



September 2000

white paper

Understanding DNS:
How to Register for, Configure,
and Change DNS Service

REAL WORLD EXPERIENCE

Certainty Solutions, Inc.
999 Main Street
Redwood City
CA 94063
650.569.4600
650.569.4697 Fax

certainty
solutions.

Introduction

DNS (the Domain Name System) is the process by which words from a common recognizable language, like www.certaintysolutions.com, are converted to IP addresses, such as 198.151.248.248. Software such as mail readers and Web browsers actually use the IP address rather than the DNS name when sending and receiving e-mail or connecting to a Web site. Since humans (and program preference files) use DNS names almost exclusively, when DNS service for a domain doesn't work, your site is effectively off the Internet, even if your site is up and functioning in all other ways.

This makes reliable DNS service a vital piece of your Internet-based service, both when you set up your site and whenever you move machines or change providers. In order to understand what potential problems are associated with setting up initial DNS or in transitioning from one provider to a new one, all the pieces involved first need to be clearly understood.

In this paper, we will explain how DNS works, the components involved, set-up requirements, and the potential problems that could arise if it is not working or set up correctly. We will also take a look at problems that can occur when transitioning to a new provider.

How to Register for DNS Service

DNS lookups

When a user types in a Web site name, like www.amazon.com, their PC asks a local DNS resolver to resolve that name into an IP address. This local resolver takes the name and, starting from right to left, looks up each part of that name. The local resolver knows that `.com` is a top level domain (TLD) and has a list of root servers that it knows to ask about domains registered within each TLD zone. This is done when the local resolver is initially configured.

The local resolver makes a query to one of these root servers asking it to resolve the second level name (i.e., `amazon.com`). The root server returns a list of servers that are authoritative for that zone, giving both DNS names and IP addresses for all the authoritative servers. The local resolver picks one of the servers (usually randomly depending on the resolver) and asks it to resolve the full name (i.e., `www.amazon.com`). The authoritative server returns the IP address to the local resolver, which returns it to the user's PC. Then their browser opens a connection to that IP address.

Registries

When a company decides they want a presence on the Internet, they first pick a domain (DNS) name, usually something like `company-name.com`. The company then chooses a registry service

Understanding DNS: How to Register for, Configure, and Change DNS Service

Certainty Solutions - white paper

with which to register that domain name. While Network Solutions had a monopoly on names with .com, .net, and .org, there are now multiple companies that handle name registration. You can find out a list of registries at <http://www.internic.net>.

Assuming that the name of your choice is not already in use, you can reserve your DNS name. The registry service will ask you to provide various information, including primary server, secondary server(s), company information, and e-mail contacts for billing, administrative, and technical problems. (See “Set Up” below for more details).

Root servers

The root servers answer queries about second level zones and registered hosts. For second level zones (such as certaintysolutions.com), the root servers give the list of authoritative servers for the zones. Registered hosts are those hosts for which the root servers are able to resolve from DNS names to IP addresses. Since many servers are within the zones they serve (i.e., ns1.certaintysolutions.com is in the certaintysolutions.com zone), the root servers need to have this information within their own local files.

When a registry service registers a new domain, they send the information on that domain to all the registries. The information consists of the list of registered hosts that are the authoritative servers for that new domain.

Whois servers

Whois is a protocol (RFC 954) that provides directory services relating to domain names and the entities that own them. This includes company addresses, the list of authoritative nameservers for zones, registered hosts, and zone contacts (NIC handles). Registries run local whois databases for the zones that they register. If you are not sure which registry serves a particular domain, you can check at the Internet whois server. Whois.internic.net will respond with the whois server name for the appropriate registry. If your PC does not come with whois software, use the Geektools WHOIS Proxy.

Set Up

You need to pick the registry you will use to register a domain name. There is certain information you will need for the registration form:

- **Company name and address** — This should be self-explanatory.
- **Zone contacts** — This is important. The listed e-mails should get to the right person/group to solve that type of problem. The zone and administrative contacts should be staff familiar with the purpose of the site. The billing contact should be the one who pays your invoices. The technical contact should be whoever is running the primary nameserver for the zone.
- **Name servers** — These will either be your providers' nameservers, your own name servers, or a mixture of the two.

Issues that might arise during your set up are:

1. **Who owns the primary zone file.**

Whichever nameserver is the primary nameserver will be the one where changes in the zone will need to be made. It is up to you to decide which nameserver this is. If your provider is not running all the nameservers, things to consider are if someone is available on pager 24-hours a day who has access to the primary zone file, how often the zone is changed, etc. Remember that in an emergency or outage, being able to change a zone file can be crucial.

2. **All nameservers must be registered hosts before the zone can be registered.**

So, if you want to use a host that is not a registered host with the registry of your choice, you won't be able to register your domain until all the nameservers are registered hosts.

3. **All nameservers should not be on the same LAN.**

Unfortunately, not all client software or server software deals politely with a domain where the root servers give a valid list of nameservers but none of them are reachable. This can cause e-mail to bounce back to the sender or some Web browsers to display odd error messages. To the end user, it may seem that the Web page or e-mail address isn't valid and give up on your company or service. The odds of this happening are much higher if all of the nameservers are on the same LAN. The IETF document BCP 16 has further details on network load and other problems related to all authoritative nameservers being unreachable.

4. **All nameservers should be reachable from the Internet at all times.**

This means that if they are behind a firewall that DNS queries are allowed through. You should never put a nameserver on an intermittent link. Remember that when a local resolver gets a list of authoritative nameservers and it can't reach one, it has to take a timeout. This means that if you have two nameservers, and one is never reachable, that half the time, every user will have to wait for a timeout (usually 60 seconds) before getting an answer.

Moving Your Site

When you switch providers, you will probably have to switch your IP address space. You will also probably be changing the authoritative nameservers. Ideally, you would leave the old site running until the new site is up and tested. If not, you will need to make sure that the authoritative nameservers for your zone are reachable during the whole move, either by putting extra machines into the new address space before the move or by having all the nameservers be in address space and physical space external to your own site.

Most of the steps in dealing with the registry, for decisions on placement of nameservers, and in decisions effecting which nameserver will be primary, are the same steps necessary for creating a new site. Here are some of the subtle differences:

Registered Hosts: Make sure that you get the new addresses registered. Since the registries track unique hosts by IP address instead of name, you can register ns1.*company.com* with a new IP address without having to change the old entry. Remember that you can't use a registered host in a domain name application or change request until it's in that registry's database.

Primary Nameserver: As soon as you can, have one of the new nameservers be the real primary nameserver. Have all the other nameservers, including all the old nameservers, be secondary off the new primary. That way, even if the root servers only have the old nameservers listed, those nameservers will have the zone file you want.

Drop TTL: TTL stands for Time To Live. This is a timer that tells resolvers how long to keep an entry from your domain before they expire it and do a new DNS lookup. You should set this down to something close to five minutes. That means when *www.company.com* changes from IP address 1.2.3.4 to 5.6.7.8, it will only take five minutes before users go to the new site.

Sequence of Change: Don't just send in a request to have the old nameservers changed to the new nameservers unless you can build a new site that will take a full load without having to take down the old site. There is a period of hours to change a registry database and then push that change to the root servers. The best way to do this is:

- Bring up new nameservers (have old IP addresses and low TTL in zone file).
- Switch all the other nameservers to secondary off of the new primary.
- Add the new nameservers to the list of nameservers in the registry.
- Do the move and change the zone file to have the new IP addresses.
- Have the registry delete the old nameservers from their database.
- Only after the root servers and your registry whois database no longer have the old nameservers should you decommission them.

Further Reading

Here are some useful RFCs that relate to DNS:

- BCP16 — Selection and Operation of Secondary DNS Servers
- FYI27 — Tools for DNS Debugging
- RFC974 — Mail Routing and the Domain System
- RFC1912 — Common DNS Operational and Configuration Errors
- STD13 — Domain Names — Concepts and Facilities

For a more detailed treatment, the O'Reilly Publishers' books on DNS are excellent:

- DNS and BIND, 3rd Edition, By Paul Albitz & Cricket Liu, 3rd Edition, ISBN 1-56592-512-2
- DNS on Windows NT, 1st Edition, By Paul Albitz, Matt Larson & Cricket Liu, ISBN 1-56592-511-4

Definitions of DNS terms:

Zone: A part of the DNS tree, that is treated as a unit.

Forward Zone: A zone containing data mapping DNS names to IP addresses, mail exchange targets, etc.

Reverse Zone: A zone containing data used to map IP addresses to DNS names.

Server: An implementation of the DNS protocols able to provide answers to queries. Answers may be from information known by the server, or information obtained from another server.

Authoritative Server: A server that knows the content of a DNS zone from local knowledge, and thus can answer queries about that zone without needing to query other servers.

Listed Server: An Authoritative Server for which there is an "NS" resource record (RR) in the zone.

Primary Server: An authoritative server for which the zone information is locally configured. Sometimes known as a Master server.

Secondary Server: An authoritative server that obtains information about a zone from a Primary Server via a zone transfer mechanism. Sometimes known as a Slave Server.

Stealth Server: An authoritative server, usually secondary, which is not a Listed Server.

Resolver: A client of the DNS which seeks information contained in a zone using the DNS protocols.

Registered Host: A host whose IP address and domain name have been put into a registry's whois database and into the root server local zone files. Usually an Authoritative Server for a zone.

Root Server: These hosts serve the root or "." domain. They contain the zone files for the top level domains, such as .com, .net, etc.

Understanding DNS: How to Register for, Configure, and Change DNS Service

Certainty Solutions - white paper

About Certainty Solutions, Inc.

Certainty Solutions is the leading integrated managed services provider (IMSP) for companies with sophisticated Internet businesses. The company provides customers with both pre-packaged and customized site architecture solutions, standard and a-la-carte managed services offerings, implementation services and hosting/bandwidth solutions.

For more information about this topic, or to speak to a Certainty Solutions representative, please call 650.569.4600 or email info@certaintysolutions.com

www.certaintysolutions.com