DNS Resolver configuration

Background

There is a great deal of literature about the operation of authoritative nameservers, but not so much about the resolver function.
This note is for system and network managers or administrators in Janet organisations (particularly smaller organisations with relatively simple networks) and is intended to give them confidence that they have correctly configured this straighforward but critical part of the DNS in their own networks.

DNS clients and resolvers

Almost all the computers and applications in your network are clients of the Domain Name System. Most of their DNS activity consists of simple lookups in which the clients issue a request containing a domain name and expect a response containing the corresponding IP address:

[1]

The server to which they make the request is called a "*DNS resolver*"; each client has to know in advance the IP address of one or more resolvers, but nothing else.

How your DNS lookups work

Your DNS resolver enables you to look up other people's domain names and IP addresses:

[2]

A typical client is a Web browser; to fetch a page it extracts a domain name from the page URL and sends it to your DNS resolver. The resolver will interrogate the rest of the DNS to find the IP address the browser needs, and will then return that address to the client in a single response. After this exchange of DNS information the browser can make a connection to the Web server at its IP address and request the specific page without further reference to the DNS (until the next time).

The resolver may have to make several separate requests of its own to various "*authoritative nameservers*

” belonging to other people (a brief explanation is given in the Glossary), but all the detail is hidden from normal DNS clients.

Real resolvers normally cache both complete and partial results, so they can return some addresses immediately and can often omit the initial stages when working through the nameservers. Caching saves time and reduces network traffic.

Other people’s lookups

In the other direction when other people want to find your domain information, they will use their own resolvers. The details they need ultimately come from your primary and secondary nameservers, which play no part in lookups you do.
Other people’s activity are out of scope for this note.

Choosing local DNS resolvers

The most efficient and reliable arrangement is for your DNS resolver to be in your own network. Even if you provide two or more resolvers for resilience, there is no benefit from locating one at a different site.

Almost any local server is capable of being configured to provide resolver service, whether on a Windows or a Unix-based platform. If your primary or secondary nameservers are located elsewhere it makes no difference; they take no part in your DNS lookups.

Configuring your DNS resolver

Network configuration

DNS resolving is an internal service and ideally your network will have a part set aside for internal servers such as domain controllers and fileservers. An existing domain controller is particularly suitable. The resolver needs to be able to receive and respond to client requests (UDP and TCP port 53 from the internal network where your client systems are), and to send its own requests (using the same ports) to Janet and the rest of the Internet.

The resolver function must **not** be made available outside your own network. If you have a stateful firewall which is able to distinguish between responses from the outside to the resolver’s own requests and requests to the resolver from outside, then it may be able to block the requests from outside. Otherwise you must configure the resolver system itself to recognise internal networks and to respond only to requests from them.

You may be able to check from a home Internet connection that your resolver is not available for unauthorised use; or another Janet organisation may be able to check for you.

Resolver configuration

Any Windows server will have the necessary software (DNS service). An Active Directory server will normally be able to offer a resolving service in which it uses its domain knowledge to resolve names within the Windows domain directly, and uses the usual DNS process for other names.
For Unix-based servers, BIND or some similar software is available without difficulty or

expense, although it may have been an optional component of the installation. Again it is straightforward both to resolve purely local names from local knowledge and to process DNS names in the usual way.

A DNS resolver will need to have available the IP addresses of one or more of the “*root nameservers*“.
Fortunately their addresses are very stable and the list is reasonably short; it is normal to install the whole of it along with the operating system or the software for the DNS service, and you will rarely need to take any action.

A normal resolver does not need the IP addresses of any other nameservers; it can if necessary find them itself at any time by starting from the root nameservers and the top of the naming tree.
Specifically, it must **not** be configured to “forward” DNS queries anywhere.
(There are, of course, some exceptions; but only in more complicated situations).

Configuring your DNS clients

Each computer that is a DNS client has to be configured with the IP address of one or more resolvers. This is a standard part of its network (IP) setup; it may be statically set on each computer, or each computer may obtain its resolver addresses through DHCP when it starts up, along with its own IP address and other basic network details.
The name “*DNS server*” is sometimes used in the configuration dialogue instead of “*resolver*“; unfortunately there are other kinds of DNS server, and this can lead to confusion.

If your computers use a Web proxy they may only need to know the address of the proxy server, because they do not directly send to or receive from the Internet. The proxy may be its own resolver; otherwise it will have to be configured with the address of the resolver or resolvers you have set up.

It is notionally possible to configure client machines to be resolvers in their own right so that they need no separate resolver, but this is less efficient and effective and is deprecated. Such machines may not be able to use local names which only a managed resolver will deal with properly.

Off-site resolvers are deprecated

Almost any network with a server of any kind will have resolver software available locally without any additional cost or management burden and should resolve its DNS queries locally. This is the most effective and efficient arrangement.

For the very smallest networks and organisations, it may still be impracticable; and Janet offers an off-site resolver service as a last resort. There is no charge to eligible organisations for this service, but it is restricted to those with a demonstrable need.

What to do in your network

Detailed advice should be treated with caution, as it depends to a large extent on how you have set up your network. Here are some comments on common scenarios.

1. Internet access through a proxy

You may have a single system through which your desktop clients make all their connections to the external Internet. It may be called a firewall, a proxy, a NAT box; it may be running ISA, Proxy Server, Border Manager, squid; and there are lots of other possibilities.

In this case the client machines are probably configured (manually or with DHCP) to use the proxy system as their DNS resolver. It is almost certain that the proxy is running DNS service; the default configuration is for it to do its own resolving and you should only check that there is no direction to “forward” requests to a separate DNS resolver (which may be called a “*DNS server*” in the documentation).

2. Server systems

Some or all of your servers are also DNS clients; certainly your e-mail server, almost certainly your Web server and probably any others that have any contact with the Internet. The issues for them, and the changes to make, are exactly the same as for desktop systems; but it is perhaps more likely that they are on dedicated network segments or VLANs. You may need to explicitly allow access to the resolver where the default rules might have blocked it.

3. Resolving local names

Windows systems using Active Directory will normally use a Windows name resolver, which may search for domain names locally before using the DNS. If you have a separate resolver (such as your primary or secondary nameserver on a different system) you will be able to configure the domain controller to forward DNS requests for non-local names to it.

4. Resolver colocated with local authoritative nameserver

If either the primary nameserver for your domain or a secondary is in your own network, it will almost certainly work as a resolver with little or no additional configuration.

You will need to review access control carefully. Other people’s DNS clients must not be able to use your system as a resolver, but other people’s resolvers must have access to the data in your own zone for which your nameserver is authoritative.
It is impracticable to implement this access control in a firewall or router; the authoritative nameservers themselves must reject recursive (resolving) requests from networks other than your own.

5. Third-party off-site primary or secondary nameservers

If your primary or secondary nameservers are operated by someone else such as an ISP, you may be able to use them as DNS resolvers, although all except the smallest networks should include a local resolver.

If you are considering using

third-party resolvers, check that you can access them from your network without them becoming available to the whole Internet. You should also think what impact it will have if a

network failure somewhere makes the resolvers inaccessible; you may decide that in that situation it is acceptable for your clients to be unable to resolve external (Internet) names, but in some configurations it could affect lookups of internal names which might have been expected to continue to work.You are also vulnerable to a policy change by the service provider, and you should confirm that resolving at their authoritative nameservers is a supported service. The JANET off-site resolver service is fully supported, but it remains a last resort.

Security considerations

DNS availability is best with a local resolver.

It is possible to damage the integrity of DNS lookups by changing the behaviour of a resolver (perhaps so that it intercepts requests for, say, `windowsupdate.microsoft.com`and supplies the IP address for a source of corrupt updates). A resolver on a system inaccessible to the Internet may be less exposed to such compromise.

One confidentiality issue is that resolvers with Janet IP addresses are allowed access to certain zones which should not be available to users outside Janet (such as Janet mirrors of spam blacklists, internal name spaces). A resolver inside your network must not answer *recursive* (resolving) requests from addresses outside your network; you must arrange access control at your router or firewall, or at the resolver system itself.

Such an open DNS resolver may also be used to amplify a DNS attack against another host on the Internet. Since the server will answer any query, and the source address can be spoofed, an open DNS resolve can be instructed to send a the largest reply permitted by the DNS protocol to any destination, in response to a small request.

It is worth noting that Windows DNS can either have recursion enabled on a particular server, or disabled. It does not allow for fine grained access control that could specify a set of clients that are allowed to perform recursive queries. Consequently it is impossible to run a public name server service, and a private resolver service on the same Windows DNS server without it being an open DNS resolver. Janet CSIRT recommend that the roles are split across two seperate Windows DNS servers.

Further reading
(but mostly about authoritative nameservers, not resolvers)

DNS and BIND 5th edition May 2006
Paul Albitz, Cricket Liu
O'Reilly, ISBN 978-0596100575
`http://www.oreilly.com/catalog/dns5/` [3] (*offsite link*)

DNS on Windows Server 2003 3rd edition December 2003
Cricket Liu, Matt Larson and Robbie Allen
O'Reilly, ISBN 0-596-00562-8
`http://www.oreilly.com/catalog/dnswinsvr/` [4] (*offsite link*)

Links

[1] http://community.ja.net/system/files/images/csirt-dns-resolver-01.jpg
[2] http://community.ja.net/system/files/images/csirt-dns-resolver-02.jpg
[3] http://www.oreilly.com/catalog/dns5/
[4] http://www.oreilly.com/catalog/dnswinsvr/