# How OpenDNS/Umbrella Resolvers Cache Resource Records

## Contents



## Introduction

This document describes how OpenDNS/Umbrella resolvers cache resource records.

## Overview

The OpenDNS/Umbrella resolvers use a program known as OpenDNSCache (ODC) to resolve DNS queries. ODC caches data that it receives in order to more quickly and efficiently return results to clients. This article focuses on how caching occurs and when it is used.

This article is aimed at users who wish to learn more about the specifics of ODC caching (typically nameserver and domain administrators), or for cases where DNS resolution might not be working as expected.

## What data is cached?

As per RFC 2181 (https://datatracker.ietf.org/doc/html/rfc2181), responses can be returned in a reply or stored in a cache based on the trustworthiness of the data. The RFC defines 7 trust levels in section 5.4.1:

1. Data from a primary zone file, other than glue data.
    - This only applies to authoritative nameservers, not to the OpenDNS resolvers
2. Data from a zone transfer, other than glue.
    - This only applies to authoritative nameservers, not to the OpenDNS resolvers
3. The authoritative data included in the answer section of an authoritative reply.
    - This applies to OpenDNSCache
4. Data from the authority section of an authoritative answer.
    - This applies to OpenDNSCache
5. Glue from a primary zone, or glue from a zone transfer.
    - This only applies to authoritative nameservers, not to the OpenDNS resolvers
6. i) Data from the answer section of a non-authoritative answer, and ii) non-authoritative data from the answer section of authoritative answers.
    - i) is an example of what our resolvers return. I.E., non-authoritative data.
    - For ii), note that the answer section of an authoritative answer normally contains only authoritative data. However when the name sought is an alias (see section 10.1.1) only the record describing that alias is necessarily authoritative. Clients can assume that other records must have come from the server's cache. Where authoritative answers are required, the client can query again, using the canonical name associated with the alias.
7. i) Additional information from an authoritative answer; ii) Data from the authority section of a non-

authoritative answer; iii) Additional information from non-authoritative answers.
    - All of these apply to OpenDNSCache
    - Records received from any of these sources must not be cached for the purposes of returning the results to queries.

OpenDNSCache caches data from responses with the trust levels 3, 4, and 6. If we receive new data that has a better or equal trust level, we replaces the old cache entry.

The exception here is for NS records, for which we only replace data with a better trust level.

# How is data added and removed from the cache?

Expired data is not deleted from the cache. This is the basis of the SmartCache feature, whereby we return expired Resource Records (RRs) from the cache if we are unable to reach the authorities for some reason.

Instead, the cache on each resolver is a fixed size, and when a new RR is added to the cache, the oldest RR is removed. This can be visualized as a queue where new entries are added to the queue, bumping old entries off of the queue (for the computer scientists out there, this is actually implemented as a circular doubly linked list).

Note that, as described above, a DNS response can contain multiple RRs that have different trust levels, not all of which were the data that was originally requested. Thus, after receiving a response, we might have multiple RRs to add to the cache.

As noted above, note that NS records are exempt from this behavior, as we only replace entries for NS records in the cache if the trust level of the data is higher than the existing entry. This is done to ensure that we can detect changes to authorities in the parent glue if the old authorities are still responding and returning themselves as the authority.