HTTP
Internet-Draft
Intended status: Standards Track
Expires: September 2, 2020

M. Nottingham
Fastly
P. Sikora
Google

March 1, 2020

The Proxy-Status HTTP Response Header Field
draft-ietf-httpbis-proxy-status-01

Abstract

This document defines the Proxy-Status HTTP header field to convey the details of intermediary handling of responses, including generated errors.

Note to Readers

RFC EDITOR: please remove this section before publication

Discussion of this draft takes place on the HTTP working group mailing list (ietf-http-wg@w3.org), which is archived at https://lists.w3.org/Archives/Public/ietf-http-wg/ [1].

Working Group information can be found at https://httpwg.org/ [2]; source code and issues list for this draft can be found at https://github.com/httpwg/http-extensions/labels/proxy-status [3].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 2, 2020.

Table of Contents

1. Introduction

HTTP intermediaries - including both forward proxies and gateways (also known as "reverse proxies") - have become an increasingly significant part of HTTP deployments. In particular, reverse proxies and Content Delivery Networks (CDNs) form part of the critical infrastructure of many Web sites.

Typically, HTTP intermediaries forward requests towards the origin server and then forward their responses back to clients. However, if an error occurs, the response is generated by the intermediary itself.

HTTP accommodates these types of errors with a few status codes; for example, 502 Bad Gateway and 504 Gateway Timeout. However, experience has shown that more information is necessary to aid debugging and communicate what's happened to the client.

Additionally, intermediaries sometimes want to convey additional information about their handling of a response, even if they did not generate it.

To enable these uses, Section 2 defines a new HTTP response header field to allow intermediaries to convey details of their handling of a response, and Section 2.2 defines a set of Proxy Error Types for use when a proxy generates the response. Section 2.3 explains how to define new Proxy Error Types.

1.1. Notational Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

This specification uses Structured Headers [I-D.ietf-httpbis-header-structure] to specify syntax. The terms sh-param-list, sh-item, sh-string, sh-token and sh-integer refer to the structured types defined therein.

Note that in this specification, "proxy" is used to indicate both forward and reverse proxies, otherwise known as gateways. "Next hop" indicates the connection in the direction leading to the origin server for the request.

2. The Proxy-Status HTTP Header Field

The Proxy-Status HTTP response header field allows an intermediary to convey additional information about its handling of a response and its associated request.

It is a Structured Headers [I-D.ietf-httpbis-header-structure] List of parameterised Tokens:

```
Cache-Status   = sh-list
```

Each member of the list represents an intermediary that has handled the response. The first member of the list represents the intermediary closest to the origin server, and the last member of the list represents the intermediary closest to the user agent.

For example:

```
Proxy-Status: FooProxy, ExampleCDN
```

indicates that this response was handled first by FooAccelerator and then ExampleCDN.

Parameters on each member convey additional information about that intermediary's handling of the response; see Section 2.1 for defined parameters.

Intermediaries determine when it is appropriate to add the Proxy-Status header field to a response. Some might decide to add it to all responses, whereas others might only do so when specifically

configured to, or when the request contains a header that activates a debugging mode.

When adding a value to the Proxy-Status header field, intermediaries SHOULD preserve the existing contents of the header, to allow debugging of the entire chain of intermediaries handling the request.

The list members identify the intermediary that inserted the value, and MUST have a type of either sh-string or sh-token. Depending on the deployment, this might be a product or service name (e.g., ExampleProxy or "Example CDN"), a hostname ("proxy-3.example.com"), and IP address, or a generated string.

Each member of the list can also have a number of parameters that describe that intermediary's handling of the request. While all of these parameters are OPTIONAL, intermediaries are encouraged to provide as much information as possible.

Proxy-Status MAY be sent in HTTP trailers, but - as with all trailers - it might be silently discarded along the path to the user agent, so this SHOULD NOT be done unless it is not possible to send it in headers. For example, if an intermediary is streaming a response and the upstream connection suddenly terminates, Proxy-Status can be appended to the trailers of the outgoing message (since the headers have already been sent).

Note that there are various security considerations for intermediaries using the Proxy-Status header field; see Section 4.

Origin servers MUST NOT generate the Proxy-Status header field.

2.1. Proxy-Status Parameters

This section lists parameters that can be used on the members of Proxy-Status.

2.1.1. origin

The "origin" parameter's value is a sh-string or sh-token that identifies the origin server selected (and used, if contacted) for this response. Its contents might be a hostname, IP address, or alias.

This is most useful for gateways (also known as "reverse proxies"), since they are often configured to use an origin server other than that which appears in the URL, and sometimes they use several origins to serve a given site.

For example:

Proxy-Status: cdn.example.org; origin=backend.example.org

2.1.2. fwd-protocol

The "fwd-protocol" parameter's value is a sh-token indicating the ALPN protocol identifier [RFC7301] used by the intermediary to connect to the next hop. This is only applicable when that connection was actually established.

For example:

Proxy-Status: "proxy.example.org"; fwd-protocol=h2

2.1.3. error

The "error" parameter's value is a sh-token that is a Proxy Error Type. When present, it indicates that the response was generated by the proxy, not the origin server or any other upstream server.

Section 2.2 lists the Proxy Error Types defined in this document; new ones can be defined using the procedure outlined in Section 2.3.

For example:

```
HTTP/1.1 504 Gateway Timeout
Proxy-Status: SomeCDN; error=connection_timeout
```

indicates that this 504 response was generated by SomeCDN, due to a connection timeout when going forward.

Or:

```
HTTP/1.1 429 Too Many Requests
Proxy-Status: SomeReverseProxy; error=http_request_error
```

indicates that this 429 Too Many Requests response was generated by the intermediary, not the origin.

Each Proxy Error Type has a Recommended HTTP Status Code. When generating a HTTP response containing "error", its HTTP status code SHOULD be set to the Recommended HTTP Status Code. However, there may be circumstances (e.g., for backwards compatibility with previous behaviours) when another status code might be used.

2.1.4. details

The "details" parameter's value is a sh-string containing additional information not captured anywhere else. This can include implementation-specific or deployment-specific information.

For example:

```
Proxy-Status: ExampleProxy; error="http_protocol_error";
              details="Malformed response header - space before colon"
```

2.2. Proxy Error Types

This section lists the Proxy Error Types defined by this document. See Section 2.3 for information about defining new Proxy Error Types.

2.2.1. DNS Timeout

- Name: dns_timeout
- Description: The intermediary encountered a timeout when trying to find an IP address for the next hop hostname.
- Extra Parameters: None.
- Recommended HTTP status code: 504

2.2.2. DNS Error

- Name: dns_error
- Description: The intermediary encountered a DNS error when trying to find an IP address for the next hop hostname.
- Extra Parameters:
  - rcode: A sh-string conveying the DNS RCODE that indicates the error type. See [RFC8499], Section 3.
- Recommended HTTP status code: 502

2.2.3. Destination Not Found

- Name: destination_not_found
- Description: The intermediary cannot determine the appropriate next hop to use for this request; for example, it may not be configured. Note that this error is specific to gateways, which

typically require specific configuration to identify the "backend" server; forward proxies use in-band information to identify the origin server.

- Extra Parameters: None.
- Recommended HTTP status code: 500

2.2.4. Destination Unavailable

- Name: destination_unavailable
- Description: The intermediary considers the next hop to be unavailable; e.g., recent attempts to communicate with it may have failed, or a health check may indicate that it is down.
- Extra Parameters: None.
- Recommended HTTP status code: 503

2.2.5. Destination IP Prohibited

- Name: destination_ip_prohibited
- Description: The intermediary is configured to prohibit connections to the next hop IP address.
- Extra Parameters: None.
- Recommended HTTP status code: 502

2.2.6. Destination IP Unroutable

- Name: destination_ip_unroutable
- Description: The intermediary cannot find a route to the next hop IP address.
- Extra Parameters: None.
- Recommended HTTP status code: 502

2.2.7. Connection Refused

- Name: connection_refused
- Description: The intermediary's connection to the next hop was refused.

- Extra Parameters: None.
- Recommended HTTP status code: 502

2.2.8. Connection Terminated

- Name: connection_terminated
- Description: The intermediary's connection to the next hop was closed before any part of the response was received. If some part was received, see http_response_incomplete.
- Extra Parameters: None.
- Recommended HTTP status code: 502

2.2.9. Connection Timeout

- Name: connection_timeout
- Description: The intermediary's attempt to open a connection to the next hop timed out.
- Extra Parameters: None.
- Recommended HTTP status code: 504

2.2.10. Connection Read Timeout

- Name: connection_read_timeout
- Description: The intermediary was expecting data on a connection (e.g., part of a response), but did not receive any new data in a configured time limit.
- Extra Parameters: None.
- Recommended HTTP status code: 504

2.2.11. Connection Write Timeout

- Name: connection_write_timeout
- Description: The intermediary was attempting to write data to a connection, but was not able to (e.g., because its buffers were full).
- Extra Parameters: None.

- Recommended HTTP status code: 504

2.2.12. Connection Limit Reached

- Name: connnection_limit_reached
- Description: The intermediary is configured to limit the number of connections it has to the next hop, and that limit has been passed.
- Extra Parameters: None.
- Recommended HTTP status code: 503

2.2.13. HTTP Incomplete Response

- Name: http_response_incomplete
- Description: The intermediary received an incomplete response to the request from the next hop.
- Extra Parameters: None.
- Recommended HTTP status code: 502

2.2.14. HTTP Protocol Error

- Name: http_protocol_error
- Description: The intermediary encountered a HTTP protocol error when communicating with the next hop. This error should only be used when a more specific one is not defined.
- Extra Parameters: None.
- Recommended HTTP status code: 502

2.2.15. HTTP Response Header Block Too Large

- Name: http_response_header_block_size
- Description: The intermediary received a response to the request whose header block was considered too large.
- Extra Parameters:
  - header_block_size: a sh-integer indicating how large the headers received were. Note that they might not be complete;

i.e., the intermediary may have discarded or refused additional data.

- Recommended HTTP status code: 502

2.2.16. HTTP Response Header Too Large

- Name: http_response_header_size
- Description: The intermediary received a response to the request containing an individual header line that was considered too large.
- Extra Parameters:
  - header_name: a sh-string indicating the name of the header that triggered the error.
- Recommended HTTP status code: 502

2.2.17. HTTP Response Body Too Large

- Name: http_response_body_size
- Description: The intermediary received a response to the request whose body was considered too large.
- Extra Parameters:
  - body_size: a sh-integer indicating how large the body received was. Note that it may not have been complete; i.e., the intermediary may have discarded or refused additional data.
- Recommended HTTP status code: 502

2.2.18. HTTP Response Transfer-Coding Error

- Name: http_response_transfer_coding
- Description: The intermediary encountered an error decoding the transfer-coding of the response.
- Extra Parameters:
  - coding: a sh-token containing the specific coding that caused the error.
- Recommended HTTP status code: 502

2.2.19. HTTP Response Content-Coding Error

- Name: http_response_content_coding
- Description: The intermediary encountered an error decoding the content-coding of the response.
- Extra Parameters:
  - coding: a sh-token containing the specific coding that caused the error.
- Recommended HTTP status code: 502

2.2.20. HTTP Response Timeout

- Name: http_response_timeout
- Description: The intermediary reached a configured time limit waiting for the complete response.
- Extra Parameters: None.
- Recommended HTTP status code: 504

2.2.21. TLS Handshake Error

- Name: tls_handshake_error
- Description: The intermediary encountered an error during TLS handshake with the next hop.
- Extra Parameters:
  - alert_message: a sh-token containing the applicable description string from the TLS Alerts registry.
- Recommended HTTP status code: 502

2.2.22. TLS Untrusted Peer Certificate

- Name: tls_untrusted_peer_certificate
- Description: The intermediary received an untrusted peer certificate during TLS handshake with the next hop.
- Extra Parameters: None.

- Recommended HTTP status code: 502

2.2.23. TLS Expired Peer Certificate

- Name: tls_expired_peer_certificate
- Description: The intermediary received an expired peer certificate during TLS handshake with the next hop.
- Extra Parameters: None.
- Recommended HTTP status code: 502

2.2.24. TLS Unexpected Peer Certificate

- Name: tls_unexpected_peer_certificate
- Description: The intermediary received an unexpected peer certificate (e.g., SPKI doesn't match) during the TLS handshake with the next hop.
- Extra Parameters:
  - identity: a sh-string containing a comma-separated list of Subject Alternative Names from the certificate received from the next hop.
  - sha256: a sh-string containing the hex-encoded SHA-256 of the certificate received from the next hop.
  - spki: a sh-string containing the base64-encoded SHA-256 of the Subject Public Key Info (SPKI) from the certificate received from the next hop.
- Recommended HTTP status code: 502

2.2.25. TLS Missing Proxy Certificate

- Name: tls_missing_proxy_certificate
- Description: The next hop requested a client certificate from the intermediary during TLS handshake, but it wasn't configured with one.
- Extra Parameters: None.
- Recommended HTTP status code: 500

2.2.26. TLS Rejected Proxy Certificate

- Name: tls_rejected_proxy_certificate
- Description: The next hop rejected the client certificate provided by the intermediary during TLS handshake.
- Extra Parameters: None.
- Recommended HTTP status code: 500

2.2.27. TLS Error

- Name: tls_error
- Description: The intermediary encountered a TLS error when communicating with the next hop.
- Extra Parameters:
  - alert_message: a sh-token containing the applicable description string from the TLS Alerts registry.
- Recommended HTTP status code: 502

2.2.28. HTTP Request Error

- Name: http_request_error
- Description: The intermediary is generating a client (4xx) response on the origin's behalf. Applicable status codes include (but are not limited to) 400, 403, 405, 406, 408, 411, 413, 414, 415, 416, 417, 429.
- Extra Parameters:
  - status_code: a sh-integer containing the generated status code.
  - status_phrase: a sh-string containing the generated status phrase.
- Recommended HTTP status code: The applicable 4xx status code

This type helps distinguish between responses generated by intermediaries from those generated by the origin.

2.2.29. HTTP Request Denied

- Name: http_request_denied
- Description: The intermediary rejected the HTTP request based on its configuration and/or policy settings. The request wasn't forwarded to the next hop.
- Extra Parameters: None.
- Recommended HTTP status code: 400

2.2.30. HTTP Upgrade Failed

- Name: http_upgrade_failed
- Description: The HTTP Upgrade between the intermediary and the next hop failed.
- Extra Parameters: None.
- Recommended HTTP status code: 502

2.2.31. Proxy Internal Response

- Name: proxy_internal_response
- Description: The intermediary generated the response locally, without attempting to connect to the next hop (e.g. in response to a request to a debug endpoint terminated at the intermediary).
- Extra Parameters: None.
- Recommended HTTP status code:

2.2.32. Proxy Internal Error

- Name: proxy_internal_error
- Description: The intermediary encountered an internal error unrelated to the origin.
- Extra Parameters:
  - error: a sh-string containing details about the error condition.
- Recommended HTTP status code: 500

2.2.33. Proxy Loop Detected

- Name: proxy_loop_detected
- Description: The intermediary tried to forward the request to itself, or a loop has been detected using different means (e.g. [RFC8586]).
- Extra Parameters: None.
- Recommended HTTP status code: 502

2.3. Defining New Proxy Error Types

New Proxy Error Types can be defined by registering them in the HTTP Proxy Error Types registry.

Registration requests are reviewed and approved by a Designated Expert, as per [RFC8126], Section 4.5. A specification document is appreciated, but not required.

The Expert(s) should consider the following factors when evaluating requests:

- Community feedback
- If the value is sufficiently well-defined
- If the value is generic; vendor-specific, application-specific and deployment-specific values are discouraged

Registration requests should use the following template:

- Name: [a name for the Proxy Error Type that is matches sh-token]
- Description: [a description of the conditions that generate the Proxy Error Type]
- Extra Parameters: [zero or more optional parameters, along with their allowable type(s)]
- Recommended HTTP status code: [the appropriate HTTP status code for this entry]

See the registry at https://iana.org/assignments/http-proxy-statuses [4] for details on where to send registration requests.

3. IANA Considerations

Upon publication, please create the HTTP Proxy Error Types registry at https://iana.org/assignments/http-proxy-statuses [5] and populate it with the types defined in Section 2.2; see Section 2.3 for its associated procedures.

4. Security Considerations

One of the primary security concerns when using Proxy-Status is leaking information that might aid an attacker. For example, information about the intermediary's configuration and back-end topology can be exposed.

As a result, care needs to be taken when deciding to generate a Proxy-Status header. Note that intermediaries are not required to generate a Proxy-Status header field in any response, and can conditionally generate them based upon request attributes (e.g., authentication tokens, IP address).

Likewise, generation of all parameters is optional.

5. References

5.1. Normative References

[I-D.ietf-httpbis-header-structure]
Nottingham, M. and P. Kamp, "Structured Headers for HTTP", draft-ietf-httpbis-header-structure-13 (work in progress), August 2019.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC7301] Friedl, S., Popov, A., Langley, A., and E. Stephan, "Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension", RFC 7301, DOI 10.17487/RFC7301, July 2014, <https://www.rfc-editor.org/info/rfc7301>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8499] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", BCP 219, RFC 8499, DOI 10.17487/RFC8499, January 2019, <https://www.rfc-editor.org/info/rfc8499>.

5.2. Informative References

[RFC8586] Ludin, S., Nottingham, M., and N. Sullivan, "Loop Detection in Content Delivery Networks (CDNs)", RFC 8586, DOI 10.17487/RFC8586, April 2019, <https://www.rfc-editor.org/info/rfc8586>.

5.3. URIs

[1] https://lists.w3.org/Archives/Public/ietf-http-wg/

[2] https://httpwg.org/

[3] https://github.com/httpwg/http-extensions/labels/proxy-status

[4] https://iana.org/assignments/http-proxy-statuses

[5] https://iana.org/assignments/http-proxy-statuses

Authors' Addresses

Mark Nottingham
Fastly

Email: mnot@mnot.net
URI: https://www.mnot.net/

Piotr Sikora
Google

Email: piotrsikora@google.com