

```

graph TD
    Client[Client] -- "Name Resolution: www.xyz.com" --> DNSClientCache[(DNS client cache)]
    DNSClientCache -- "FIRST" --> Client
    DNSClientCache -- "www.xyz.com 10.1.1.1" --> Client
    Client -- "Web 10.1.1.1" --> Web[Web 10.1.1.1]
    DNSClientCache -- "SECOND" --> DNSServer[DNS server]
    DNSServer -- "www.xyz.com 10.1.1.1 (TTL)" --> DNSClientCache
    DNSServer -- "zone xyz.com www A 10.1.1.1" --> Zone[(zone)]
    
```

DNS Server Resolution

- 1. Locally Cached Zones:** The DNS server first checks its own locally cached zones for the FQDN. If the DNS server is authoritative for the domain in question (meaning it holds the zone file for that domain), it will have the answer and return it immediately.
- 2. DNS Server Cache:** If the DNS server is not authoritative for the domain, it will then check its DNS server cache. The cache contains recent queries the server has resolved. If the FQDN is in the cache, the server will return the cached answer.
- 3. Conditional Forwarding:** If the FQDN is not in the cache, the server will then check if there are any conditional forwarders configured. A conditional forwarder is a DNS server that is designated to handle queries for specific domain names. If a conditional forwarder is configured for the domain in question, the query will be sent to that server.
- 4. Forwarding:** If there are no conditional forwarders for the domain, the server will then check if there are any forwarders configured. A forwarder is a DNS server that handles all queries the local server can't resolve. If a forwarder is configured, the query will be sent to that server.
- 5. Root Hints:** If there are no forwarders, or if the forwarders can't resolve the query, the server will then use its root hints. Root hints are a list of authoritative servers for the root zone of DNS (".") and they know which servers are authoritative for top-level domains (like .com, .org, etc.). The local server will query a root hint server, which will direct it to the server authoritative for the top-level domain, and so on, until it finds the server that can answer the query.

The diagram illustrates the DNS resolution process for the query `www.xyz.co.nz`. It shows the flow of data between a Client, DNS client cache, DNS server, and zone. The process starts with the Client sending a query to the DNS client cache. The DNS client cache checks its local cache. If the query is not found, it sends the query to the DNS server. The DNS server then checks its local cache. If the query is not found, it sends the query to the zone. The zone returns the answer to the DNS server, which then returns the answer to the DNS client cache. Finally, the DNS client cache returns the answer to the Client.

1. Locally Cached Zones: The DNS server first checks its own locally cached zones for the FQDN. If the DNS server is authoritative for the domain in question (meaning it holds the zone file for that domain), it will have the answer and return it immediately.

2. DNS Server Cache: If the DNS server is not authoritative for the domain, it will then check its DNS server cache. The cache contains recent queries the server has resolved. If the FQDN is in the cache, the server will return the cached answer.

3. Conditional Forwarding: If the FQDN is not in the cache, the server will then check if there are any conditional forwarders configured. A conditional forwarder is a DNS server that is designated to handle queries for specific domain names. If a conditional forwarder is configured for the domain in question, the query will be sent to that server.

4. Forwarding: If there are no conditional forwarders for the domain, the server will then check if there are any forwarders configured. A forwarder is a DNS server that handles all queries the local server can't resolve. If a forwarder is configured, the query will be sent to that server.

5. Root Hints: If there are no forwarders, or if the forwarders can't resolve the query, the server will then use its root hints. Root hints are a list of authoritative servers for the root zone of DNS (".") and they know which servers are authoritative for top-level domains (like .com, .org, etc.). The local server will query a root hint server, which will direct it to the server authoritative for the top-level domain, and so on, until it finds the server that can answer the query.

The diagram illustrates the DNS resolution process for the domain `www.xyz.co.nz`. It shows a Client, a DNS client cache, a DNS server, and two zones. The Client sends a query for `www.xyz.co.nz` to the DNS client cache. The cache checks its local zone (containing `xyz.com` and `www A 10.1.1.1`) and forwards the query to the DNS server. The DNS server checks its cache and forwards the query to another DNS server, which then checks its zone (containing `xyz.co.nz` and `www A 10.1.1.1`) and returns the answer to the first DNS server, which finally returns it to the client.

The diagram illustrates the DNS resolution process for the domain `www.comp.com.au`. It shows the flow of queries and responses between various DNS components:

- Client** and **DNS client cache**: The Client sends a query to the DNS client cache (labeled "FIRST"). The DNS client cache sends the query to the DNS server (labeled "SECOND").
- DNS server**: The DNS server checks its cache and then the Root server.
- DNS server Root**: The Root server delegates to the `.au` server.
- DNS server au.**: The `.au` server delegates to the `com.au` server.
- DNS server com.au.**: The `com.au` server delegates to the `comp.com.au` server.
- DNS server www.comp.com.au.**: The `comp.com.au` server delegates to the specific DNS server for `www.comp.com.au`.
- DNS server www.comp.com.au.**: This server returns the IP address `11.1.1.1` to the `comp.com.au` server, which then returns it to the `com.au` server, then to the `.au` server, and finally to the DNS server.
- DNS server**: The DNS server returns the IP address `11.1.1.1` to the DNS client cache, which then returns it to the Client.

The diagram also includes a list of DNS resolution steps:

- Locally Cached Zones**: The DNS server first checks its own locally cached zones for the FQDN. If the DNS server is authoritative for the domain in question (meaning it holds the zone file for that domain), it will have the answer and return it immediately.
- DNS Server Cache**: If the DNS server is not authoritative for the domain, it will then check its DNS server cache. The cache contains recent queries the server has resolved. If the FQDN is in the cache, the server will return the cached answer.
- Conditional Forwarding**: If the FQDN is not in the cache, the server will then check if there are any conditional forwarders configured. A conditional forwarder is a DNS server that is designated to handle queries for specific domain names. If a conditional forwarder is configured for the domain in question, the query will be sent to that server.
- Forwarding**: If there are no conditional forwarders for the domain, the server will then check if there are any forwarders configured. A forwarder is a DNS server that handles all queries the local server can't resolve. If a forwarder is configured, the query will be sent to that server.
- Root Hints**: If there are no forwarders, or if the forwarders can't resolve the query, the server will then use its root hints. Root hints are a list of authoritative servers for the root zone of DNS ("."). They know which servers are authoritative for top-level domains (like `.com`, `.org`, etc.). The local server will query a root hint server, which will direct it to the server authoritative for the top-level domain, and so on, until it finds the server that can answer the query.

The diagram illustrates the DNS lookup process for the domain `www.abc.com.au`. It shows the flow of queries and responses between various components:

- Client:** Initiates the request and receives the final IP address (`134.1.2.1`) from the DNS server. The client also has a local **cache**.
- DNS Server:** Acts as the central authority, checking its **cache** and querying the hierarchy of servers.
- Root Server:** Provides the IP address for the `au.` top-level domain.
- au. Server:** Provides the IP address for the `com.au.` domain.
- com.au. Server:** Provides the IP address for the `abc.com.au.` domain.
- abc.com.au. Server:** Provides the IP address for the specific host `www.abc.com.au`.
- Web Server:** The destination of the request, located at `134.1.2.1`.

The diagram uses color-coded arrows to represent different types of data flow:

- Blue arrows:** Represent the initial request from the client to the DNS server and the final response from the DNS server to the client.
- Pink arrows:** Represent the recursive queries from the DNS server to the hierarchy of domain servers.
- Green arrows:** Represent the responses from the hierarchy of domain servers back to the DNS server.

The diagram illustrates the Clear-DNS architecture. On the left, a 'client' (represented by a rounded rectangle) is connected to a 'Clear-DnsClientCache' (represented by a cylinder labeled 'cache'). The client sends requests to the 'DNS' server (represented by a rounded rectangle). The 'DNS' server is connected to a 'Clear-DnsServerCache' (represented by a cylinder labeled 'cache') and a 'zone' (represented by a cylinder). The 'zone' contains the following information:

```
lumify.com
svr1 172.18.1.2
svr2 172.18.1.3
```

The 'DNS' server sends responses back to the client. The client also sends requests directly to the authoritative servers 'svr1' and 'svr2' (represented by rectangles) within a triangular network boundary. The 'DNS' server also sends requests to 'svr1' and 'svr2'.