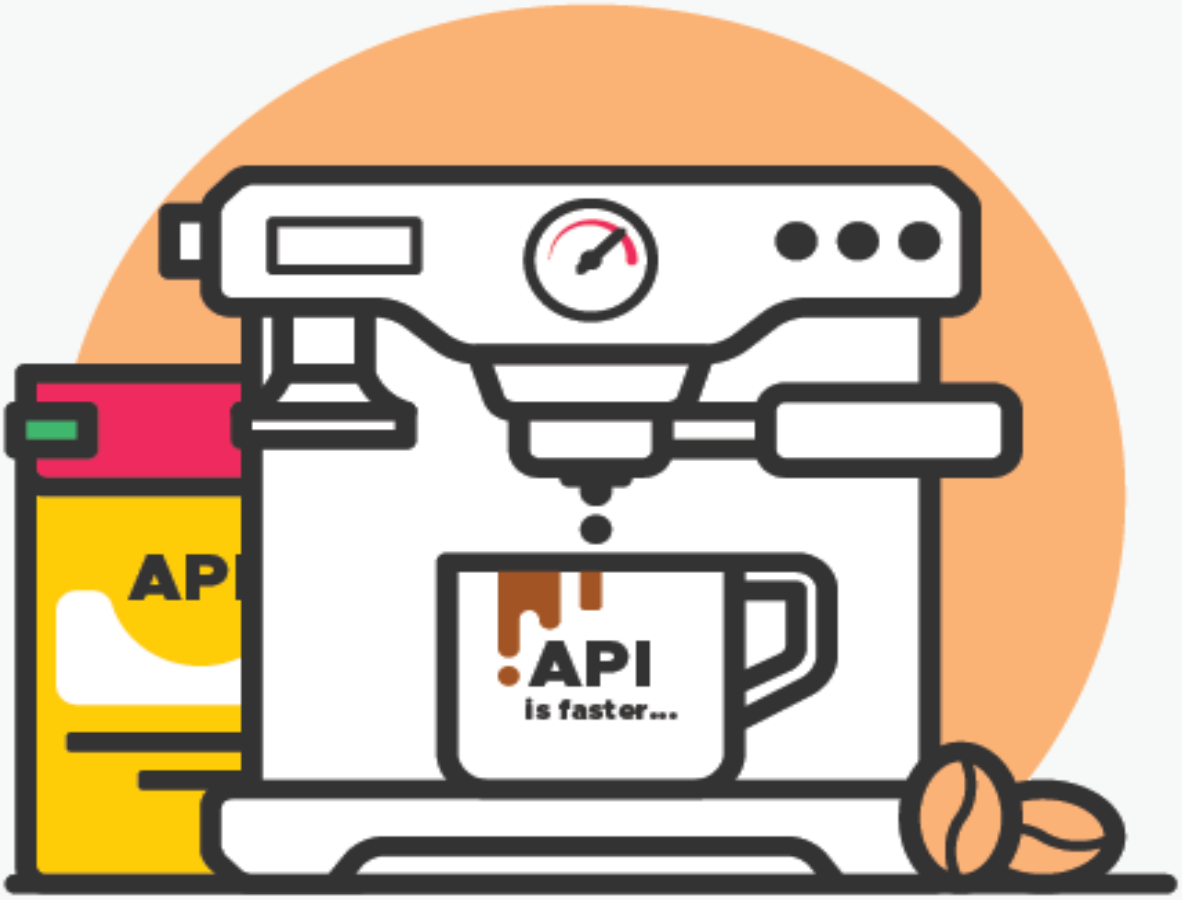
LIMITED
BUNDLE EDITION

Marinko Spasojevic
Vladimir Pecanac

THE HTTP REFERENCE TABLES

Make API Faster Than Your Morning Coffee



Made with ♥ by: CodeMaze

THE HTTP REFERENCE TABLES

This reference is a bonus material that will help you develop your API more quickly. We compiled everything related to HTTP so you don’t ever need to search the internet for a status code or anything else related to HTTP inside your API.

Request Methods

Method	Description	Has body?
CONNECT	This specification reserves the method name CONNECT for use with a proxy that can dynamically switch to being a tunnel (e.g. SSL tunneling).	No
DELETE	The DELETE method requests that the origin server delete the resource identified by the Request-URI.	No
GET	The GET method retrieves whatever information (in the form of an entity) is identified by the Request-URI.	No
HEAD	The HEAD method is identical to GET except that the server MUST NOT return a message-body in the response.	No
OPTIONS	The OPTIONS method represents a request for information about the communication options available on the request/response chain identified by the Request-URI.	No
POST	The POST method is used to request that the origin server accept the entity enclosed in the request as a new subordinate of the resource identified by the Request-URI in the Request-Line.	Yes
PUT	The PUT method requests that the enclosed entity be stored under the supplied Request-URI.	Yes
TRACE	The TRACE method is used to invoke a remote, application-layer loop-back of the request message.	No

Status Codes

These two tables define status code ranges (classification) and describe all the status codes.

Status Code Classification

Overall range	Defined range	Category
100-199	100-101	Informational
200–299	200–206	Successful
300–399	300–305	Redirection
400–499	400–415	Client error
500–599	500–505	Server error

Status Codes

Status code	Reason phrase	Meaning
100	Continue	An initial part of the request was received, and the client should continue.
101	Switching Protocols	The server is changing protocols, as specified by the client, to one listed in the Upgrade header.
200	OK	The request is okay.
201	Created	The resource was created (for requests that create server objects).
202	Accepted	The request was accepted, but the server has not yet performed any action with it.
203	Non-Authoritative Information	The transaction was okay, except the information contained in the entity headers was not from the origin server, but from a copy of the resource.
204	No Content	The response message contains headers and a status line, but no entity body.
205	Reset Content	Another code primarily for browsers; basically means that the browser should clear any HTML form elements on the current page.
206	Partial Content	A partial request was successful.
300	Multiple Choices	A client has requested a URL that actually refers to multiple resources. This code is returned along with a list of options; the user can then select which one he wants.

Status code	Reason phrase	Meaning
301	Moved Permanently	The requested URL has been moved. The response should contain a Location URL indicating where the resource now resides.
302	Found	Like the 301 status code, but the move is temporary. The client should use the URL given in the Location header to locate the resource temporarily.
303	See Other	Tells the client that the resource should be fetched using a different URL. This new URL is in the Location header of the response message.
304	Not Modified	Clients can make their requests conditional by the request headers they include. This code indicates that the resource has not changed.
305	Use Proxy	The resource must be accessed through a proxy, the location of the proxy is given in the Location header.
306	(Unused)	This status code currently is not used.
307	Temporary Redirect	Like the 301 status code; however, the client should use the URL given in the Location header to locate the resource temporarily.
400	Bad Request	Tells the client that it sent a malformed request.
401	Unauthorized	Returned along with appropriate headers that ask the client to authenticate itself before it can gain access to the resource.
402	Payment Required	Currently this status code is not used, but it has been set aside for future use.
403	Forbidden	The request was refused by the server.
404	Not Found	The server cannot find the requested URL.
405	Method Not Allowed	A request was made with a method that is not supported for the requested URL. The Allow header should be included in the response to tell the client what methods are allowed on the requested resource.
406	Not Acceptable	Clients can specify parameters about what types of entities they are willing to accept. This code is used when the server has no resource matching the URL that is acceptable for the client.
407	Proxy Authentication Required	Like the 401 status code, but used for proxy servers that require authentication for a resource.
408	Request Timeout	If a client takes too long to complete its request, a server can send back this status code and close down the connection.
409	Conflict	The request is causing some conflict on a resource.

Status code	Reason phrase	Meaning
410	Gone	Like the 404 status code, except that the server once held the resource.
411	Length Required	Servers use this code when they require a Content-Length header in the request message. The server will not accept requests for the resource without the Content-Length header.
412	Precondition Failed	If a client makes a conditional request and one of the conditions fails, this response code is returned.
413	Request Entity Too Large	The client sent an entity body that is larger than the server can or wants to process.
414	Request URI Too Long	The client sent a request with a request URL that is larger than what the server can or wants to process.
415	Unsupported Media Type	The client sent an entity of a content type that the server does not understand or support.
416	Requested Range Not Satisfiable	The request message requested a range of a given resource, and that range either was invalid or could not be met.
417	Expectation Failed	The request contained an expectation in the Expect request header that could not be satisfied by the server.
500	Internal Server Error	The server encountered an error that prevented it from servicing the request.
501	Not Implemented	The client made a request that is beyond the server's capabilities.
502	Bad Gateway	A server acting as a proxy or gateway encountered a bogus response from the next link in the request response chain.
503	Service Unavailable	The server cannot currently service the request but will be able to in the future.
504	Gateway Timeout	Similar to the 408 status code, except that the response is coming from a gateway or proxy that has timed out waiting for a response to its request from another server.
505	HTTP Version Not Supported	The server received a request in a version of the protocol that it can't or won't support.

Headers

Both HTTP request and HTTP response can contain header fields. These two tables describe those fields and provide simple examples.

Request Headers

Field	Description	Example
Accept	Can be used to specify certain media types which are acceptable for the response	Accept: text/plain
Accept-Charset	Indicates what character sets are acceptable for the response	Accept-Charset: utf-8
Accept-Encoding	Similar to Accept, but restricts the content-codings that are acceptable in the response.	Accept-Encoding: gzip, deflate
Accept-Language	Similar to Accept, but restricts the set of natural languages that are preferred as a response.	Accept-Language: en-US
Authorization	Authentication credentials for HTTP authentication.	Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
Cache-Control	Used to specify directives that must be obeyed by all caching mechanisms along the request-response chain.	Cache-Control: no-cache
Connection	Allows the sender to specify options that are desired for that particular connection and MUST NOT be communicated by proxies over further connections.	Connection: keep-alive
Content-Encoding	Content-Encoding is primarily used to allow a document to be compressed without losing the identity of its underlying media type.	Content-Encoding: gzip
Cookie	An HTTP cookie previously sent by the server with Set-Cookie (below).	Cookie: $Version=1;
Content-Length	The length of the request body in octets (8-bit bytes).	Content-Length: 1024
Content-MD5	A Base64-encoded binary MD5 sum of the content of the request body.	Content-MD5: Q2hlY2sgSW50ZWdyaXR5IQ==
Content-Type	The MIME type of the body of the request (used with POST and PUT requests).	Content-Type: application/ x-www-form-urlencoded
Date	The date and time that the message was sent.	Date: Tue, 19 Jun 2012 10:10:10 GMT

Field	Description	Example
Expect	Indicates that particular server behaviors are required by the client.	Expect: 100-continue
From	The email address of the user making the request.	From: codemazeblog@gmail.com
Host	The domain name of the server (for virtual hosting), and the TCP port number on which the server is listening. The port number may be omitted if the port is the standard port for the service requested. Mandatory since HTTP/1.1.	Host: code-maze.com
If-Match	Only perform the action if the client supplied entity matches the same entity on the server. This is mainly for methods like PUT to only update a resource if it has not been modified since the user last updated it.	If-Match: "737060cd8c284d8af7ad3082f209582d"
If-Modified-Since	Allows a 304 Not Modified to be returned if content is unchanged.	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
If-None-Match	Allows a 304 Not Modified to be returned if content is unchanged.	If-None-Match: "737060cd8c284d8af7ad3082f209582d"
If-Range	If the entity is unchanged, send me the part(s) that I am missing; otherwise, send me the entire new entity.	If-Range: "737060cd8c284d8af7ad3082f209582d"
If-Unmodified-Since	Only send the response if the entity has not been modified since a specific time.	If-Unmodified-Since: Sat, 29 Oct 1994 19:43:31 GMT
Max-Forwards	Limit the number of times the message can be forwarded through proxies or gateways.	Max-Forwards: 10
Origin	Initiates a request for cross-origin resource sharing (asks server for an 'Access-Control-Allow-Origin' response field).	Origin: https://code-maze.com/
Pragma	Implementation-specific headers that may have various effects anywhere along the request-response chain.	Pragma: no-cache
Proxy-Authorization	Authorization credentials for connecting to a proxy.	Proxy-Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==

Field	Description	Example
Range	Request only part of an entity. Bytes are numbered from 0.	Range: bytes=500-999
Referer	This is the address of the previous web page from which a link to the currently requested page was followed. (The word "referrer" is misspelled in the RFC as well as in most implementations.)	Referer: https://code-maze.com/
TE	The transfer encodings the user agent is willing to accept: the same values as for the response header TE can be used, plus the "trailers" value (related to the "chunked" transfer method) to notify the server it expects to receive additional headers (the trailers) after the last, zero-sized, chunk.	TE: trailers, deflate
Upgrade	Ask the server to upgrade to another protocol.	Upgrade: HTTPS/1.3, IRC/6.9, RTA/x11, websocket
User-Agent	The user agent string of the user agent	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:12.0) Gecko/20100101 Firefox/12.0
Via	Informs the server of proxies through which the request was sent.	Via: 1.0 fred, 1.1 example.com(Apache/1.1)
Warning	A general warning about possible problems with the entity body.	Warning: 199 Miscellaneous warning

Response Headers

Field	Description	Example
Access-Control-Allow-Origin	Specifying which web sites can participate in cross-origin resource sharing	Access-Control-Allow- Origin: *
Accept-Ranges	Allows the server to indicate its acceptance of range requests for a resource.	Accept-Ranges: bytes
Age	Conveys the sender's estimate of the amount of time since the response (or its revalidation) was generated at the origin server.	Age: 24
Allow	Lists the set of methods supported by the resource identified by the Request-URI. The purpose of this field is strictly to inform the recipient of valid methods associated with the resource.	Allow: GET, HEAD, PUT

Field	Description	Example
Cache-Control	Tells all caching mechanisms from server to client whether they may cache this object. It is measured in seconds	Cache-Control: max-age=3600
Connection	Options that are desired for the connection	Connection: close
Content-Encoding	The type of encoding used on the data. See HTTP compression.	Content-Encoding: gzip
Content-Language	The language the content is in.	Content-Language: en
Content-Length	The length of the response body in octets (8-bit bytes)	Content-Length: 1024
Content-Location	An alternate location for the returned data	Content-Location: /index.htm
Content-MD5	A Base64-encoded binary MD5 sum of the content of the response	Content-MD5: Q2hlY2sgSW50ZWdyaXR5IQ==
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-Range	Where in a full body message this partial message belongs	Content-Range: bytes 21010-47021/47022
Content-Type	The MIME type of this content	Content-Type: text/html; charset=utf-8
Date	The date and time that the message was sent	Date: Sun, 17 Jun 2017 10:11:12 GMT
ETag	An identifier for a specific version of a resource, often a message digest	ETag: "737060cd8c284d8af7ad3082f209582d"
Expires	Gives the date/time after which the response is considered stale	Expires: Date: Sun, 17 Jun 2017 10:11:12 GMT
Last-Modified	The last modified date for the requested object, in RFC 2822 forma	Last-Modified: Date: Sun, 17 Jun 2017 10:11:12 GMT
Link	Used to express a typed relationship with another resource, where the relation type is defined by RFC 5988	Link: ; rel="alternate"
Location	Used in redirection, or when a new resource has been created.	Location: https://code-maze.com/index.html
P3P	This header is supposed to set Platform for Privacy Preferences Project (P3P) policy, in the form of P3P:CP="your_compact_policy".	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."

Field	Description	Example
	However, P3P did not take off, most browsers have never fully implemented it, a lot of websites set this header with fake policy text, that was enough to fool browsers the existence of P3P policy and grant permissions for third party cookies.	
Pragma	Implementation-specific headers that may have various effects anywhere along the request-response chain.	Pragma: no-cache
Proxy-Authenticate	Request authentication to access the proxy.	Proxy-Authenticate: Basic
Refresh	Used in redirection, or when a new resource has been created. This refresh redirects after 5 seconds. This is a proprietary, non-standard header extension introduced by Netscape and supported by most web browsers.	Refresh: 5; url=https://code-maze.com/index.html
Retry-After	If an entity is temporarily unavailable, this instructs the client to try again after a specified period of time (seconds).	Retry-After: 240
Server	A name for the server	Server: Apache/2.4 (Unix)
Set-Cookie	Sets an HTTP Cookie	Set-Cookie: UserID=1; Max-Age=3600; Version=1
Strict-transfer-Security	A HSTS Policy informing the HTTP client how long to cache the HTTPS only policy and whether this applies to subdomains.	Strict-transfer-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
Transfer-Encoding	The form of encoding used to safely transfer the entity to the user. Currently defined methods are: chunked, compress, deflate, gzip, identity.	Transfer-Encoding: chunked
Vary	Tells downstream proxies how to match future request headers to	Vary: *

Field	Description	Example
	decide whether the cached response can be used rather than requesting a fresh one from the origin server.	
Via	Informs the client of proxies through which the response was sent.	Via: 1.0 mick, 1.1 baselogic.com(Apache/2.4)
Warning	A general warning about possible problems with the entity body.	A general warning about possible problems with the entity body.
WWW-Authenticate	Indicates the authentication scheme that should be used to access the requested entity.	WWW-Authenticate: Basic

MIME TYPES

Because of the sheer quantity of Internet Media Types, we've listed the most commonly used ones.

Common Primary Mime Types

Type	Description
application	Application-specific content format (discrete type)
audio	Audio format (discrete type)
chemical	Chemical data set (discrete IETF extension type)
image	Image format (discrete type)
message	Message format (composite type)
model	3-D model format (discrete IETF extension type)
multipart	Collection of multiple objects (composite type)
text	Text format (discrete type)
video	Video movie format (discrete type)

Common Application Mime Types

Type	Description
application/atom+xml	Atom Feeds
application/ecmascript	ECMAScript/JavaScript (equivalent to application/javascript but with stricter processing rules)
application/json	JavaScript Object Notation JSON
application/javascript	ECMAScript/JavaScript (equivalent to application/ecmascript but with looser processing rules) It is not accepted in IE 8 or earlier
application/octet-stream	Unclassified binary data.
application/pdf	Portable Document Format

application/postscript	PostScript
application/rss+xml	RSS feeds
application/soap+xml	SOAP
application/font-woff	Web Open Font Format
application/xhtml+xml	XHTML
application/xml-dtd	Document Type Definition (DTD) files
application/xop+xml	XML-binary Optimized Packaging (XOP)
application/zip	ZIP archive files
application/gzip	Gzip

Common Multipart Mime Types

Type	Description
multipart/mixed	MIME Email
multipart/form-data	MIME Webform

Common Text Mime Types

Type	Description
text/css	Cascading Style Sheets.
text/csv	Comma-separated values
text/html	HTML file
text/plain	Textual data
text/xml	Extensible Markup Language