Workgroup: HTTP
Internet-Draft:
draft-ietf-httpbis-alias-proxy-status-05
Published: 20 June 2023
Intended Status: Standards Track
Expires: 22 December 2023
Authors: T. Pauly
Apple, Inc.

HTTP Proxy-Status Parameter for Next-Hop Aliases

Abstract

This document defines the next-hop-aliases HTTP Proxy-Status Parameter. This parameter carries the list of aliases and canonical names an intermediary received during DNS resolution as part establishing a connection to the next hop.

About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-httpbis-alias-proxy-status/.

Discussion of this document takes place on the HTTP Working Group mailing list (mailto:ietf-http-wg@w3.org), which is archived at https://lists.w3.org/Archives/Public/ietf-http-wg/. Working Group information can be found at https://httpwg.org/.

Source for this draft and an issue tracker can be found at https://github.com/httpwg/http-extensions/labels/alias-proxy-status.

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 22 December 2023.

Table of Contents

1. Introduction

The Proxy-Status HTTP response field [PROXY-STATUS] allows intermediaries to convey information about how they handled the request in HTTP responses sent to clients. It defines a set of parameters that provide information, such as the name of the next hop.

[PROXY-STATUS] defines a next-hop parameter, which can contain a hostname, IP address, or alias of the next hop. This parameter can contain only one such item, so it cannot be used to communicate a chain of aliases encountered during DNS resolution when connecting to the next hop.

Knowing the full chain of names that were used during DNS resolution via CNAME records [DNS] is particularly useful for clients of forward proxies, in which the client is requesting to connect to a specific target hostname using the CONNECT method [HTTP] or UDP proxying [CONNECT-UDP]. CNAME records can be used to "cloak" hosts that perform tracking or malicious activity behind more innocuous hostnames, and clients such as web browsers use the chain of DNS

names to influence behavior like cookie usage policies [COOKIES] or blocking of malicious hosts.

This document allows clients to receive the CNAME chain of DNS names for the next hop by including the list of names in a new next-hop-aliases Proxy-Status parameter.

1.1. Requirements

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.

2. next-hop-aliases Parameter

The next-hop-aliases parameter's value is a String [STRUCTURED-FIELDS] that contains one or more DNS names in a comma-separated list. The items in the list include all alias names and canonical names received in CNAME records [DNS] during the course of resolving the next hop's hostname using DNS, not including the original requested hostname itself. The names SHOULD appear in the order in which they were received in DNS. If there are multiple CNAME records in the chain, the first name in the next-hop-aliases list would be the value in the CNAME record for the original hostname, and the final name in the next-hop-aliases list would be the name that ultimately resolved to one or more addresses.

The list of DNS names in next-hop-aliases uses a comma (",") as a separator between names. Note that if a comma is included in a name itself, the comma must be encoded as described in Section 2.1.

For example, consider a proxy "proxy.example.net" that receives the following records when performing DNS resolution for the next hop "host.example.com":

```
host.example.com.           CNAME   tracker.example.com.
tracker.example.com.        CNAME   service1.example.com.
service1.example.com.       AAAA    2001:db8::1
```

The proxy could include the following proxy status in its response:

```
Proxy-Status: proxy.example.net; next-hop="2001:db8::1";
    next-hop-aliases="tracker.example.com,service1.example.com"
```

This indicates that proxy.example.net, which used the IP address "2001:db8::1" as the next hop for this request, encountered the names "tracker.example.com" and "service1.example.com" in the DNS resolution chain. Note that while this example includes both the

next-hop and next-hop-aliases parameters, next-hop-aliases can be included without including next-hop.

The next-hop-aliases parameter only applies when DNS was used to resolve the next hop's name, and does not apply in all situations. Clients can use the information in this parameter to determine how to use the connection established through the proxy, but need to gracefully handle situations in which this parameter is not present.

The proxy MAY send the empty string ("") as the value of next-hop-aliases to indicate that no CNAME records were encountered when resolving the next hop's name.

2.1. Encoding special characters

DNS names commonly just contain alphanumeric characters and hyphens ("-"), although they are allowed to contain any character ([RFC1035], Section 3.1), including a comma. To prevent commas or other special characters in names leading to incorrect parsing, any characters that appear in names in this list that do not belong to the set of URI Unreserved Characters ([RFC3986], Section 2.3) MUST be percent-encoded as defined in [RFC3986], Section 2.1.

For example, consider the DNS name comma,name.example.com. This name would be encoded within a next-hop-aliases parameter as follows:

```
Proxy-Status: proxy.example.net; next-hop="2001:db8::1";
    next-hop-aliases="comma%2Cname.example.com,service1.example.com"
```

It is also possible for a DNS name to include a period character (".") within a label, instead of as a label separator. In this case, the period character MUST be first escaped as "\.". Since the "\" character itself will be percent-encoded, the name "dot\.label.example.com" would be encoded within a next-hop-aliases parameter as follows:

```
Proxy-Status: proxy.example.net; next-hop="2001:db8::1";
    next-hop-aliases="dot%5C.label.example.com,service1.example.com"
```

Upon parsing this name, "dot%5C.label" MUST be treated as a single label.

Similarly the "\" character in a label MUST be escaped as "\\". Other uses of "\" MUST NOT appear in the label after percent-decoding.

3. Implementation Considerations

In order to include the next-hop-aliases parameter, a proxy needs to have access to the chain of alias names and canonical names received in CNAME records.

Implementations ought to note that the full chain of names might not available in common DNS resolution APIs, such as getaddrinfo. getaddrinfo does have an option for AI_CANONNAME, but this will only return the last name in the chain (the canonical name), not the alias names.

An implementation MAY include incomplete information in the next-hop-aliases parameter to accommodate cases where it is unable to include the full chain, such as only including the canonical name if the implementation can only use getaddrinfo as described above.

4. Security Considerations

The next-hop-aliases parameter does not include any DNSSEC information or imply that DNSSEC was used. The information included in the parameter can only be trusted to be valid insofar as the client trusts the proxy to provide accurate information. This information is intended to be used as a hint, and SHOULD NOT be used for making security decisions about the identity of a resource accessed through the proxy.

Inspecting CNAME chains can be used to detect cloaking of trackers or malicious hosts. However, the CNAME records could be omitted by a recursive or authoritative resolver that is trying to hide this form of cloaking. In particular, recursive or authoritative resolvers can omit these records for both clients directly performing DNS name resolution and proxies performing DNS name resolution on behalf of client. A malicious proxy could also choose to not report these CNAME chains in order to hide the cloaking. In general, clients can trust information included (or not included) in the next-hop-aliases parameter to the degree that the proxy and any resolvers used by the proxy are trusted.

5. IANA Considerations

This document registers the "next-hop-aliases" parameter in the "HTTP Proxy-Status Parameters" registry <https://www.iana.org/assignments/http-proxy-status>.

Name: next-hop-aliases

Description: A string containing one or more DNS aliases or canonical names used to establish a proxied connection to the next hop.

Reference:
This document

6. References

6.1. Normative References

[CONNECT-UDP] Schinazi, D., "Proxying UDP in HTTP", RFC 9298, DOI 10.17487/RFC9298, August 2022, <https://www.rfc-editor.org/rfc/rfc9298>.

[DNS] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <https://www.rfc-editor.org/rfc/rfc1034>.

[HTTP] Fielding, R., Ed., Nottingham, M., Ed., and J. Reschke, Ed., "HTTP Semantics", STD 97, RFC 9110, DOI 10.17487/RFC9110, June 2022, <https://www.rfc-editor.org/rfc/rfc9110>.

[PROXY-STATUS] Nottingham, M. and P. Sikora, "The Proxy-Status HTTP Response Header Field", RFC 9209, DOI 10.17487/RFC9209, June 2022, <https://www.rfc-editor.org/rfc/rfc9209>.

[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/rfc/rfc2119>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <https://www.rfc-editor.org/rfc/rfc3986>.

[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/rfc/rfc8174>.

[STRUCTURED-FIELDS] Nottingham, M. and P. Kamp, "Structured Field Values for HTTP", RFC 8941, DOI 10.17487/RFC8941, February 2021, <https://www.rfc-editor.org/rfc/rfc8941>.

6.2. Informative References

[COOKIES] Barth, A., "HTTP State Management Mechanism", RFC 6265, DOI 10.17487/RFC6265, April 2011, <https://www.rfc-editor.org/rfc/rfc6265>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/rfc/rfc1035>.

Author's Address

Tommy Pauly
Apple, Inc.

Email: tpauly@apple.com