

## Domain Name Server (DNS)

**DNS** is a system that stores information associated with **domain names** in a distributed database on networks, such as the Internet. The domain name system (Domain Name Server) associates many types of information with domain names, but most importantly, it provides the IP address associated with the domain name. It also lists mail exchange servers accepting e-mail for each domain. In providing a worldwide keyword-based redirection service, DNS is an essential component of contemporary Internet use.

DNS is useful for several reasons. Most well known, the DNS makes it possible to attach easy-to-remember domain names (such as "Adjigol.com") to hard-to-remember IP addresses (such as 207.176.224.100). Humans take advantage of this when they recite URLs and e-mail addresses. Less recognized, the domain name system makes it possible for people to assign authoritative names, without needing to communicate with a central registrar each time.

### Understanding the parts of a domain name

A domain name usually consists of two or more parts (technically labels), separated by dots. For example Adjigol.com.

- The rightmost label conveys the top-level domain (for example, the address adjigol.com has the top-level domain com).
- Each label to the left specifies a subdivision or subdomain of the domain above it. Note that "subdomain" expresses relative dependence, not absolute dependence: for example, adjigol.com comprises a subdomain of the com domain, and Music.adjigol.com is a subdomain of the domain adjigol.com. In theory, this subdivision can go down to 127 levels deep, and each label can contain up to 63 characters, as long as the whole domain name does not exceed a total length of 255 characters. But in practice some domain registries have shorter limits than that.
- A domain name that has one or more associated IP addresses is called a hostname. For example, the Music.adjigol.com adjigol.com domains are both hostnames, but the com domain is not.

The DNS consists of a hierarchical set of DNS servers. Each domain or subdomain has one or more authoritative DNS servers that publish information about that domain and the name servers of any domains "beneath" it. The hierarchy of authoritative DNS servers matches the hierarchy of domains. At the top of the hierarchy stand the root servers: the servers to query when looking up (resolving) a top-level domain name.

### How the DNS works in theory

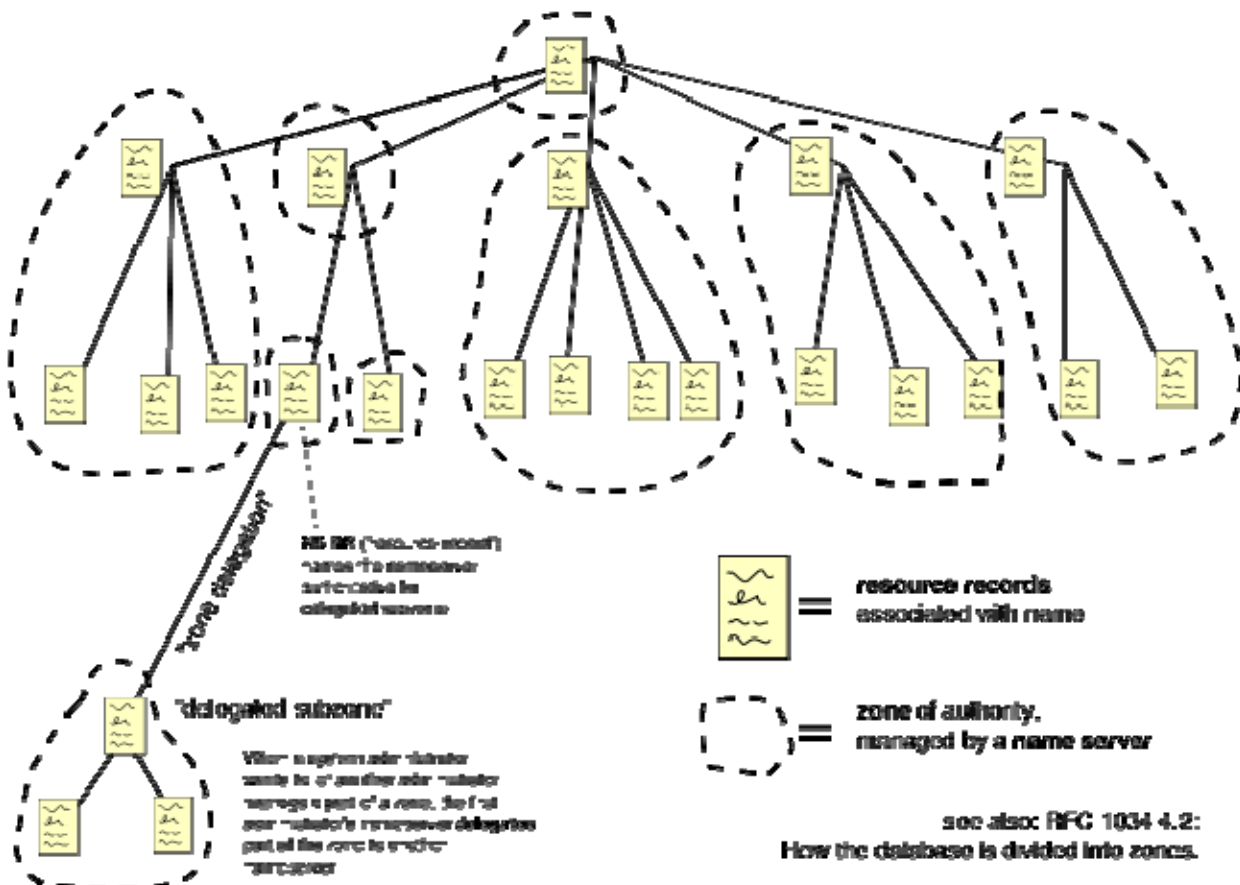
The domain name space is a tree of domain names. Each node or leaf in the tree is associated with resource records, which hold the information associated with the domain name. The tree is divided into zones. A zone is a collection of connected nodes that are authoritatively served by an authoritative DNS nameserver. (Note that a single nameserver can host several zones.)

When a system administrator wants to let another administrator control a part of the domain name space within his or her zone of authority, he or she can delegate control to the other administrator. This splits a part of the old zone off into a new zone, which is served by the second administrator's nameservers. The old zone is no longer authoritative for what is under the authority of the new zone.

The information associated with nodes is looked up by a resolver. A resolver knows how to communicate with name servers by sending DNS requests, and heeding DNS responses. Resolving usually entails recursing through several name servers to find the needed information.

Some resolvers are simple, and can only communicate with a single name server. These simple resolvers rely on a recursing name server to perform the work of finding information for them.

### Domain Name Space



## Microsoft DNS

The DNS support in Microsoft Windows NT (and thus its derivatives Microsoft Windows 2000, Microsoft Windows XP, and Microsoft Windows Server 2003) comprises two clients and a server. Every Microsoft Windows machine has a DNS lookup client, to perform ordinary DNS lookups. Some machines have a Dynamic DNS Update client, to perform Dynamic DNS Update transactions, registering the machine's name(s) and IP address(es). Some machines run a DNS server, to publish DNS data, to service DNS lookup requests from DNS lookup clients, and to service DNS update requests from DNS update clients.

The server software is only supplied with the "server" versions of the operating system, such as Microsoft Windows Server 2003.

## Planning for Microsoft DNS Server Implementation

You will want to install a Microsoft DNS server if the following conditions exist on your network:

- You have established your own domain on the Internet and need a DNS name server.
- Your enterprise needs to implement DNS names on a TCP/IP-based intranet.
- You need a DNS name server that provides a GUI-based administration tool.
- You need to migrate existing non-Microsoft DNS name services to the Windows NT-based DNS server.

The number and location of computers running Microsoft DNS server that are needed to effectively manage DNS name data and name query traffic within your enterprise is a function of the size (number of hosts and their locations) of your network, the links between network subnets, and your network's security requirements.

When planning for the installation of Microsoft DNS server in your enterprise, there are several choices you can make. One option is to create one DNS zone that contains your entire enterprise domain.

The minimum number of DNS servers needed to serve each zone is two—a primary and a secondary—to provide database redundancy. As with any fault tolerant system, the computers should be as independent as possible, for example, by placing the primary and secondary servers on different subnets.

There are some disadvantages to using a single zone. One of the disadvantages is that the primary DNS server may have a problem responding to polling from secondary DNS servers. There are several ways to resolve this problem, such as increasing the secondary refresh interval, configuring some of the secondaries to obtain zone data from other secondaries, and configuring DNS servers in remote locations (or on the far side of a slow network link) as

caching-only servers. (Caching-only servers allow you to avoid the overhead of zone transfers to remote locations or over slow network links.)

Large networks which span multiple sites should not use a single zone but instead use multiple zones to manage their DNS services. This implementation would consist of one root domain with (1) a primary DNS server and one or more secondary DNS servers and (2) one or more zones (and sub-zones as needed), each with a primary DNS server and one or more secondary DNS servers.

A network architect usually breaks up a corporate DNS domain into multiple subdivisions to distribute the administration of parts of the domain to various entities within the enterprise.

Whenever possible, plan to align your Windows NT domains with the organizational structure of your DNS domain, zones, and subdomains.