

Prepared By:

VeriSign Global Registry Services
21345 Ridgetop Circle
Dulles, VA 20166
1.703.948.3200



A White Paper on VeriSign Managed DNS Services

November 2001

VeriSign Secondary Name Server Hosting

Introduction

If your business depends on the Internet, you understand the importance of a reliable Domain Name System (DNS) infrastructure. Every Web site request and every email sent through the Internet must pass through the DNS in order to reach its intended location. A less than optimal DNS infrastructure to support your Web presence can result in poor resolution time or even complete inaccessibility, meaning lost business and dissatisfied customers. Conversely, a robust and reliable DNS can reduce resolution times, leading to an enhanced customer experience and increased sales.

The domain name space is comprised of zones that many companies manage on their own name servers. Although the term is often used interchangeably with domain, the difference is that a zone is the administratively delegated portion of the domain that comprises the authoritative information used to direct Internet users to a company's Web site(s). Managing a zone and its authoritative name servers requires time, money, and an administrator with substantial training and experience. The expertise of an administrator is critical, as the syntax of zone data files and name server configuration files is subtle and unforgiving.

To ensure robustness, name servers on different networks should service a zone. To provide optimal performance, a zone's name servers should be distributed throughout the Internet, as close to users and hosts as possible. These two steps will greatly reduce the likelihood of inaccessibility and ensure that resolution times are kept to a minimum. Studies have shown that in today's fast-paced world of e-commerce, delays of as little as one second can greatly affect the "bail out" rates of potential customers visiting Web sites. Building DNS infrastructures close to these customers can help reduce resolution times.

The cost of placing and operating servers in multiple, strategic locations is prohibitive to most organizations. The result is that companies often limit the number and distribution of their name servers, which makes them vulnerable to catastrophic failures when DNS problems occur.

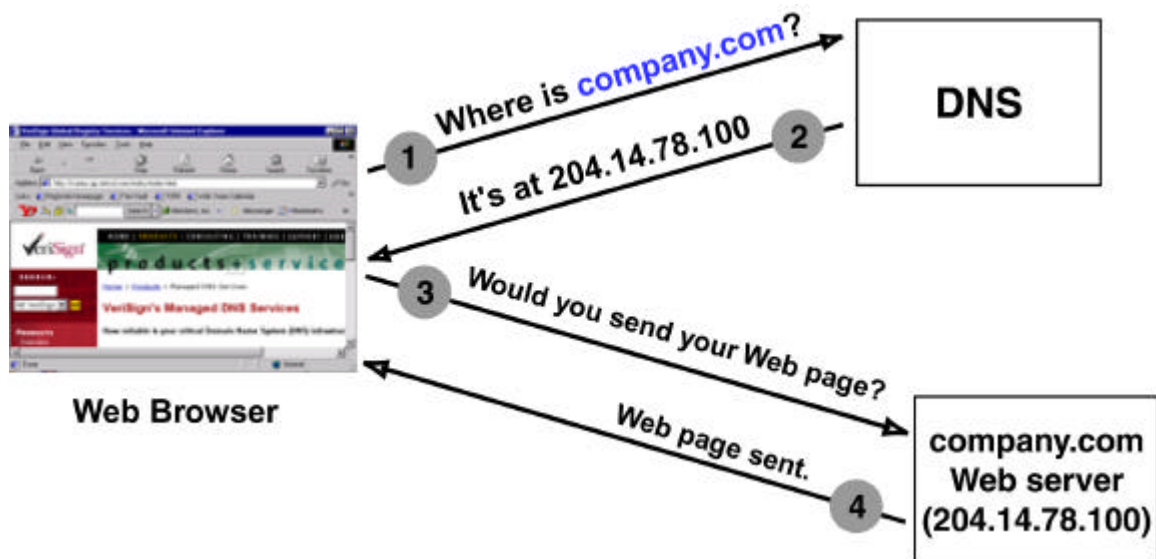
This paper outlines the intricacies of DNS in terms of how it works and what its biggest challenges are for a company administering its own DNS. In addition, it discusses VeriSign Secondary Name Server Hosting, which can help companies alleviate some of their concerns around DNS and concentrate their resources on core business initiatives.

Domain Name System Overview

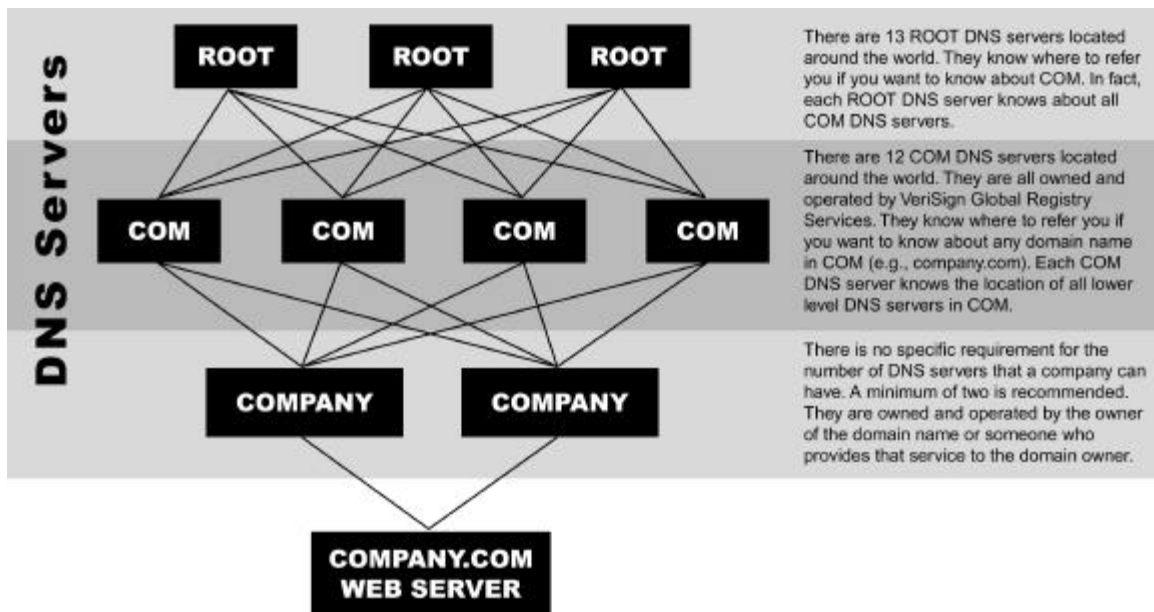
The Domain Name System (DNS) is part of the fabric that holds together today's modern Internet. It performs a simple, straightforward function: mapping names to IP addresses and back. When it breaks, the effects are severe and widespread.

Every Web server on the Internet has one or more unique IP addresses. An IP address is a simple set of four numbers separated by dots (e.g., 204.14.78.100). Any Internet user (via a Web browser) can contact any Web server on the Internet by simply typing in the IP address. However, it is difficult for most people to remember more than a few IP addresses, just as it is difficult for most people to remember more than a few phone numbers.

DNS allows people to use names (e.g., “company.com”) to identify Web servers, rather than IP addresses. DNS performs the translation between the name and the IP address or addresses. When an Internet user types “company.com” into a Web browser, DNS translates that domain name into an IP address. The browser then connects to the Web server at that address. The diagram below demonstrates this simple process.



The service DNS provides—mapping names to addresses—is supported by an entire global network of **name servers**, managed by many different organizations and arranged in a tree-like structure. No single name server knows every Web server’s address, but each can navigate the hierarchy until it eventually finds another name server that does know the address.



As the diagram above demonstrates, the root name servers do not know where the company.com Web server is located, but they can refer an inquiry to the .com name servers. While the .com name servers also do not know where the company.com Web server is located, they can refer an inquiry to the company.com name servers, which do know the IP address of the company.com Web server. Understanding this hierarchy is critical to understanding the need for geographically distributed name servers.

The information that translates domain names into IP addresses has two other characteristics that are important to understand.

Name servers around the world cache information from other name servers. For example, the first time one of an ISP's customers tries to access company.com, the ISP's name servers will likely have to ask one of the com name servers and then one of the company.com name servers, to get the IP address of company.com's Web server. But the ISP's name server remembers that answer so that the next time it's asked, it will refer the user directly to company.com's Web server.

There is a time limit on how long name servers can cache the information. This limit, called Time-To-Live (TTL), is determined by company.com's name servers. They basically say, "Here is the answer, and I would appreciate it if you would remember this only for the next hour" (or whatever period the administrator of company.com has chosen).

Managing the Process

Although this illustration seems basic, a DNS administrator knows how much can go wrong and how much administration is involved in keeping it running. Comprehensive DNS management is complex. It requires careful planning, substantial expertise, and considerable resources, and is critical to the effective operations of business on the

Internet. Unfortunately, most companies do not recognize the faults in their existing DNS infrastructure until it is too late—and they have lost revenue and customers.

A study conducted by IDC determined that only 41% of small companies and 35% of large organizations monitor Internet DNS response times. The majority of time devoted to DNS is spent on updating and fixing DNS problems. In addition to poor monitoring habits, companies also tend to have their DNS servers poorly distributed. In a study conducted by Men & Mice of six thousand randomly selected .com domains, 38% of tested zones were located in one subnet, increasing the risk of a single point of failure bringing down a company's name service. This can result in preventing customers from reaching a company's site.

According to the IDC study, the number of DNS name servers around the world is growing at an annual rate of close to 30% and companies recognize the impact of poor name resolution. Regardless, the relative importance placed on DNS servers within a company may not be growing as rapidly.

Key DNS Management Lessons

Whether a company is managing its own DNS infrastructure or outsourcing management to another organization, there are important guidelines to follow to ensure that DNS is designed properly and can provide robust, uninterrupted service:

Establish multiple name servers to serve zones.

This ensures that the failure of one of your name servers does not cut zones off from the Internet.

Distribute name servers geographically.

Locating name servers close to the communities of users who need them will help users access Web sites quickly and insulate them from the frequent failures of transoceanic Internet links. For example, a substantial user base in Asia could justify at least one name server in Asia.

Connect name servers to different ISP networks.

This ensures that the failure of one ISP does not cut zones off.

Provide name servers with fast, high-bandwidth connections to the Internet.

Combined with geographic diversity and the use of multiple ISPs, this would make DNS infrastructure highly resistant to a distributed denial of service attack.

Ensure that skilled DNS administrators maintain DNS infrastructure.

¹ IDC Study, March 1999

² Men & Mice Study, 2000

Inexperienced administrators can make seemingly minor configuration mistakes that have a profound and wide-ranging impact on customers.

Monitor name servers.

Monitoring only the hardware or operating system is insufficient. A company must monitor the availability and responsiveness of the name server itself. There are not many off-the-shelf tools to do this, but even the simplest monitor is beneficial.

Create a business continuity plan for DNS.

A company should consider augmenting its DNS infrastructure with additional DNS servers in additional locations.

Institute a change process.

Ensure that new name server configurations and zone data are tested before they are put into production.

VeriSign Managed DNS Services: An Overview

VeriSign understands the complexities of operating a reliable, secure, and robust DNS infrastructure and has implemented these key points in developing a DNS management product suite: VeriSign Managed DNS Services. VeriSign Managed DNS Services will offer customers the ability to outsource a part of or their entire Internet facing DNS infrastructure and operations. First two offerings within the suite are VeriSign DNS Hosting and DNS High-Availability Service.

VeriSign DNS Hosting provides customers the ability to easily and securely manage their zones through a Web-based user interface, or delegate management authority to their outsourced technical service provider, relieving staff of those administrative duties. Customer and domain name data is stored securely behind a firewall on an Oracle database. Zone data is generated from the database and transferred over a VPN to an extensive secondary name server constellation. VeriSign's server constellation receives 24x7 operational support from the same skilled operators and engineers who manage the .com, .net, and .org generic Top Level Domain (gTLD), arguably the most critical zones in the world.

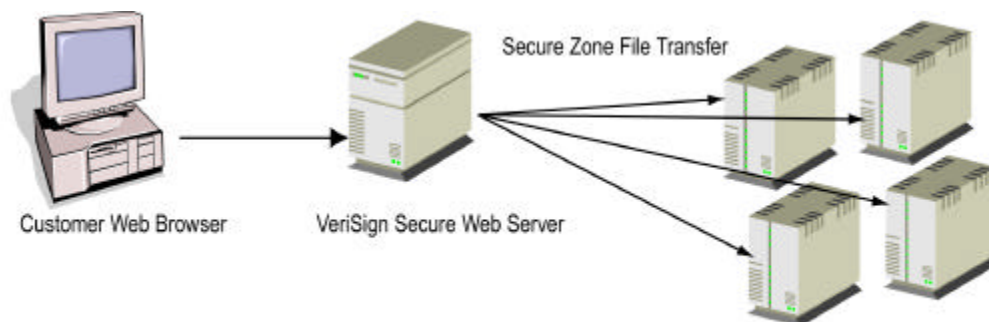


Figure 1 VeriSign DNS Hosting Service

VeriSign DNS High-Availability service offers an outsourced secondary DNS solution for companies that want to maintain control over their zone data, yet do not want to incur the added expense of implementing and supporting extensive DNS infrastructure. It allows a company's zones to be hosted on VeriSign's global name server constellation. The company retains complete control over the zone data by maintaining its own primary name server and using established tools and processes to update the zone files. VeriSign name servers take the load off a company's name server by answering all Web and email queries, providing unmatched performance, reliability, and geographical distribution.



Figure 2 VeriSign DNS High-Availability Service

The Constellation

The VeriSign gTLD sites are the heart of Secondary Name Server Hosting. VeriSign operates the thirteen gTLD name servers, which answer queries for data in the .com, .net, and .org zones. These gTLD name servers are located at the topological cores of the Internet around the world, providing local name service throughout North America, in Europe, and in Asia. This “constellation” of name servers is one of the lynchpins of the Internet's DNS infrastructure.

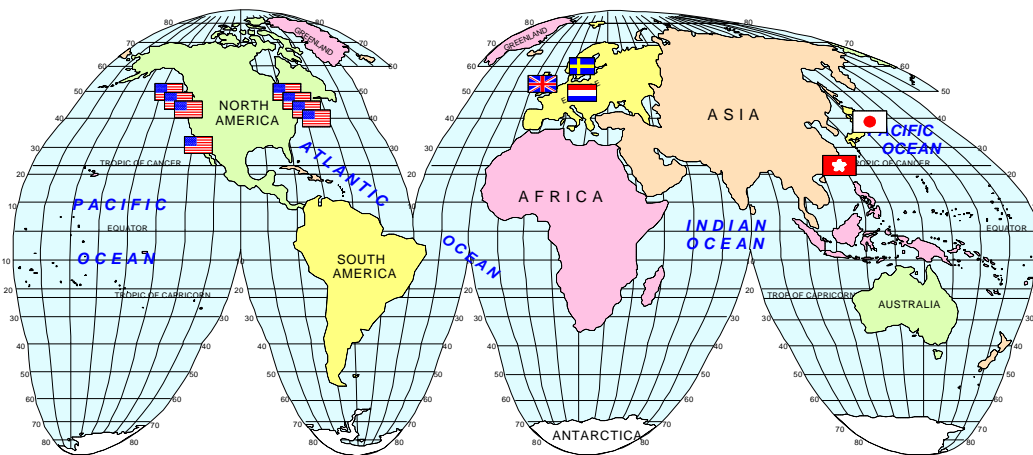


Figure 3 Global gTLD Locations

In addition to supporting the gTLD name servers, each of the VeriSign gTLD sites houses two name servers that host a company's zones. These name servers are connected to the same networks that the gTLD name servers use, and are monitored by VeriSign operations staff around the clock.

Server Platform

VeriSign hosts a company's zones on dual 1 GHz Pentium III-based servers running Linux and BSD-based operating systems. Each server is loaded with 2 GB of RAM and 36 GB of hot-swappable SCSI disks in a RAID configuration. Multiple power distribution units feed each server, which are, in turn, fed by different power sources in each data center.

Server Software

VeriSign runs special name server software tuned to the requirements of an authoritative (rather than caching) name server. With this software, the VeriSign name servers boast exceptional performance, sustaining query rates an order of magnitude greater than the performance of a standard BIND name server.

Network Connectivity

Each gTLD site has four 100 Mbps connections to the Internet. One, the primary connection, carries query and response traffic. One is used solely for management of the name servers and staging of zones. The last two provide redundant backup connections to the Internet.

In 2001, VeriSign will upgrade most gTLD sites to 1 Gbps connections.

Management

VeriSign operations staff uses Somix Technology's WebNM, Concord's eHealth Suite, and custom-built support tools to monitor and manage the name servers at the gTLD sites. VeriSign also has aggressive support contracts with all of its hardware vendors stipulating rapid response times for repair and replacement.

Security

All management of the VeriSign name servers is conducted over a virtual private network (VPN) between the VeriSign corporate network and the gTLD sites. Staging zones over an encrypted VPN connection helps ensure the integrity of zone data, while administering the name servers over the VPN helps maintain the security of the name server platforms. The use of the separate VPN connection also ensures that VeriSign operations staff is able to manage the name servers at the gTLD sites no matter how busy the name servers are answering queries.

Scalability and Availability

The name servers at the gTLD sites are designed to operate at no more than 20% of their capacity. VeriSign continuously monitors the name servers and will upgrade as necessary to ensure premium performance levels. All the components at the gTLD sites are fully redundant. This, coupled with the use of commercial Alteon load balancers to distribute incoming query load between name servers, ensures that the failure of any single component will not result in a disruption of service.

System Capabilities

VeriSign name servers support all of the latest DNS protocol enhancements, providing a company with outstanding security and flexibility.

Zone Transfers

VeriSign name servers support both old-style zone transfers (AXFR) and more efficient incremental zone transfers (IXFR). Customers running IXFR-capable primary master name servers may choose to have VeriSign name servers use incremental zone transfers to reduce load on their primary masters and to speed synchronization between authoritative name servers.

VeriSign name servers also support transaction signatures (TSIG), which cryptographically authenticate zone data transferred from a company's primary master name servers to the VeriSign name servers.

DNS Security (DNSSEC) Support

DNSSEC, the DNS Security Extensions, provide cryptographic origin authentication and integrity verification of zone data. For a company conducting electronic commerce, DNSSEC-secured zones are invaluable.

VeriSign name servers support all DNSSEC resource records. Customers still maintain absolute control over their secure zones, securing their zones on their primary master name servers. VeriSign name servers then transfer and advertise those zones.

Summary

DNS is a critical part of a company's Web presence and email system, and requires a comprehensive management strategy. Even a small improvement in DNS infrastructure can lead to increased profits through greater customer satisfaction. VeriSign Managed DNS Services provide outsourced solutions to help companies meet their on-going demands of their Web-based markets so they can focus on key business objectives. While outsourced DNS is not the right solution for every company, it is the right solution for companies that want to maximize the benefits of a well-managed DNS without incurring the significant costs of operating a DNS infrastructure in-house.