

CACHING NAME SERVERS (RESOLVER)

A DNS Caching Server (frequently called a Resolver) obtains information from another server (a Zone Master) in response to a host query and then saves (caches) the data locally. On a second or subsequent request for the same data the Caching Server (Resolver) will respond with its locally stored data (the cache) until the time-to-live (TTL) value of the response expires, at which time the server will refresh the data from the zone master.

If the caching server (resolver) obtains its data directly from a zone master it will respond as 'authoritative', if the data is supplied from its cache the response is 'non-authoritative'.

The default BIND behaviour is to cache and this is associated with the recursion parameter (the default is 'recursion yes'). There are many configuration examples which show caching behaviour being defined using a *type hint* statement in a zone declaration. These configurations confuse two distinct but related functions.

If a server is going to provide caching services then it must support recursive queries and recursive queries need access to the root servers which is provided via the 'type hint' statement.

Recursive and Iterative Queries

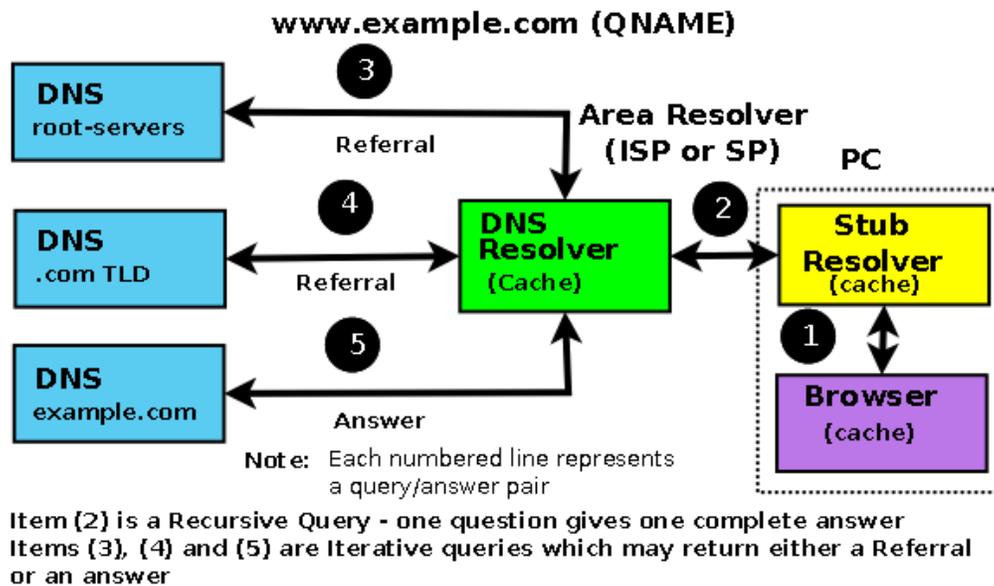


Diagram 3 DNS Resolver (Recursive Server)

A caching server will typically have a named.conf file which includes the following fragment:

```
// options section fragment of named.conf

// recursion yes is the default and may be omitted

options {

    directory "/var/named";
```

```
version "not currently available";

recursion yes;

};

// zone section

....

// the DOT indicates the root domain = all domains

zone "." IN {

    type hint;

    file "root.servers";

};
```

Notes:

1. BIND defaults to recursive queries which by definition provides caching behaviour. The named.conf recursion parameter controls this behaviour.
2. The zone '.' is shorthand for the root domain which translates to 'any domain not defined as either a master or slave in this named.conf file'.
3. cache data is discarded when BIND is restarted.

The most common DNS server caching configurations are:

- A DNS server acting as master or slave for one or more zones (domains) and as cache server for all other requests. A general purpose DNS server.
- A caching only local server - typically used to minimise external access or to compensate for slow external links. This is sometimes called a Proxy server though we prefer to associate the term with a Forwarding server

To cache or not is a crucial question in the world of DNS. BIND is regarded as the reference implementation of the DNS specification. As such it provides excellent - if complex to configure - functionality. The down side of generality is suboptimal performance on any single function - in particular caching involves a non-trivial performance overhead.

For general usage the breadth of BIND functionality typically offsets any performance concerns. However if the DNS is being 'hit' thousands of times per second performance is a major factor. There are now a number of alternate Open Source DNS servers some of which stress performance. These servers typically do NOT provide caching services (they are said to be 'Authoritative only' servers).

Example configuration files for a caching DNS are provided.

Note: The response to a query is Authoritative under three conditions:

1. The response is received from a Zone master.
2. The response is received from a Zone slave with non time-expired zone data.
3. The response is received by a caching server directly from either a Zone master or slave. If the response is read from the cache directly it is not authoritative.

Source: <http://www.zytrax.com/books/dns/ch4/>