HTTP Proxy-Status Parameter for DNS Information

draft-pauly-masque-dns-proxy-status

Tommy Pauly
MASQUE
IETF 115, November 2022, London
What is Proxy-Status?

RFC 9209 defines a header field that lets proxies tell clients extra information in responses

Provides proxy identifier(s)

Includes extensible list of parameters for errors, upstream details, etc.
Why is this relevant here?

This is very useful for CONNECT / CONNECT-UDP / CONNECT-IP proxies

For Private Relay, we use the status to communicate DNS failures, unreachable IPs, etc

Proxy-Status: ExampleProxy;error=dns_error;rcode="NXDOMAIN"
DNS Failures

CONNECT(-UDP):
bad.example.com

DNS Resolver

NXDOMAIN

502
Proxy-Status: Proxy;error=dns_error;rcode="NXDOMAIN"
What's missing?

In successful cases, there isn't a parameter to communicate DNS response details

There is "next-hop" which can contain a name, IP address, or alias, but it only contains one

This could make proxies more vulnerable to DNS cloaking / CNAME cloaking

Clients could do DNS on their own, but this is much less performant
DNS Success

CONNECT(-UDP):
example.com

200
Proxy-Status: Proxy; next-hop=example.com
DNS Success
CNAME / IP cloaking

CONNECT(-UDP): example.com

200
Proxy-Status: Proxy; next-hop=example.com
Clients (like browsers) apply different policies to specific hosts based on IP address or CNAME, generally preventing cookie sharing with trackers, etc.

A new proxy-status parameter can solve this!

Proxy-Status: proxy.example.net; next-hop=target.example.com
dns-used="2001:db8::1,tracker.example.com."

Lists IP address and CNAME/Alias chain
Choice of Scope

The dns-used parameter is very minimal

Simple way to add more information that can solve a client use case and improve debugging

More complex DNS work via proxy is expected

DNSSEC records or proofs, SVCB parameters for ECH / ALPN, etc

These require much more detailed requests and responses

Proxies also need to start making record requests beyond A/AAAA
Next steps

Is this a useful enhancement?

MASQUE? HTTPBIS? Should have review in both

Let's also kick off work on more advanced proxied DNS use cases