Registry Operations

A Reference Guide for
Top-Level Domain Operators

Version 1

The Internet Names Authorization & Information Center
1 Rockefeller Center, PO Box 210
New York City, New York, 10020
United States

Table of Contents

Registry Operations

A Reference Guide for Top-Level Domain Operators, Version 1

Introduction

This document provides information to the Internet community. It does not specify an Internet standard of any kind. This document is for information purpose only. It details the basic functions required to administer a domain directory service database. These databases are used to provide registry services to the Internet community. They resolve the Domain Name System (DNS) and provide contact information for domain name registrants (WHOIS).

This document also discusses the separation of the registry and registrar roles in the administration of a directory services database. This document, however, does not address the protocols and operational rules required for the transmission of information between the registrar and registry. This document is a general discussion of registry operations and will assume that the registry and registrar are the same. References to registries and registrars will be made where appropriate.

This document does not detail the specific technical requirements of any protocol designed for registry operations. Instead this document discusses the basic functions and operational rules essential to domain registries.

This document assumes that the reader has a basic understanding of the DNS and Internet protocols.

This document is a work in progress. Readers are welcomed to contribute to it. All contributions will be recognized.

A brief history, The Internet and DNS

The Internet (ARPAnet) was first introduced as a US Defense Department experiment in 1969. There were only 4 initial sites interconnected via a packet switched network. These sites were located at the University of California – Los Angeles (UCLA), the Stanford Research Institute (SRI), University of California, Santa Barbara (UCSA), and the University of Utah.

Static tables were incorporated to resolve host names to machine addresses. These tables are known as the "hosts.txt" file. This file was centrally maintained by the Defense Data Network (DDN) Network Information Center (NIC) at SRI. The NIC was the Internets sole registry. The hosts.txt file was distributed from the NIC at SRI to all hosts on a regular basis.

In 1971 the Internet grew to 15 hosts. Email was introduced that year. By 1977 the number of hosts exceeded 100. These systems were primarily located at universities and US military installations.

In 1982 the number of hosts reached 300. By this time the difficulties of managing a human edited flat file database from a central location caused problems. Many hosts on the old ARPAnet were more than a day out of sync with the master hosts.txt file.

It became apparent to the Internet community that as the host table increased in size it would prove very difficult to provide directory services from one central location. The anticipated size and dynamics of the data required to accommodate this rapid growth made such an approach impractical.

To address these problems a method for labeling hosts was developed that would facilitate communications through a numbering system. The schema used a hierarchical-distributed system for mapping machine addresses to host names. The approach became very popular with the public as it provided them an intelligible and easy way to navigate the Internet. The technology was officially introduced in 1985, and continues to exist today. It is called the Domain Name System, or DNS.

The implementation of the DNS came just in time to support the exponential growth in Internet hosts. From 1985 to 1995 the number of hosts increased from 2,000 to 8 million. It was fortunate that this distributed technology was introduced or the Internet would be a very different place today.

The Role of Registry and Registrar

The DNS solution distributed the administrative burden of mapping hostnames to addresses through entities known as registrars. A registrar is an entity that provides a public (front-end) interface to registry services (the back-end) for domain name registrations. Registries may provide the back-end interface for domain name registration services to registrars.

Historically the role of registry and registrar were synonymous. The commercialization of the Internet necessitated a “competitive” and “non-monopolistic” model that distributed the responsibilities of providing registration services among several independent operated organizations.

The registry manages the zone or central repository of information associated with domain name delegations. Registries are typically responsible for publication and distribution of zone files used in the DNS. Likewise, registrars provide services to individuals and organizations that facilitate domain registration. The duties of registry and registrar may be logically separated but many registries perform both functions.

The Registry Model, “Thick” or “Thin”

Domain registries use one of two models to facilitate domain registration. The "thick" model contains directory service data for DNS operations and contact information. “Thick” registries usually provide service directly to the domain registrant but may also interface with other domain registrars.

The "thin" model on the other hand contains only operational data for domains. This data would be composed of technical elements required to resolve the DNS. The minimum technical elements required are domain names, name server hosts, and address “resource records” (RRs, in the form of “A” and “NS”) associating hosts, name servers, and IP addresses registered in the zone.

In the "thin" model the registrar maintains the domains contact data. Registrars may accept both “thick” and “thin” domain registrations from registrants on behalf of domain registries.

This document discusses the “thick” registry model. Where appropriate, references to the “thin” model will be made.

Manual or Automated Registries

A registry maintains and administers a database of objects required to resolve the zone in the DNS. Domain name registrants usually modify their zone data (domain) through a public web interface. This automates the process of maintaining the database.

Registries can maintain their databases manually. The manual maintenance of a public registry database is not typical in today’s computing environment, nor is it recommended in most cases.

Manual maintenance can be used in special cases. A registry may use manual updates to limit potential abuse or where domain registrations are for a temporary, transient period.

The verification process would prevent direct access to the registry databases. The verification procedure would ensure that any modifications, deletions, or additions to domains are first authorized. Banks and other financial institutions are a community of users this model would benefit.

Verification procedures could be an integral part of the registry business plan. A good example would be DNS services exclusively tailored to the special needs of recognized financial institutions. The registry that administers this zone may require a recognized signature on file to authorize any changes to zone data.

This document provides recommended procedures on the maintenance of a zone database. These recommendations can be used to administer either manual or automated databases.

The Database Engine

The choice of a database engine is dependent on the technical requirements of the registry. This document does not review the merits of any database engines or related applications. This document does provide recommended procedures that can be applied to the development of applications that control access and manage the registry databases.

Popular database programs used by registries are Oracle, MySQL, PostgreSQL, Sybase, and INGRES. The Internet Software Consortium has an implementation of a domain registry called OpenReg. This is an integrated package of applications that registry operators and registrars can use to manage the delegation of domains.

Contacts and Zone Records

The basic operation of a registry database is divided into two parts: contact records for domain registrants and administrators support directory services. Zone resource records (RRs) for the domain's "Start of Authority", hosts, or name servers and IP addresses (SOA, A, NS, and PTR resource records, respectively) store the technical elements required to publish, propagate, and distribute the TLD's zone file.

Contact records identify the registrants and administrators of domains. Some registries assign specific roles to administrators such as billing, technical, administrative, and abuse. This document treats all contacts as administrators.

A registrant may be a person or an organization. A contact may be a person or a "Role Account", that is, an entity where an employee or team of people fill the role of that particular contact.

An administrator may be a person, organization, or department. Some registries may provide restrictions that prevent administrators with specific roles from making certain designated changes to the domains records.

Registrant contact records contain the proper name of an organization, person, or other legal and serviceable entity that has authority over the domain record. The contact address, telephone numbers, and email of the registrant are also stored in registrant records.

A registrant contact record must be maintained by an administrative contact. This administrative contact has authority over modifications made to the registrants contact and name server records. The legal entity that is named in the registrant contact record has final "legal" authority over any modifications made.

Administrative contact records are maintained by the person, company, or organization named in the record. The entity named in the administrative contact record has direct authority over any modifications made.

Zone records store the 'Start of Authority (SOA)', host names, IP addresses, refresh rates, zone version serial number, and responsible party (RP) data for their respective domain names. These are the basic technical elements required to publish a TLD zone file.

All domain names are associated with registrant and administrative contact records. A domain may have many administrators. It is recommended that the registry allow for a minimum of three administrative contacts per domain. A domain may only have one registrant.

Domains, Hosts and Name Servers

Domain name labels follow rules established by ARPAnet. Domains may include any combination of alphanumeric characters including the "-" (hyphen) symbol. Labels must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphens.

Domain name labels must be 63 characters or less. While upper and lower case letters are allowed no significance is attached to the case. Two labels with the same spelling but different case shall be treated as being identical or equal.

Domain names are always associated with host names. These hosts are the name servers that maintain the authoritative data on the zone. There must be a minimum of two hosts per domain. This is to provide the zone with redundancy. If one host is unavailable the other host can respond to a DNS query.

Early registries, such as SRI, required each registrant to have at least two name servers. It was also mandated that the hosts must be on geographically distant or separate packet switched networks. Hosts were tested to see if they answered authoritatively for the domain – before a domain registration would occur.

A DNS zone file should contain no more than a maximum of thirteen name server resource records (NS RRs). Contrary to common assumptions this is not due to technical limitations in the DNS. This limitation on the number of name servers is influenced by the packet size limitation in the UDP protocol.

The UDP protocol is the primary transport protocol used in the transmission of DNS queries and responses. DNS is able to also use the TCP protocol, if necessary, as the transport.

It is perfectly legal in DNS to have more than 13 NS RRs per zone file. This results in increased traffic during the DNS resolution process. On average no more than 13 NS RRs can be transmitted in the confined size of a UDP packet.

If more then 13 NS RRs exist in the zone the DNS would have to transmit multiple UDP packets. At the very least this would double or triple the traffic. It is possible to include more then 13 NS RRs in a UDP packet only if the host names are extremely short.

Therefore we strongly recommend registries restrict the maximum number of name server hosts to thirteen.

Parking Domains and Lame Delegations

Modern domain registries provide registrants the ability to "park" their domains with the registry. This type of service offering facilitates the registration of domain names to prospective registrants who don't have name servers readily available.

Parking also avoids the vagaries of a problematic phenomenon known as "Lame Delegation". Lame delegations cause serious problems mainly associated with increased traffic in the DNS. A lame delegation is a situation where a domain has no name servers associated with it.

A lame delegation can also happen when the servers to whom the zone is delegated have authoritative data for the zone but are unavailable. The domain is effectively not locatable from the net. It doesn't matter if there are other servers that have authoritative data for the zone, because they are not listed in the delegation.

Domain "Parking" permits the prospective registrant to complete the registration process without having name servers available and avoids the senseless DNS traffic due to lame delegations.

The registry or registrars business policy determines what answers these hosts provide the DNS when queried. The industry standard practice is to forward all queries for parked domains to servers that advertise the registry. This is a marketing consideration for a registry operator and not a recommendation.

Early models for domain registration included provisions for “Reserving” a domain, as opposed to registering domains. This effectively protected the name from being registered by some other individual or organization.

This was usually done to provide the registrant time to setup at least two name servers answering authoritatively for the domain. It is strongly recommended that a registry park their domains instead of registering them.

Parked domains are associated with a minimum of two name server hosts operated by the registry. These hosts answer authoritatively for the parked domains. Providing services such as domain parking is strongly recommended.

Hosts created within the TLD zone must be validated. Special rules apply to these hosts and their parent domains. Special rules also apply to the administration of hosts and their parent domains. These rules restrict administrators’ rights to modify or delete these hosts and domains. All host records of parent domains in the zone must be associated with IP addresses.

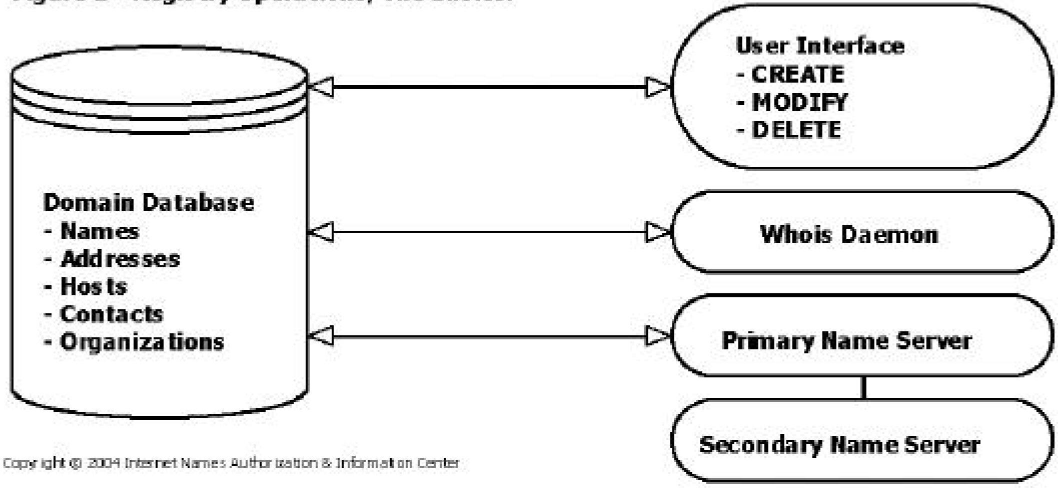
Registry Basics - The Mechanics

The operation of a registry facilitates the maintenance of a database of records and the provisioning of associated support services. Figure 1 provides a comprehensive overview of a registry operation.

The services that access the registry database are the user interface, WHOIS directory services, and DNS referrals to authoritative (AUTH) name servers.

Administrators are permitted access through the user interface. This is usually accommodated via a website where administrators can CREATE, MODIFY, or DELETE records.

Figure 1 - Registry Operations, The Basics.



Copyright © 2004 Internet Names Authorization & Information Center

WHOIS services provide the Internet community with directory services detailing the contact records for domain registrants, administrative contacts, and timestamps for the creation, modification, and expiration dates of the domain registration.

WHOIS daemons are servers which answer on TCP port 43, providing WHOIS services. The WHOIS service is an Internet standard protocol. It is recommended that registries provide directory services via a whois daemon.

In addition to the standard availability of WHOIS services on TCP port 43, registries also commonly provide access to their WHOIS directory services via a web interface as a convenience. Some registries do not operate WHOIS daemons or provide WHOIS services – this is not recommended.

With regards to DNS resolution of TLDs; DNS queries for TLDs are answered by the TLD Servers designated by the registry as AUTH for that particular TLD. A registry must have a minimum of two TLD Servers. These hosts, according to the Internet RFCs, must be on separate packet switched networks at geographically equidistant locations.

Multiple name servers provide the zone redundancy and prevent potential outages. If one TLD server is unavailable the other(s) will respond instead to the query. A TLD zone may have a maximum of thirteen name server hosts. This is due to technical limitations in the UDP protocol, not DNS.

Administrative Controls

Administrative contacts have the right to access and manipulate database records associated with them. Administrators can CREATE, MODIFY, and DELETE domain registration records. Special rules may restrict an administrator's right to CREATE, MODIFY, or DELETE these records. These rules may be administrative or they may reflect intentional technical limitations in the DNS – i.e., in order to prohibit lame delegation due to orphaned child domains.

Registry database objects and records are dependent. For example, a registrant should not be allowed the right to delete a registrant contact record if that record is associated with a domain. If the deletion is allowed the domain ends up orphaned. This should never be allowed. This is an example of an administrative rule.

Domain names should not be deleted if they are parents of active child domains registered in the zone. These zones, and their associated registrations, can be deleted if their hosts only provide authoritative DNS responses to the parent domain. In this case the domain and associated host records are deleted.

If the host provides authoritative DNS responses to another domain in the zone the parent domain and hosts can not be deleted. If these domains are deleted the host names end up orphaned. If the hosts are deleted the domains associated with those hosts stop resolving. This example reflects an inherent technical limitation in the DNS.

If these issues are not addressed the registry could be held hostage. Abusive registrants could register domain names and hosts. They would then associate those hosts in a chain of dependence within the zone. This would prevent the deletion of any domain or record that is a part of the chain.

This is an example of a technical limitation discovered when the Internet domain system was undergoing commercialization. Network Solutions, the former registry operator of the .com, .net, and .org TLDs had this problem when they started charging registrants yearly fees.

Attempts to delete domains associated with overdue accounts failed and resulted in damage to the DNS. Child host domains were orphaned, with no parent zones pointing to them any longer.

A Solution to Lame Delegations

There are two types of lame delegations to be found in a TLD zone file. The first type is hosts that are children of domains listed in the TLD zone file. We shall call these hosts "Zone Hosts". This type of lame delegation is preventable.

The next types of lame delegation are orphaned children from domains deleted in other TLD zones. We shall call these hosts "Foreign Hosts" for the purpose of this discussion. This document does not make any recommend on procedures for fixing the lame delegations of Foreign Hosts. We only focus on Zone Hosts in this discussion.

The first procedure to overcoming this technical limitation in the DNS is to create a domain in the TLD zone for lame delegations. For the purpose of providing an example we shall use the label "lame" as our domain name.

The administrator of this domain shall be a person or role account. This account shall be assigned by the Registry that is in control of the publication of the TLD zone file. This domain shall have a minimum of two name server hosts operated by the Registry. These hosts answer authoritatively for the "lame" domain.

The Fully Qualified Domain Name (FQDN) would in this case be "lame.tld" where "tld" is the TLD label in the root zone. The domain "lame.tld" will then be used for the sole purpose of creating host names. These host names shall be assigned the IP addresses of orphaned name server hosts.

For demonstration purposes we will assume an administrator or Registry wants to delete a domain name called "delete-me.tld". This domain is the parent of a Zone Host listed in the TLD zone file as "ns1.delete-me.tld" with the IP address 192.168.123.111.

If the host "ns1.delete-me.tld" only provides DNS services to itself ("delete-me.tld") then the host and domain records (A & NS RRs) can be safely deleted. If the host "ns1.delete-me.tld" provides DNS services to another domain listed in the TLD zone file then additional steps are taken to prevent a lame delegation.

If these steps are not taken and we delete the domain "delete-me.tld" from the zone we orphan the host "ns1.delete-me.tld". If we delete the host we in turn terminate any DNS services it is provides to other domains in the TLD zone. This will cause a lame delegation affecting the dependent domain(s). For the purpose of discussion we shall call the dependent domain "example.tld".

In order to prevent a lame delegation when the Zone Host "ns1.delete-me.tld" is deleted we must first create a new host using the "lame.tld" domain. We shall call this host "ns-1002.lame.tld". This host is then listed in the TLD zone file with the same IP address as "ns1.delete-me.tld". In this case the IP 192.168.123.111 would now be the address resource record (A RR) for "ns-1002.lame.tld".

Then we replace the name server resource record (NS RR) "ns1.delete-me.tld" for the "example.tld" domain with the new host name "ns-1002.lame.tld". This process is repeated until all NS RRs for domains formerly associated with "ns1.delete-me.tld" are replaced with the new host name "ns-1002.lame.tld".

Once the modification are in place the host and parent domain records for "delete-me.tld" can be safely deleted without putting other domains in jeopardy of disappearing from the DNS.