Basic DNS Concepts

This section provides brief definitions of additional DNS concepts, which are described in more detail in the following sections of this chapter.

DNS servers. Computers that run DNS server programs containing DNS database information about the DNS domain tree structure. DNS servers also attempt to resolve client queries. When queried, DNS servers can provide the requested information, provide a pointer to another server that can help resolve the query, or respond that it does not have the information or that the information does not exist.

DNS resolvers . Programs that use DNS queries to query for information from servers. Resolvers can communicate with either remote DNS servers or the DNS server program running on the local computer. Resolvers are usually built into utility programs or are accessible through library functions. A resolver can run on any computer, including a DNS server.

Resource records . Sets of information in the DNS database that can be used to process client queries. Each DNS server contains the resource records it needs to answer queries for the portion of the DNS namespace for which it is authoritative. (A DNS server is authoritative for a contiguous portion of the DNS namespace if it contains information about that portion of the namespace.)

Zones. Contiguous portions of the DNS namespace for which the server is authoritative. A server can be authoritative for one or more zones.

Zone files. Files that contain resource records for the zones for which the server is authoritative. In most DNS implementations, zones are implemented as text files.

Domain Namespace

The naming system on which DNS is based is a hierarchical and logical tree structure called the *domain namespace* . Organizations can also create private networks that are not visible on the Internet, using their own domain namespaces. Figure 5.1 shows part of the Internet domain namespace, from the root domain and top-level Internet DNS domains, to the fictional DNS domain named reskit.com that contains a host (computer) named Mfgserver.

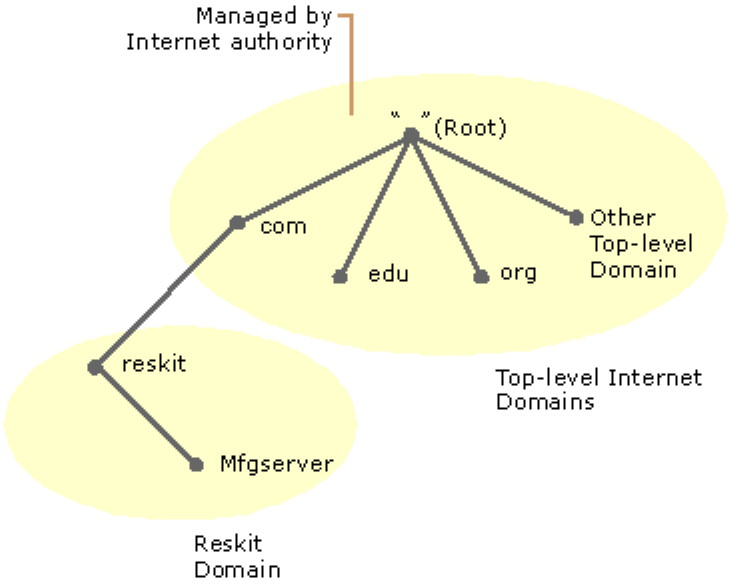

Figure 5.1 Domain Name System

Each node in the DNS tree represents a DNS name. Some examples of DNS names are DNS domains, computers, and services. A DNS domain is a branch under the node. For example, in Figure 5.1, reskit.com is a DNS domain. DNS domains can contain both hosts (computers or services) and other domains (referred to as *subdomains*). Each organization is assigned authority for a portion of the domain namespace and is responsible for administering, subdividing, and naming the DNS domains and computers within that portion of the namespace.

Subdividing is an important concept in DNS. Creating subdivisions of the domain namespace and private TCP/IP network DNS domains supports new growth on the Internet and the ability to continually expand name and administrative groupings. Subdivisions are generally based on departmental or geographic divisions.

For example, the reskit.com DNS domain might include sites in North America and Europe. A DNS administrator of the DNS domain reskit.com can subdivide the domain to create two subdomains that reflect these groupings: noam.reskit.com. and eu.reskit.com. Figure 5.2 shows an example of these subdomains.

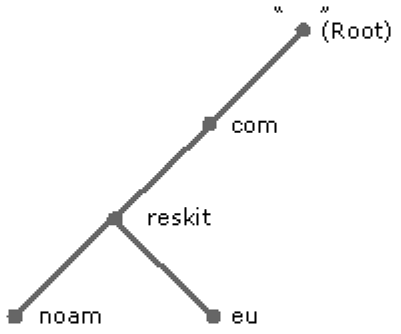

Figure 5.2 Subdomains

Domain Name

Computers and DNS domains are named based on their position in the domain tree. For example, because reskit is a subdomain of the .com domain, the domain name for reskit is reskit.com.

Every node in the DNS domain tree can be identified by a *fully qualified domain name* (FQDN). The FQDN is a DNS domain name that has been stated unambiguously so as to indicate with absolute certainty its location relative to the root of the DNS domain tree. This contrasts with a relative name, which is a name relative to some DNS domain other than the root.

For example, the FQDN for the server in the reskit.com DNS domain is constructed as Mfgserver.reskit.com ., which is the concatenation of the host name (Mfgserver) with the primary DNS suffix (reskit.com), and the trailing dot (.). The trailing dot is a standard separator between the top-level domain label and the empty string label corresponding to the root.

Note

In general, FQDNs have naming restrictions that allow only the use of characters a-z, A-Z, 0-9, and the dash or minus sign (-). The use of the period (.) is allowed only between domain name labels (for example, "reskit.com") or at the end of a FQDN. Domain names are not case-sensitive.

You can configure the Windows 2000 DNS server to enforce some or all RFC character restrictions or to ignore all character restrictions. For more information, see "Windows 2000 DNS" in this book.

Top Of Page

Internet Domain Namespace

The root (the top-most level) of the Internet domain namespace is managed by an Internet name registration authority, which delegates administrative responsibility for portions of the domain namespace to organizations that connect to the Internet.

Beneath the root DNS domain lie the top-level domains, also managed by the Internet name registration authority. There are three types of top-level domains:

- Organizational domains . These are named by using a 3-character code that indicates the primary function or activity of the organizations contained within the DNS domain. Organizational domains are generally only for organizations within the United States, and most organizations located in the United States are contained within one of these organizational domains.
- Geographical domains . These are named by using the 2-character country/region codes established by the International Standards Organization (ISO) 3166.

- Reverse domains . This is a special domain, named in-addr.arpa, that is used for IP address-to-name mappings (referred to as *reverse lookup*). For more information, see "Name Resolution" later in this chapter. There is also a special domain, named IP6.INT, used for IP version 6 reverse lookups. For information, see RFC 1886.

The most commonly used top-level DNS name components for organizations in the United States are described in the Table 5.1.

Table 5.1 Top-Level Name Component of the DNS Hierarchy

Top-Level Name Component	Description	Example DNS Domain Name
.com	An Internet name authority delegates portions of the domain namespace under this level to commercial organizations, such as the Microsoft Corporation.	microsoft.com
.edu	An Internet name authority delegates portions of this domain namespace to educational organizations, such as the Massachusetts Institute of Technology (MIT).	mit.edu
.gov	An Internet name authority delegates portions of this domain namespace to governmental organizations, such as the White House in Washington, D.C.	whitehouse.gov
.int	An Internet name authority delegates portions of this domain namespace to international organizations, such as the North Atlantic Treaty Organization (NATO).	nato.int
.mil	An Internet name authority delegates portions of this domain namespace to military operations, such as the Defense Date Network (DDN).	ddn.mil
.net	An Internet name authority delegates portions of this domain namespace to networking organizations, such as the National Science Foundation (NSF).	nsf.net
.org	An Internet name authority delegates portions of this domain namespace to noncommercial organizations, such as the Center for Networked Information Discovery and Retrieval (CNIDR).	cnidr.org

In addition to the top-level domains listed above, individual countries have their own top-level domains. For example, .ca is the top-level domain for Canada.

Beneath the top-level domains, an Internet name authority delegates domains to organizations that connect to the Internet. The organizations to which an Internet name authority delegates a portion of the domain namespace are then responsible for naming the computers and network devices within their assigned domain and its subdivisions. These organizations use DNS servers to manage the name-to-IP address and IP address-to-name mappings for host devices contained within their portion of the namespace.