INTERNAL: Guide to Website HTTP Status Codes

07/24/2024 5:50 pm EDT

Basic Terms

- **Server**: A specialized computer with a massive amount of drive space in which we store the files that our website is composed of.
- **Client**: The computer that is trying to access our website.
- **Request**: When a customer types in a URL, a little bit of data is sent to our servers, which asks our servers to send over text, images, etc that make up our webpages. This is known as a request.
- **HTTP Status Code**: When a server returns information, it also includes a 3-digit status code. Most frequently this code is 200, which indicates that the request was successful.
- **Gateway**: A server that acts as a connecting point between different networks. The internet is a bunch of networks linked together.
- **Time Out**: The time elapsed has passed the maximum period of time that a device will wait for an action.

4XX: Client Based Errors - Fault is on the customer's end

400 Bad Request: The server cannot or will not process the request due to an apparent client error

401/403 Unauthorized/Forbidden: The request was a valid request, but the server is refusing to respond to it. The user might be logged in but does not have the necessary permissions for the resource.

404 Not Found: The requested resource could not be found but may be available in the future. Subsequent requests by the client are permissible.

408 Request Time-Out: The server timed out waiting for the request. The client did not produce a request within the time that the server was prepared to wait.

418 I'm a teapot: In RFC 2324, Hyper Text Coffee Pot Control Protocol, it is stated that this code should be returned by teapots requested to brew coffee. April Fools' joke was implemented by the ETF in 1998.

5XX: Server Based Errors - Fault is on our end, an intermediate connection, or our hosting company

500 Internal Server Error: A generic error message, given when an unexpected condition was encountered and no more specific message is suitable.

501 Not Implemented: The server either does not recognize the request method, or it lacks the ability to fulfill the request. Usually, this implies future availability (e.g., a new feature of a web-service API

502 Bad Gateway: The server was acting as a gateway or proxy and received an invalid response from the upstream server.

503 Service Unavailable: The server is currently unavailable. The server could be overloaded or down for maintenance.

504 Gateway Time-Out: The server was acting as a gateway or proxy and did not receive a timely response from the upstream server.

505 HTTP Version Not Supported: The server does not support the HTTP protocol version used in the request.

52X: Cloudflare Server-Based Errors

Cloudflare is the DNS service that converts DrChrono URLs to IP addresses that are used to access our content off of our server, hosted by Rackspace. If there is a Cloudflare error, it may not mean that our server is down, but access to the site may not be possible.

520 Unknown Error: The 520 error is used as a "catch-all response for when the origin server returns something unexpected", listing connection resets, large headers, and empty or invalid responses as common triggers.

521 Web Server Is Down: The origin server has refused the connection from Cloudflare.

522 Connection Timed Out: Cloudflare could not negotiate a TCP handshake with the origin server.

523 Origin Is Unreachable: Cloudflare could not reach the origin server; for example, if the DNS records for the origin server are incorrect.

524 A Timeout Occurred: Cloudflare was able to complete a TCP connection to the origin server but did not receive a timely HTTP response.

525 SSL Handshake Failed: Cloudflare could not negotiate an SSL/TLS handshake with the origin server.
526 Invalid SSL Certificate: Cloudflare could not validate the SSL/TLS certificate that the origin server presented.

527 Railgun Error: A 527 error indicates that the requests timeout or failed after the WAN connection has been established.

Other Errors

CSRF Errors: Cross-Site Request Forgery Error. In the data that is sent, there is a section of the data (header) that identifies that the data is not from a hijacker. Some IT devices, firewalls, or antiviruses remove this header and the browser identifies the data as potentially malicious and discards it.