WHITEPAPER SERIES

A Pedestrian's Guide to the DNS

Version 1.0 **June 1998**

Hong Kong Computer Center, 3/F
54-62 Lockhart Road
Wan Chai
HONG KONG
Tel: +852 2520-0300
Fax: +852 2648-5913

The Peak Tower, 15/F
107 Alfaro Street
Salcedo Village, Makati City
PHILIPPINES
+63 (2) 811-3999
+63 (2) 811-3939

USA Support/Sales: +1 (408) 481-9985
USA Fax: +1 (888) 562-3561

Email: info@ima.com
Website: http://www.ima.com

Please send all comments and suggestions related to the Whitepaper Series to *doc@ima.com*

Introduction

The Domain Name System (DNS) serves as the major telephone directory for the Internet. It is a distributed database that contains a collection of servers used by TCP/IP applications to perform two-way mapping between hostnames and IP addresses and to provide electronic mail routing information.

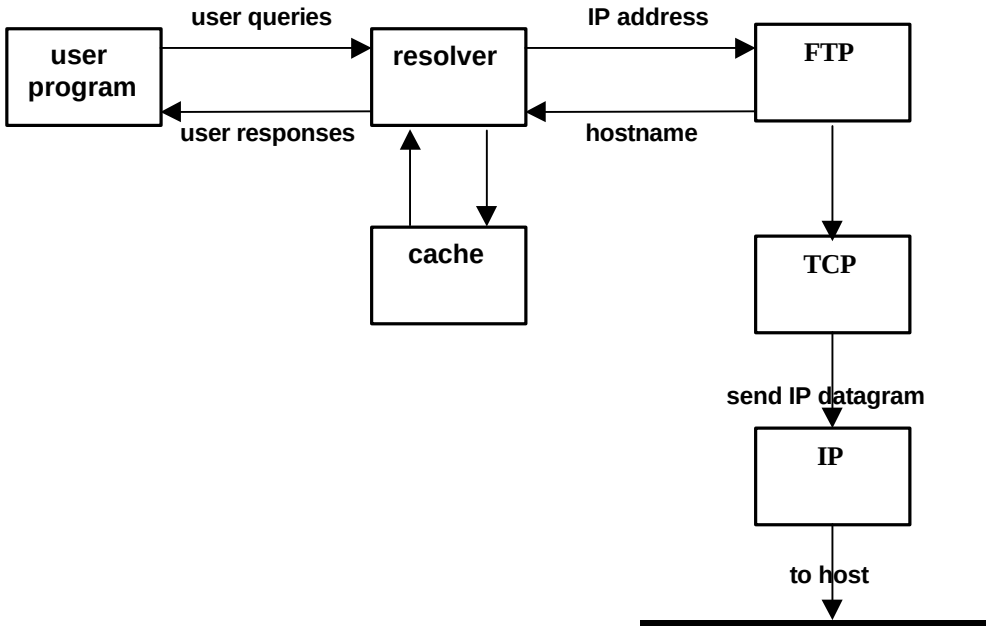
Why there is a need for the DNS

The Internet Protocol (IP) address is a 32-bit integer. In order for a user to send messages via the Internet, he or she must remember the IP address of the recipient. But Internet users prefer to use descriptive, easy-to-remember names instead of numbers. The purpose of the DNS is to translate human readable names into their counterpart IP addresses.

For example, the domain name www.microsoft.com has an IP address of 198.105.232.4. When the domain name www.microsoft.com is submitted to a local DNS server, the DNS protocol returns its corresponding IP address (198.105.232.4). This 32-bit integer is the one used by the underlying networking equipment to convey messages between computers connected to the Internet. If the local DNS server cannot find the appropriate IP address, it directs the request to one of the top-level DNS servers.

Each site (university, company, government institution, etc.) maintains its own database of information. This database can be queried by other systems across the Internet via a DNS server program run by the site.

Figure 1
The DNS Working Scheme



A user program gains access to the DNS by means of a resolver (see Figure 1), software that asks the DNS server for information. The resolver gets the hostname from the client via the user program and returns the corresponding IP address or gets an IP address and returns the corresponding hostname. The resolver returns the IP address before requesting for a connection or sending a datagram using either TCP or UDP.

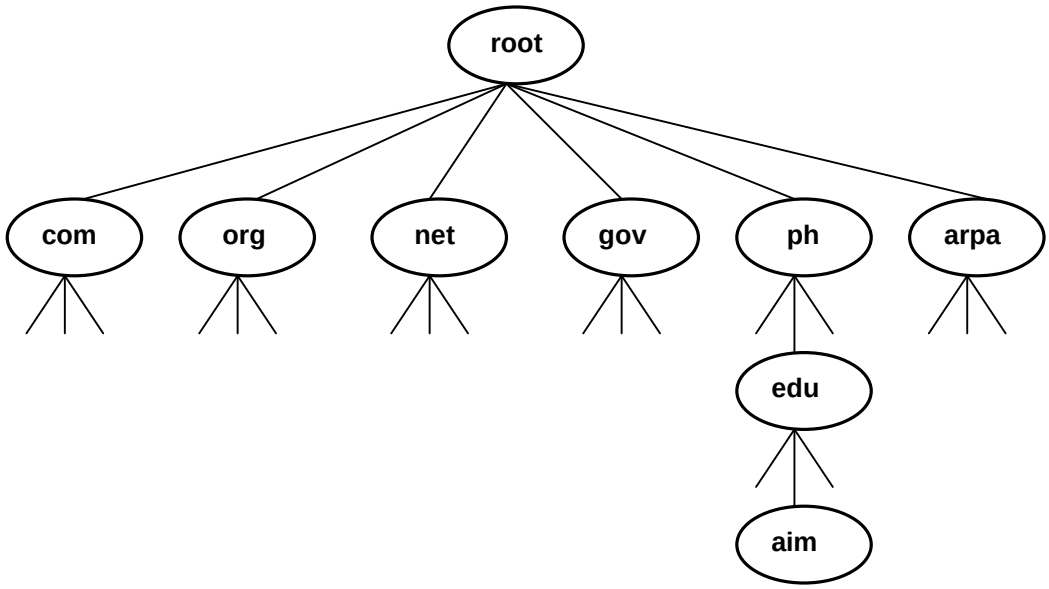
User queries will typically be operating system calls, and the resolver and its cache will be part of the host operating system. Less capable hosts may choose to implement the resolver as a subroutine to be linked to every program that needs its services. Resolvers answer user queries with information they acquire via queries to foreign name servers and the local cache. Most servers have a cache memory for storing recently used domain names as well as the mapping information about these names. The ***time to live*** is the duration wherein information can be cached by a client.

The resolver may have to make several queries to several different foreign name servers to answer a particular user query, and hence the resolution of a user query may involve several network accesses and an arbitrary amount of time. This type of querying is known as ***recursive query***. *RFC 1035: Domain Names – Implementation and Specification* describes the standard format of queries to foreign name servers and their corresponding responses.

The Domain Naming Scheme

The DNS uses a hierarchical naming scheme known as domain names. This is similar to the Unix filesystem tree. The highest label of the hierarchy is known as the ***root,*** which is the last component or ***label*** of the IP address. The root of the DNS tree is a special node with a null label. The domain name of any node in the tree consists of a list of labels starting at that particular node up to the root.

Figure 2
Hierarchical DNS Organization



Top-level Domains

There are two classes of top-level domains used by the DNS. The 2-character domains, which are based on country codes (e.g. us, uk, ph, fr, and ca) as defined in ISO-3166, and the 3-character domains. *RFC 1591: Domain Name System Structure and Delegation* defines five 3-character generic domains used worldwide: *com, edu, net, int, and org*. It also defines two 3-character generic domains used only in the United States: *gov* and *mil*.

Domain Name	Meaning
COM	Commercial organizations
MIL	Military groups
EDU	Educational institutions
GOV	Government institutions
INT	International organizations
NET	Major network support centers
ORG	Organizations other than those above

In practice, most organizations or institutions in the United States are under the 3-character generic top-level domains, while those outside the United States are often under the domain of their country. For example, the domains *ac.jp* and *co.jp* used in Japan are counterparts of the *edu* and *com* domains used in the United States. An exception to this convention is Netherlands, where all organizations are placed directly under *nl.* It does not mean, however, that host listed under a specific country domain is actually located in that particular country. It just means that the host is registered with that country's Network Information Center (NIC). It must also be noted that each country's NIC is free to organize host names in whatever way it wants.

Another domain, ***arpa***, is a special domain used for address-to-name mapping or reverse translation (translating an IP address into its corresponding DNS name). Historically, arpa was the first top-level domain, implemented by the Advanced Research Project Agency (ARPA) in 1969 as part of the ARPA computer network (ARPANET), the predecessor of the Internet.

Second-level Domains

After the top-level domains come the second-level domains, which are assigned by the naming authority for the appropriate top-level domain (in the United States, it is the Internet Network Information Center or InterNIC that oversees domain name registration and IP network number assignment). Lower-level subdomains may be created as desired by organizations that have second-level domains. However, to create a new lower-level domain, permission from the authority that manages the second-level domain is required. So if an interactive multimedia group is created at IMA Philippines, Inc. and wants to be known as *im.ima.com*, it needs to get permission from whoever is managing *ima.com.*

The labels in a domain name are separated by dots or periods. For example, referring to Figure 1, the domain name ***aim.edu.ph*** has three labels: ***aim***, ***edu***, and ***ph***.

This makes it a ***fully qualified domain name***, meaning it includes all the relevant domains. The lowest level domain is ***aim.edu.ph*** (the domain name of the Asian Institute of Management in the Philippines); the second level domain is ***edu.ph*** (the domain name for educational institutions in the Philippines); and the top-level domain is ***ph*** (the domain name for the Philippines). A domain name must start with a letter and must consist only of letters, digits, and hyphens. Starting a domain name with a digit may confuse the software in determining whether the search is being made in terms of a DNS name or an IP address.

DNS Servers

There are currently about 10 DNS servers worldwide that store information about top-level domains and several second-level domains. These servers are known as ***root*** servers. Root servers do not maintain information about machines within an organization, for example, ***aim.edu.ph***, but they store the IP addresses of the domain name servers that contain information about ***aim.edu.ph***. The 10 top-level DNS servers operate based on the principle of redundancy, meaning they contain identical information. This is to ensure that users can always get information about the domain names stored in such servers.

A group of computers using the DNS naming scheme is likely to have a single definitive list of DNS names and their corresponding IP addresses. The group of computers included in the list is called a ***zone***. The computer maintaining the master list for a particular zone has ***authority*** for that zone and will serve as the zone's ***primary*** name server. The ***secondaries*** are servers that download a copy of the domain table from the primary. Secondaries query the primary regularly to determine if the information stored by the latter has changed. If changes have occurred since the previous downloading, the secondaries simply download the entire table again.

Part of the job of a zone administrator is to maintain the zones at all of the name servers that are authoritative for the zone. When the inevitable changes are made, they must be distributed to all of the name servers. While this distribution can be accomplished using File Transfer Protocol (FTP) or some other ad hoc procedure, the preferred method is the zone transfer part of the DNS protocol.

DNS and Electronic Mail

For a computer to send electronic mail (e-mail) via the Internet, it must first know the e-mail address of the recipient.

The e-mail address jsmith@uxa.cso.uiuc.edu, for example, exemplifies a domain-style address, Generally speaking, everything to the left of the @ delimiter is referred to as the local part of the address, usually a mailbox where a user reads his/her mail. A mailbox name often serves as a person's login name as well. In the example, jsmith is the local part, here signifying a mailbox as well as a login name. Domain names are not involved in the local part of an address.

Everything to the right of the @ sign, on the other hand, is referred to as the domain name, which is based upon DNS and outlines where a mailbox is located. The complete domain name, also called the Fully Qualified Domain Name, in the example is uxa.cso.uiuc.edu. It consists of a sequence of symbolic labels, called subdomains, separated by periods.

In most Internet addresses, as in this example, the first subdomain (in listing from left to right) refers to an actual computer, or host, on which the mailbox resides. Uxa is the name of the host where the mailbox for jsmith is found. The next subdomain, cso, refers to the Computing Services Office (CSO), the local organization which owns or runs the host uxa. CSO categorically falls under the next listed subdomain, uiuc, which denotes the University of Illinois. The subdomain listed farthest to the right in a complete domain name is called the top-level-domain. In this example, edu is the top-level-domain signifying the broad category of educational institutions.

The DNS maintains mail-routing information for each domain name. This information tells the sender which computer to send the mail to. It also provides the names of backup computers in case the receiving computer is temporarily down or unreachable. This information is often referred to as MX (Mail eXchanger) records. If the MX records are not available, the mail will be delivered directly to the recipient's host.

Note: *RFC 974: Mail Routing and the Domain System* presents a description of how mail systems on the Internet are expected to route messages based on information from the domain system described in *RFCs 1034 and 1035.*

Security Issues

The Internet Engineering Task Force (IETF) has several working documents that deal specifically with security issues concerning DNS. These working documents propose several schemes to ensure optimum DNS security, including:

- mapping of Autonomous Systems Number into the DNS;
- use of the DNS inverse key domain;
- use of indirect key resource records (RR) in the DNS;
- use of the DNS Security Authentication Referral Record (ARR);
- storage of certificates in the DNS;
- storage of Diffie-Hellman Keys in the DNS;
- use of the zone KEY RRset signing procedure;
- use of DNS security extensions;
- establishment of a shared secret key (TKEY RR) between a DNS server and a resolver;
- and the storage of RSA keys and RSA/MD5-based signatures in the DNS.

The IETF working documents are valid for a maximum of six months, and may be updated, replaced, or obsoleted by other documents at any time.

DNS Requirements

Several requirements that must be met to establish a domain are listed in *RFC 920: Domain Requirements*. First, there must be a responsible person to serve as an authoritative coordinator for domain related questions. This person must have some technical expertise and the authority within the domain to see that problems are fixed.

Second, there must be a robust domain name lookup service, which must be of at least a minimum size. Top-level domains (such as .com, .net, .org, etc.) must be specially authorized. In general, they will only be authorized for domains expected to have over 500 hosts. Second-level domains must have more than 50 hosts.

Third, the domain must be registered with the central domain administrator, namely the NIC Domain Registrar. This governing body requires the administrator of a domain to make sure that host and sub-domain names within a specific jurisdiction conform to the standard name conventions and are unique within that domain.

References

RFC 883
P. Mockapetris, "Domains Names – Implementation and Specification," November 1983.

RFC 1035
P. Mockapetris, "Domain Names – Implementation and Specification," November 1987.

RFC 1591
J. Postel, "Domain Name System Structure and Delegation," March 1994.

RFC 974
Craig Partridge, "Mail Routing and the Domain System," January 1986.

RFC 920
J. Postel and J. Reynolds, "Domain Requirements," October 1984.