thu, 01 Dec 1994 16:00:00 GMT
Last-Modified	所请求的对象的最后修改日期(按照 RFC 7231 中定义的“超文本传输协议日期”格式来表示)	Last-Modified: Tue, 15 Nov 1994 12:45:26 GMT
Link	用来表达与另一个资源之间的类型关系，此处所说的类型关系是在 RFC 5988 中定义的	Link: ; rel="alternate"
Location	用来进行重定向，或者在创建了某个新资源时使用。	Location: http://www.w3.org/pub/WWW/People.html
P3P	This field is supposed to set P3P policy, in the form ofP3P:CP="your_compact_policy". However, P3P did not take off, most browsers have never fully implemented it, a lot of websites set this field with fake policy text, that was enough to fool browsers the existence of P3P policy and grant permissions for third party cookies.	P3P: CP="This is not a P3P policy!See http://www.google.com/support/accounts/bin/answer.py?hl=en&answer=151657 for more info."
Pragma	与具体的实现相关，这些字段可能在请求/回应链中的任何时候产生多种效果。	Pragma: no-cache
Proxy-Authenticate	要求在访问代理时提供身份认证信息。	Proxy-Authenticate: Basic
Public-Key-Pins	用于缓解 中间人攻击，声明网站的认证用的 传输 层安全协议 证书的散列值	Public-Key-Pins: max-age=2592000; pin-sha256="E9CZ9INDbd+2eRQozYqqbQ2yXLVKB9+xcprMF+44U1g=";
Refresh	Used in redirection, or when a new resource has been created. This refresh redirects after 5 seconds.	Refresh: 5; url=http://www.w3.org/pub/WWW/People.html
Retry-After	如果某个实体临时不可用，则，此协议头用来告知客户端日后重试。其值可以是一个特定的时间段(以秒为单位)或一个超文本传输协议日期。	Example 1: Retry-After: 120 Example 2: Retry-After: Fri, 07 Nov 2014 23:59:59 GMT
Server	服务器的名字	Server: Apache/2.4.1 (Unix)
Set-Cookie	HTTP cookie	Set-Cookie: UserID=JohnDoe; Max-Age=3600; Version=1
Status	通用网关接口 协议头字段，用来说明当前这个超文本传输协议回应的 状态 。普通的超文本传输协议回应，会使用单独的“状态行”（"Status-Line"）作为替代，这一点是在 RFC 7230 中定义的。	Status: 200 OK
Strict-Transport-Security	A HSTS Policy informing the HTTP client how long to cache the HTTPS only policy and whether this applies to subdomains.	Strict-Transport-Security: max-age=16070400; includeSubDomains
Trailer	The Trailer general field value indicates that the given set of header fields is present in the trailer of a message encoded with chunked transfer coding.	Trailer: Max-Forwards

回应头字段(Header)	说明	示例
Transfer-Encoding	用来将实体安全地传输给用户的编码形式。 当前定义 的方法 包括： 分 块 、压缩（compress）、缩小（deflate）、压缩（gzip）、实体（identity）。	Transfer-Encoding: chunked
pgrade	要求客户端升级到另一个协议。	Upgrade: HTTP/2.0, SHTTP/1.3, IRC/6.9, RTA/x11
Vary	告知下游的代理服务器，应当如何对未来的请求协议头进行匹配，以决定是否可使用已缓存的回应内容而不是重新从原始服务器请求新的内容。	Vary: *
Via	告知代理服务器的客户端，当前回应是通过什么途径发送的。	Via: 1.0 fred, 1.1 example.com (Apache/1.1)
Warning	一般性的警告，告知在实体内容体中可能存在错误。	Warning: 199 Miscellaneous warning
WWW-Authenticate	表明在请求获取这个实体时应当使用的认证模式。	WWW-Authenticate: Basic
X-Frame-Options	Clickjacking protection: deny- no rendering within a frame, sameorigin - no rendering if origin mismatch, allow-from - allow from specified location,allowall - non-standard, allow from any location	X-Frame-Options: deny

常见的非标准回应字段

字段名	说明	示例
X-XSS-Protection	跨站脚本攻击 (XSS)过滤器	X-XSS-Protection: 1;mode=block
Content-Security-Policy, *X-Content-Security-Policy* , *X-WebKit-CSP*	内容安全策略定义。	X-WebKit-CSP: default-src 'self'
X-Content-Type-Options	The only defined value, "nosniff", prevents Internet Explorer from MIME-sniffing a response away from the declared content-type. This also applies to Google Chrome, when downloading extensions.	X-Content-Type-Options: nosniff
X-Powered-By	表明用于支持当前网页应用程序的技术（例如PHP）（版本号细节通常放置在 X-Runtime 或 X-Version 中）	X-Powered-By: PHP/5.4.0
X-UA-Compatible	Recommends the preferred rendering engine (often a backward-compatibility mode) to use to display the content. Also used to activate Chrome Frame in Internet Explorer.	X-UA-Compatible: IE=EmulateIE7 X-UA-Compatible: IE=edge X-UA-Compatible: Chrome=1
X-Content-Duration	Provide the duration of the audio or video in seconds; only supported by Gecko browsers	X-Content-Duration: 42.666