



The Domain Name System (DNS)

A Brief Overview and Management Guide

Table of

Contents

Introduction	1
What Exactly Is DNS?	2
Potential Pitfalls of DNS	4
DNS Management and Zone Hosting	5
DNS Management Do's and Don'ts	6
VeriSign's DNS Assurance Solutions	8
Learn More About DNS Assurance Solutions	10

Introduction

One of the conveniences of computer technology is that it often masks complex interactions behind a simple human experience. The Internet is a perfect example. Everyday, millions of users move from Web site to Web site by simply typing domain names (e.g., `www.verisign.com`) into a computer's Internet browser. Yet, unseen and often unknown to the user, each entry actually triggers a critical, time-sensitive process before the Web site can be accessed.

In order for Internet users to reach a Web site, their computer must find the address of the Web server that hosts the desired site. Computers locate one another across the Internet using numbers, not letters. For each Web site on the Internet there is a unique domain name and numeric address, known as an Internet Protocol (IP) address (e.g., `205.139.94.60`). This number, while quite convenient for the computer to use, is difficult for Internet users to remember; thus the need for domain names.

Each time a user enters a domain name into a computer's browser, a process translates the user-friendly name into the computer-friendly IP address needed to locate the appropriate Web server. This critical process is the primary function of the Domain Name System (DNS).

What Exactly Is DNS?

The DNS is a distributed database of information that computers use to match domain names to IP addresses. The data that makes up the Internet's DNS is propagated through a network of thousands of name servers, each responsible for pointing the users it supports in the right direction to get the information they need.

It all starts with a component called a resolver that is a part of a user's browser application. Once a domain name is keyed into the browser, a request is forwarded to the local name server.

Sometimes, the name server already knows the information needed:

User's computer: "What is the IP address of
www.verisign.com?"

Local Name server: "I know that. The IP address for
www.verisign.com is 205.139.94.60."

At other times, the name server must refer to another name server to find the answer:

User's computer: "What is the IP address of
www.verisign.com?"

Local Name server: "I do not know that. But I'll check
with a name server that does."

"DNS is the fabric that holds together today's modern Internet. It performs a basic and simple function. Yet when it breaks, no one is immune to its sting."

In such an instance, the local name server uses a process called recursive resolution. The name server will query the closest known authoritative name server for the requested IP address, which may be one of the Internet's root servers. These servers contain information about the name servers responsible, or authoritative, for every top-level domain. In this case, the top-level domain in question is .com.

Continuing our example, the root server would reply to the local name server with information about the authoritative name server:

Local name server: "What is the IP address of www.verisign.com?"

Root name server: "Here are the addresses of the authoritative name servers for .com."

The local name server then queries an authoritative .com name server:

Local name server: "What is the IP address of www.verisign.com?"

Authoritative .com name server: "Here are the addresses of the authoritative name servers for verisign.com."

Finally, the local name server queries an authoritative verisign.com name server:

Local name server: "What is the IP address of www.verisign.com?"

Authoritative verisign.com name server: "Here is the IP address for www.verisign.com: 205.139.94.60"

The local name server would then pass the IP address on to the user's computer, which could then access the Web site.

The entire process happens in milliseconds and is transparent to the end user. And because of its behind-the-scenes nature, it is a process often taken for granted . . . at least until something goes wrong.

Potential Pitfalls of DNS

DNS, as with any system, is only as good as the sum of its components. A weakness in any of the DNS components, such as hardware, software, or support staff, can render DNS inoperable and Web sites or mail servers inaccessible. Increasingly, news wires flash headlines about leading Web sites and Internet businesses suffering breakdowns that cost them money, customers, and credibility.

In truth, most internal DNS problems say little about the general Internet knowledge and ability within the walls of these companies. Rather, they highlight the very specific expertise required to adequately manage a complex DNS infrastructure.

Despite its mission-critical nature, the vast majority of major companies largely overlook careful DNS design and proper administration. Rather, they choose to focus on more highly visible Web server issues. Yet, there are myriad potential DNS problems that will render even the most robust Web server infrastructure inaccessible. Hardware problems, DNS configuration issues, denial-of-service attacks, routing problems, and software bugs can all lead to DNS failures that effectively take a company offline.

Despite the risks involved, the vast majority of companies with extensive online systems manage their own DNS. They do so because of the level of control it affords them in managing their Internet infrastructure.

A recent survey showed that over 80% of the DNS zones locally managed within .com are setup incorrectly, potentially leading to lookup problems or access problems for Web sites and E-mail.*

Domain Health Survey, conducted by Men&Mice, Nov. 2000.

DNS Management and Zone Hosting

Often, large organizations that rely heavily on the Internet to conduct business, either through e-commerce or just through communications over the Internet, benefit from maintaining control over their DNS zones. This added control assures that any changes to Web server infrastructure are reflected promptly on the Internet.

A zone is a collection of server names and associated data managed by an organization on a single set of authoritative name servers. The verisign.com zone, for example, contains the server name www.verisign.com and the corresponding IP address for this Web server. Verisign.com also contains mail routing information that applies to all email addressed to users at verisign.com.

The failure of, or even simple maintenance to, a Web server requires updating the DNS information to redirect users to another server. A delay in this DNS update would render the Web site (or sites) temporarily inaccessible. For a major e-commerce site or any business reliant upon the Internet, such a situation could be very costly.

Since it is critical to have the ability to change zone data quickly, most companies manage their own authoritative name servers. Unfortunately, few give the maintenance of these zone an appropriate level of attention or expertise.

“VeriSign now provides DNS management, by offering DNS Assurance Solutions. Companies can now supplement their DNS infrastructure with the expertise of the world’s leading Internet Infrastructure company”

DNS Management

Do's and Don'ts

Clearly, management of DNS infrastructure is far too involved to cover here. However, there are some basic rules and minimum requirements that any organization managing its own zones should be sure to have in place.

DNS should be designed and managed in order to support both physical and logical diversity. This means using multiple DNS servers that are geographically distributed and hosted on separate networks. It is critical to locate these servers on separate network segments, but they should also have separate backbone connectivity so that the failure of one Internet service provider does not take down an entire Internet presence. With geographic diversity, multiple Internet service providers, and adequate bandwidth, loss of service due to a denial of service attack or other attacks would be very unlikely. Poorly designed DNS infrastructure and inadequate management, however, is an open invitation to even an amateur attack.

Within a site there should be no single point of failure. There should be redundant systems, network devices and cabling, and Internet connectivity. Separate power sources ensure that a

Over 40% of incorrect DNS zone setups are the result of delegation errors made by the DNS administrator.*

Domain Health Survey, conducted by Men & Mice, Nov. 2000.

failure in a single power distribution unit will not bring down all the systems. Ideally, the location would have backup power generators and air conditioning units, and 24x7 support staff to respond quickly to any problems.

DNS problems are almost always time-critical. An unskilled DNS administrator working under pressure presents a real risk. Resolving DNS problems requires skilled DNS expertise. Few companies have such expertise in-house.

DNS servers operated in-house must be monitored. This monitoring should not be limited to just hardware or operating systems. The condition of the DNS services running on the server is also critical to continued performance.

A business continuity plan for DNS is a must. Companies should consider augmenting their DNS infrastructure, including adding DNS servers and additional locations if needed. This way, if servers go down, there are backups available at a moment's notice.

A change process should be established that ensures that production is not the first place a new configuration is tried.

As you can see, the risks and resources involved in DNS management are by no means minor. Though good DNS management can be complicated, it is also critical to the effective operations of an Internet-reliant business. Unfortunately, few realize there are faults in their DNS infrastructure until it is too late - by that time they may have lost thousands even millions of dollars in business, not to mention the loss of customers from interrupted service.



VeriSign's DNS Assurance Solutions

As you can see, managing a zone and its authoritative name servers requires time, money and expertise. Navigating the subtle syntax of zone data files and name server configuration requires an administrator with substantial training and experience.

To ensure robustness, a zone should be served by name servers on different networks. To provide optimal performance, a zone's name servers should be distributed throughout the Internet, as close to users and hosts as possible. But the cost of placing servers in multiple, strategic locations and the burden of operating them is prohibitive to most organizations.

For over nine years, VeriSign has managed the .com and .net zones. These are the most mission-critical top-level zones in the world, comprising over 28 million domains names.

VeriSign's DNS Assurance Solutions offers a complete, primary and secondary DNS solution. Using VeriSign's DNS Assurance Solutions a customer's zone is hosted on name servers located at VeriSign's gTLD (generic top-level domain) name server locations around the world. The customer retains complete control over the zone data, editing it through an easy-to-use Web interface called DNS Manager. VeriSign's name servers then answer all queries for data in the zone, providing unmatched performance and geographical distribution.

Learn More About

DNS Assurance Solutions

Every modern business relies on the Internet in some capacity. Many would cease to function without it. Yet, despite this enormous dependency, the DNS, a critical component of operability, remains an often overlooked aspect of a business Internet system.

Beyond the threat of loss of Internet operations, enhanced DNS capabilities also hold the promise of an improved Internet experience for businesses and customers alike.

We encourage you to consider the benefits of enhancing your company's DNS infrastructure. And when you do, we invite you to learn more about VeriSign DNS Assurance Solutions by visiting our Web site, www.verisign.com.

VeriSign, the leader in Internet Infrastructure, is now offering DNS Assurance Solutions to help your organization fortify your critical DNS infrastructure.



21345 Ridgetop Circle • Dulles, Virginia 20166
703.948.3200
www.verisign.com

© 2001, VeriSign, Inc. All rights reserved.
The VeriSign logo is a trademark of VeriSign, Inc.