# DNS Technical Overview

Domain name system (DNS) is the service for dynamically maintaining hostname-to-IP address relationships. DNS is an Internet standard service that maintains a dynamic database of network resources and their corresponding IP addresses. It is the service for locating resources on the Internet as well as in Active Directory.

DNS is a hierarchical naming system. A so-called fully qualified hostname such as `london.braincore.net` is composed of a name (`london`) and a domain (`braincore.net`). The name uniquely identifies the machine in the DNS domain, and the DNS domain is such that the domain is unique throughout the network (in the case of the Internet, the network is the world). Thus, the fully qualified hostname uniquely identifies the machine on the network.

## What Is DNS?

DNS domains are organized in a hierarchical structure to ensure that all domains are unique. At the top is the root (`.`) domain. Beneath that are the top-level domains, such as `com`, `net`, `org`, `mil`, and so on. Beneath each of those are domain names you can purchase. Note that you can have the same second-level domain name exist beneath more than one of the top-level domains. For example, `braincore.com` and `braincore.net` are completely different domains. After you have purchased a domain on the Internet, you can create your own hierarchy underneath it by using subdomains. *Subdomains* are simply further subdivisions of your network naming structure, as in `ad.braincore.net`.

### DNS Zones

DNS *zones* are physical databases that store the domain records. In Windows Server 2003, three types of zones exist: primary, secondary, and stub zones. Each of these zones can be either standard zones (in which the records are stored in a `.dns` file on the DNS server) or Active Directory integrated (in which the records are stored in Active Directory itself). A zone is the actual database that resides on a particular server. It can contain a single domain or a domain and one or more child domains. Child domains can also be delegated to other DNS servers. The server that has the parent domain would have a *glue* record (*delegated subdomain* in Microsoft terminology) that designates the IP address of the server responsible for the subdomain. In that case, the server would have the parent domain in its zone but would redirect requests for the child domain to the designated subdomain server. The server designated would simply have a zone for the subdomain, although it too could further subdivide the subdomain and delegate it to other servers. For example, consider the domain `braincore.net`. DNS Server1 is `authoritative` for that domain, meaning it has a writeable copy of the `braincore.net` zone. Within `braincore.net` are two subdomains—`na.braincore.net` and `eu.braincore.net`. You could delegate one (or both) of the subdomains to different servers. Suppose you delegate `na.braincore.net` to Server2. Server1 would then have a zone for `braincore.net` that would contain all the records for `braincore.net` as well as `eu.braincore.net` (because that domain was not delegated) and a glue record for `na.braincore.net` pointing to Server2. Server2 would simply have a zone for `na.braincore.net`.

There are actually two categories of zones: *forward lookup* zones, which resolve names to IP addresses, and *reverse lookup* zones, which resolve IP addresses to names. Because network communications are based on IP addresses, you usually look for the IP address for a particular server or service. Consequently, most DNS queries are for forward lookup zones. Reverse lookup zones are used to find server names for a given IP address, usually for diagnostic purposes.

### DNS Records

Several types of DNS records exist: *host* records, which map server names to IP addresses; *alias* records, which provide alternative names for your servers and map to host records; *MX* records, which locate mail servers; and so forth. A particularly important type of record is the service record. *Service* records are just that—records for locating services. Active Directory, in particular, heavily uses service records. Active Directory requires that a bunch of service records be loaded into DNS so clients can locate directory services, such as domain controllers, Global Catalog servers, and the like.

## DNS Resolution Process

Similar to WINS resolution, the hostname resolution process potentially uses several resources. First, a client checks to see whether the name requested is its own hostname (it should know how to find itself). Then, it checks the DNS client cache. You can display the DNS client cache by running `ipconfig /displaydns` or clear it by running `ipconfig /flushdns`. Next, it checks the hosts file. The hosts file is a static file (stored in `%systemroot%\system32\drivers\...`) that maintains a list of hostnames and their corresponding IP addresses. Finally, if all these methods fail, it queries the primary DNS server. If the primary DNS server is unavailable (does not respond), the client queries the secondary DNS server. If the whole hostname resolution process fails to return a result, the client then attempts to resolve the request via the NetBIOS name resolution process.

For more information on WINS and the NetBIOS resolution process, visit `www.samspublishing.com` and enter this book's ISBN number (no hyphens or parenthesis) in the Search field; then click the book cover image to access the book details page. Click the Web Resources link in the More Information section, and locate article ID# **A010801**.

DNS servers provide administrators with a centralized, dynamic method for maintaining hostname-to-IP address resolution. DNS is of particular importance to the Internet because Internet resources are located via hostname resolution. Additionally, Windows 2000 and better register in DNS by default and preferentially resolve via DNS, which lessens the requirements for WINS. Eventually, when applications no longer require NetBIOS and all Windows clients and servers are Windows 2000 or better, NetBIOS resolution will be unnecessary and it will all be DNS.