FORWARDING (A.K.A PROXY) NAME SERVERS

A forwarding (a.k.a. Proxy, Client, Remote) server is one which simply forwards requests to another DNS and caches the results. On its face this looks like a pretty pointless exercise. It is. however, a frequently undervalued and extremely useful configuration in a number of situations:

1. Where access to the external network is slow or expensive:
    1. Local DNS caching - results are cached in the forwarding server so that frequently requested domains will provide fast results from the cache.
    2. The Remote (forwarded to) DNS server provides recursive query support - results in a single query across the network (from the forwarding DNS to the forwarded to DNS) thus reducing traffic congestion (on busy networks) and increasing performance (on slow networks).
2. Forwarding servers also can be used to ease the burden of local administration by providing a single point at which changes to remote name servers may be managed, rather than having to update all hosts.

Thus, all hosts in a particular network section or area can be configured to point to a fixed forwarding DNS which can be configured to stream DNS traffic as desired and changed over time with minimal effort.

3. Sanitizing traffic. Especially in larger private networks it may be sensible to stream DNS traffic for local domain access by forwarding to the local DNS servers while forwarding external DNS requests to a **dirty** or hardened caching DNS (or resolver).
4. Forwarding can also be used as part of a Split Server configuration for perimeter defence.

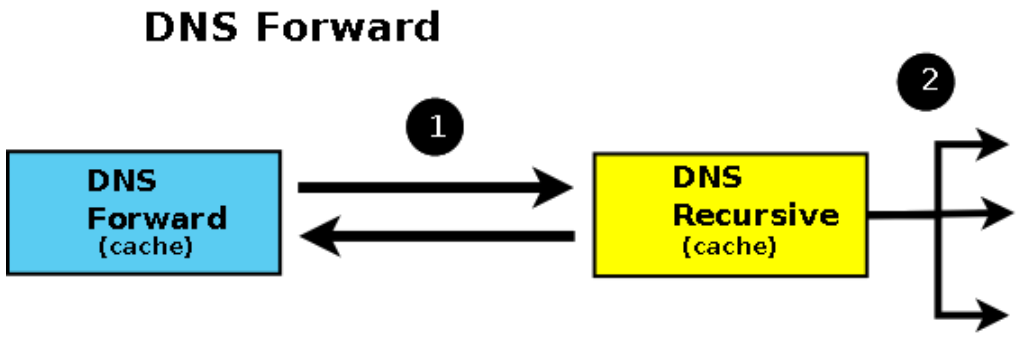

Diagram 4 - DNS Forwarding Server

BIND allows configuration of forwarding using

the forward and forwarders parameters either at a 'global' level (in an options section) or on a per-zone basis in a zone section of the named.conf file.

Both configurations are shown in the examples below:

a. Global Forwarding - All Requests

```
// options section fragment of named.conf
// forwarders can have multiple choices
options {
        directory "/var/named";
        version "not currently available";
        forwarders {10.0.0.1; 10.0.0.2;};
        forward only;
};
// zone file sections
....
```

b. Per Domain Forwarding

```
// zone section fragment of named.conf
zone "example.com" IN {
        type forward;
        forwarders {10.0.0.1; 10.0.0.2;};
};
```

Where dial-up links are used with DNS forwarding servers BIND's general purpose nature and strict standards adherence may not make it an optimal solution. A number of the Alternate DNS solutions specifically target support for such links. BIND provides two parameters dialup and heartbeat-interval (neither of which is currently supported by BIND 9) as well as a number of others which can be used to minimise connection time.

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