Domain Name System (DNS)

The DNS is the engine that makes Internet use simple and accessible. The DNS not only facilitates e-commerce and email, but is also the backbone of ATM machines, bankcard payments for groceries, and an increasing volume of long-distance telephone calls.

Every device connected to the Internet has a unique address – just like a telephone number – which is a long string of numbers called IP addresses (IP stands for "Internet Protocol") that are hard to remember. Domain names were created to make it easier to remember and type the address in a browser. So, instead of typing the IP address 66.116.138.39 in your browser, you can type domainmart.com. Ensuring a wide adoption of the mapping of a domain name to its IP address requires secure storage facilities and an efficient mechanism to retrieve the information. To that effect, the management of this system (i.e., DNS) has been delegated to a single entity, ICANN, but not without a controversy.

The Five Components:
The DNS has five integrated components: domain names, IP addresses, servers, communication protocols, and a management structure.

1. **Domain Names:** Also referred to as Internet name or Internet address, a domain name is a unique, intangible asset that represents a virtual address. For a business entity, it is a storefront and a name that customers will remember and use to identify the associated brand.

   Every domain name contains two or more components separated by periods, called "dots." The last part of the address, .com, is called the top-level domain (TLD). To the left of the dot is what is called the second-level domain, DomainMart, which is our brand name. It is also possible to have sub-domains such as accounting.DomainMart.com.[1]

2. **Servers:**
   Servers are computers that perform various functions, which are not necessarily mutually exclusive. There are four types of DNS-related servers:

   a. **Root Servers**. At the heart of the DNS are 13 special computers, called root servers. They all contain the same information, the IP addresses of all the TLDs (called the root zone file). Thus, the files are very small, but the control of their content confers significant soft and hard power upon the managing entity, ICANN. The root servers under ICANN management are referred to as legacy root servers.

[1] For basic information on domain names, see Domain Names: An Introduction, available at http://domainmart.com/DomainNames/information/DomainNames-Introduction.pdf.

For security and system stability reasons the servers are spread across many countries (10 in the US., 2 in Europe, and 1 in Japan).

No Internet traffic passes through these servers. They only respond to queries from other servers when local servers cannot resolve a domain name.

b. **Name Servers**. These computers generally have complete information about some part (a zone) of the distributed domain namespace. The DNS specs define two types of name servers: primary and secondary. Both the primary and the secondary servers for a zone are authoritative for that domain name.[2] Their job is to store names or to get them from other name servers. They are responsible for providing referrals to queries of the domain's sub-domains. Responses that the name server gets from other servers are temporarily stored in cache to eliminate unnecessary network traffic.

c. **Web Servers.** This is where website pages are stored. They can be part of a name server or a stand-alone computer.

d. **E-mail Servers.** This is where e-mail is stored. As in the case of Web servers, they can be part of a name server or a stand-alone computer.

3. **IP addresses:** These are a series of four numbers separated by dots. As a scarce commodity, their value has increased with the global explosion of devices connected to the Internet.

4. **Protocols:** For various devices to seamlessly communicate on the Internet, standards need to be developed and adopted. The Transmission Control Protocol/Internet Protocol (TCP/IP), which was developed in the early 1980s, is the standard host-networking protocol on the Internet.

5. **Management Structure:** The DNS mapping is designed as a distributed database in which domain names are maintained in a hierarchical tree structure, with autonomous zones (administrative units of the domain namespace). For example, Berkeley.edu is an independent zone from .edu, which can be divided into sub-domains, such as cs.Berkeley.edu, which might be a separate zone if administration of Berkeley.edu delegates management responsibility to another organization. ICANN is responsible for the management of the root zone, while each registry is responsible of the management of its TLD zone.

[2] You can find out information about the name servers by performing a Whois search on the domain name.

What goes on behind the scenes?

Translating the domain name into the IP address, called "resolving the domain name," is accomplished by hierarchical name-servers. At the top of the hierarchy are the root servers. Below the root servers are the authoritative servers for each of the TLDs,[3] which are managed by their respective ICANN-approved registries.

To understand how a domain name is resolved, we start with a newly registered domain name, say, NewCompanyName.com. NewCompany hosts its domain name with a unique IP provided by an Internet Service Provider (ISP) who also hosts the content of NewDomainName.com Website.

If anyone types www.NewDomainName.com in a browser:

Stage 1: User's browser queries user's ISP name-server for the IP address.

Stage 2: The ISP name-server will not find the domain name, as it has no information on NewCompanyName.com that has been newly set-up.

Stage 3: User's ISP name-server queries the authoritative .com TLD server.

Stage 4: The authoritative TLD server searches for the IP of the name-server hosting NewCompanyName.com.

Stage 5: The authoritative TLD server contacts the user's ISP local server.

Stage 6: The user's ISP server (a) caches (copies) the IP-domain name information and (b) contacts the NewCompanyName.com hosting-ISP name server.

Stage 7: Depending on whether the request if for a webpage or e-mail delivery, the hosting-ISP name server locates the IP address of the Web server or that of the e-mail server (technically referred to as the MX Record).

Stage 8: For a webpage request, the name server returns the requested page associated with NewCompanyName.com website. Thus, the domain name is resolved.[4] If there is no Web page associated with the domain name, the user gets an error message that the requested site is not found. If the ISP server cannot resolve the IP of an email address, the message will be queued for a latter delivery attempt.

---

[3] Unlike the root servers, these serves do not have names, just IP addresses.

[4] Resolvers are the clients that access name servers. They handle querying a name server, interpreting responses, and return information to the program that requested it. A resolver can generally directly query up to three name servers.

Below the authoritative servers in the DNS hierarchy are local name servers. Each domain name has at least one local name-server that stores the IP, website, and email.[5] The local name-servers are managed by the user (individual or corporate), an ISP, or a registrar. These servers also routinely cache (or store) the information that they receive from queries to the root servers. Below the name servers in the hierarchy are the local Web and e-mail servers.

To locate third-level domain names, for example, accounting.DomainMart.com, the resolver queries a local name-server to find the IP address of accounting.DomainMart.com.

As users try to access WalMart.com through various ISPs, the next time any of these local servers are queried, the process starts at Stage 6b. Thus, caching speeds up responses to queries for popular names considerably. Another important effect of caching is to reduce the load on the DNS as a whole, because many queries do not go beyond the caching servers.

Internet, “internet,” and “intranet”

An internet, with lowercase “i” refers to any network made up of multiple smaller networks each using internet working protocols. An internet is not necessarily connected to the Internet nor does it necessarily use TCP/IP.

An intranet is a TCP/IP-based internet typically used within a company’s internal corporate network. An extranet is also a TCP/IP-based internet that connects partner companies to each other, or a company to its customers, distributors, and suppliers.

Alternative Roots

Anyone can create a new TLD, say, .law. The main concern to the owners of associated domain names is their accessibility by Internet users. Nevertheless, a number of organizations have launched alternative roots or competitive roots (referred to as “alt roots”) to the legacy root. Selecting alternative TLDs is based on a first-come-first-served principle. Thus, their uniqueness is not guaranteed.[6]

The most visible alternative root is New.net, which is the source of more than thirty English-language TLDs such as .kids, .xxx, .law, in addition to a number of Spanish, French, and Portuguese TLDs. A domain name registered through New.net, say, AdultDots.xxx is entered in the New.net DNS. However, since the New.net servers are not directly in the path of traditional domain name resolution, noted in Stages 1-7 above,

---

[5] The local servers do not have to have the same TLD as the domain name they resolve. In fact, most of the local name servers have a .net TLD.

[6] The now defunct Alternic originally launched .biz, currently one of the ICANN-sponsored TLD.

to resolve such names, New.net has resorted to two creative strategies. The fist is to convince a number of ISPs to create a fourth-level domain name for each domain name registered under their alterative TLDs. Thus, AdultDots.xxx would also have a record as adultdots.xxx.new.net. The second is providing a “plug-in” for users to install on their computers. Once this program is installed it intercepts attempts by the user to access any new.net TLD and appends it to the “new.net” domain name. Thus, for those users with the plug-in or use of any of the participating ISPs, the domain name AdultDots.xxx will resolve. However, difficulties start when a user has neither a participating ISP nor the plug-in; they have to type the rather lengthy and cumbersome legacy address -- adultdots.xxx.new.net. New.net boasts that as of March 2005, their domain names were accessible to over 174 million users worldwide.

Persons that neither use one of New.net's partner ISPs nor the New.net plug-in can send and reply to e-mails containing New.net domain names by manually adding ".new.net" to the end of the e-mail address. Such persons also can receive emails containing New.net domain names (without adding ".new.net") in most cases unless the provider of their e-mail service has configured its mail servers to reject e-mails received from addresses containing domain names that its mail servers cannot resolve.

The success of any root directory depends on network effects. The more people connect to a network, the more valuable the network; the more valuable the network, the more people connect to it. Thus, alternative root managers have an up hill battle to convince users of the value in registering domain names under their alternative TLDs. Nevertheless, registration trends for the various New.net TLDs can be a useful guide in selecting future ICANN-approved TLDs.

Appendix: Root Server Operators

The thirteen root servers are operated by twelve organizations referred to as the “root server operators.”

Server	Operator	IP Address
A	VeriSign Global Registry Services	198.41.0.4
B	Information Sciences Institute	IPv4: 192.228.79.201 IPv6: 2001:478:65::53
C	Cogent Communications	192.33.4.12
D	University of Maryland	128.8.10.90
E	NASA Ames Research Center	192.203.230.10
F	Internet Systems Consortium, Inc.	IPv4: 192.5.5.241 IPv6: 2001:500::1035
G	U.S. DOD Network Information Center	192.112.36.4
H	U.S. Army Research Lab	IPv4: 128.63.2.53 IPv6: 2001:500:1::803f:235
I	Autonomica/NORDUnet	192.36.148.17
J	VeriSign Global Registry Services	192.58.128.30
K	Reseaux IP Europeens - Network Coordination Centre (RIPE NCC)	IPv4: 193.0.14.129 IPv6: 2001:7fd::1
L	ICANN	198.32.64.12
M	WIDE Project	202.12.27.33 IPv6: 2001:dc3::35