Don’t Overlook DNS Management When Protecting Your Website Against Downtime and Attacks

Call it the paradox of infrastructure: a steady progression from the sublime to the mundane. Regardless of the era, from the electric grid and telephone system to GPS and the Internet, infrastructure that was once universally hailed as magical and transformative soon becomes routine and boring.

Nothing exemplifies this phenomenon better than the plumbing undergirding the Internet and all the apps and services relying upon it. Few people think about, much less understand, the routers, fiber links, and software protocols required to deliver content to their smartphones, until they fail. As the Net’s 411 directory assistance system, DNS is one of those oft-unappreciated yet critical components that allows people to work with readable website names and application architects to build seamless redundancy and scalability into their systems.

DNS problems can befall even the largest, most technically savvy organizations, as Google found out when its public DNS server went offline two years ago. Of course, DNS is a mature and highly redundant protocol, so total blackouts such as Google’s are rare outside of malicious hacking or distributed denial-of-service attacks designed to take down a site. More common are DNS-related performance problems caused by overloaded
servers and poorly designed implementations that don’t exploit the protocol’s inherent reliability and security features like replication, failover, caching, forwarding, and namespace/service separation.

For most network applications, the typical problem is DNS-related performance bottlenecks. A browser or mobile app can’t run code or display information from a remote site until it knows where that code or information is. That means DNS query performance — translating names and network protocols into addresses and ports — directly affects the user experience. Yet there can be surprisingly wide variability in query response across geographic regions and DNS providers. CloudHarmony has software and network probes that measure the performance of various network services, including DNS queries. Over a recent one-month period, its system of more than 6,500 monitoring sites illustrated the inconsistent landscape of DNS performance. For example, in the U.S. East region, there was almost a 2-to-1 difference between the fastest and slowest services. Similar spreads were the norm for other regions.

The problem with poor DNS performance is that it’s not just a one-time hit. Today’s network applications and websites make dozens of calls to other systems for things like style sheets, images, boilerplate headers, and traffic monitoring beacons, each requiring a DNS lookup. For example, an analysis of InformationWeek’s home page showed more than 200 requests for various objects — images, scripts, HTML, CSS — with 38 percent of the total load time spent on DNS. Another analysis of the same site showed more than 60 separate DNS lookups, with several to external partner sites taking more than 100 milliseconds to complete.

Enterprise DNS Options

Given the importance of DNS to public-facing website performance and its consequent effect on customer satisfaction, company image, and online sales revenue, we wanted to understand how enterprises manage DNS. To do this, we surveyed IT and business professionals with public, business-critical websites who are personally involved in the purchase, implementation, or management of DNS or DNS services at their organizations constitute the final data set.

Most of the 263 respondents still use in-house servers, although a sizeable share let their Web hosting providers manage DNS. The share of respondents using a managed DNS provider (22%) hasn’t changed much over the years, indicating that many people probably don’t understand the full range of critical services cloud providers have to offer in this area.

Methodology

In April 2015 UBM Tech conducted an online survey on behalf of Neustar exploring how organizations manage Web traffic to ensure availability and uptime.

A total of 263 business technology professionals at companies with business-critical public websites who are personally involved in the purchase, implementation, and/or management of DNS or DNS services at their organizations constitute the final data set.

Respondents were from small, medium, and large companies, with more than 40 percent working at companies with 1,000 or more employees. About half of respondents held job titles of director level or above, and various vertical industries were represented.

The greatest possible margin of error for the total respondent base (N=263) is +/- 6 percentage points. UBM Tech was responsible for all programming and data analysis. These procedures were carried out in strict accordance with standard market research practices.
Our results are undoubtedly skewed by the fact that only 42 percent of respondents hailed from companies with 1,000 or more employees, whereas managed DNS caters to large enterprises and top-500 Internet retailers, like this list from Alexa, with critical traffic sites. These businesses clearly have the most to lose if their websites go dark, making DNS performance a higher priority.

State of Enterprise DNS: Not Too Dynamic

Our survey is a good barometer for the state of enterprise DNS operations and shows that the environments aren’t exactly dynamic. Most respondents have few people dedicated to DNS. Nearly half (48%) devote less than one full-time equivalent to DNS management; just 20 percent devote more than three people. For most respondents, DNS is clearly a “set it and forget it” system, albeit one that would quickly escalate into an all-hands fire drill should anything fail.

DNS is easy to ignore for smaller organizations with infrequent changes. Indeed, our survey found that 55 percent of respondents make changes no more than quarterly, but for the rest, especially those with online commerce sites, traffic management services are appropriate and valuable. Although we found that more than three-quarters (78%) of respondents are aware of such services, only 8 percent use them. The primary reasons nonusers give for not using third-party DNS services are that they aren’t aware of the benefits (31%) or don’t see ROI for their business (31%).

Forty-four percent of respondents use some form of advanced traffic routing like geolocation targeting or global load balancing to complement...
DNS, a figure nearly identical to the percentage of respondents from large enterprises, and we think there’s a correlation. The larger, more advanced, and more distributed your infrastructure, the more likely you’ll need to intelligently route customer traffic to the closest or fastest website.

Importance of DNS to Online Operations

By now, we hope it’s clear how critical DNS is to online operations: Lose it and you’re suddenly offline, losing business, and tarnishing your company’s image. However, DNS has evolved into much more than a simple address lookup system. For all but the smallest organizations, DNS management isn’t just about editing a static directory of host names; instead, managed services have evolved to include features that improve site performance, availability, disaster preparedness, and prevention.

Indeed, DNS is a critical part of disaster planning and mitigation as it provides the ability to transparently move customers from one location to another. For example, during Hurricane Sandy, most news organizations and banking operations suffered minimal to no downtime even though they had primary data centers in the eye of the storm. DNS-based traffic management transparently redirected users to

Figure 3. Are you aware of and/or have you investigated DNS-based traffic management services?

- Not aware of third-party traffic management services (29%)
- Aware of, but never considered (22%)
- Have considered, but don’t use (41%)
- Currently use third-party traffic management services for hosted sites (8%)

DATA: UBM survey of 263 IT and business professionals responsible for DNS or DNS services at organizations that operate a business-critical public website, April 2015

Figure 4. Why did you decide not to use a third-party DNS and traffic management service?

- Didn’t see significant benefits to our business (31%)
- Couldn’t justify service versus costs (31%)
- Budget wouldn’t allow incremental spending on external IT services (11%)
- Security concerns (10%)
- Cloud and/or managed service provider does DNS and traffic management; no need for self-managed sites (8%)
- Didn’t understand the service details (5%)
- Other (4%)

BASE: 184 who do not use DNS and traffic management services
DATA: UBM survey of 263 IT and business professionals responsible for DNS or DNS services at organizations that operate a business-critical public website, April 2015
alternative locations unaffected by the disaster.

Basic features of managed DNS services include improved directory availability, query performance and scalability, site security and DDoS protection, central management, and traffic reports. These features can be useful whether you have just a few large sites or dozens of globally distributed locations. Although the top vendors have redundant nodes throughout the world and can scale to meet the largest traffic loads, as we saw above,

---

**State of Enterprise Traffic Management**

Our survey examined the methods IT uses to ensure site uptime and found that although most organizations stick with the basics, 41 percent have managed to eliminate downtime incidents in the past year.

- Most respondents use simple methods to improve site availability. Thirty percent just have inactive standby servers, while another 23 percent have active-active redundancy, but only within a single location.
- Nevertheless, you can’t argue with success since most organizations have few DNS-related outages: 86 percent had two or fewer downtime incidents in the past year.
- However, dependence on a single site is risky. Of those who have experienced website downtime, 57 percent reported it was caused by a site outage, with another 35 percent citing inadequate performance due to traffic load (see Figure 7, p. 7).

---

**Figure 5. What features are most important when managing Web traffic?**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Important</th>
<th>Neutral</th>
<th>Not Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service availability or uptime</td>
<td>93%</td>
<td>5%</td>
<td>2%</td>
</tr>
<tr>
<td>Service performance or response time</td>
<td>89%</td>
<td>8%</td>
<td>3%</td>
</tr>
<tr>
<td>Automated site failover</td>
<td>66%</td>
<td>24%</td>
<td>10%</td>
</tr>
<tr>
<td>Ease of use</td>
<td>58%</td>
<td>29%</td>
<td>13%</td>
</tr>
<tr>
<td>Monitoring and reporting</td>
<td>53%</td>
<td>35%</td>
<td>12%</td>
</tr>
<tr>
<td>Global load balancing</td>
<td>38%</td>
<td>25%</td>
<td>37%</td>
</tr>
<tr>
<td>Geolocation-based traffic routing</td>
<td>31%</td>
<td>28%</td>
<td>41%</td>
</tr>
</tbody>
</table>

**DATA:** UBM survey of 263 IT and business professionals responsible for DNS or DNS services at organizations that operate a business-critical public website, April 2015
there are still large performance differences among them that can vary among regions. Thus, buyers must balance feature sets with infrastructure and corresponding performance results that best match the locations of their online infrastructure and customers.

Traffic management services augment core DNS functionality with features like site monitoring and failover, geolocation-based routing, and traffic-weighted load balancing for mission-critical, globally distributed sites. These are particularly important for seasonally variable or event-driven workloads that can cause traffic bottlenecks.

Consider, for example, last summer’s World Cup-fueled record Twitter and Facebook activity during the final match, with traffic at news sites such as ESPN, BBC, and Eurosport reaching 300 percent above normal. Furthermore, one analysis found that the games shifted peak traffic from prime evening hours to game times. Although the World Cup’s traffic ramifications were extreme in scale, similar episodic changes occur with most large public websites, and such traffic variability would be impossible to manage without advanced DNS traffic services.

Features Enterprise Users Most Value

It’s no surprise that respondents to our survey tagged reliability and uptime, resilience and site failover, performance, and security as the most valued DNS traffic features.

Figure 6. **When thinking about using a DNS management service versus in-house DNS operations, what attributes would be most important in your decision?**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Important</th>
<th>Neutral</th>
<th>Not Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>89%</td>
<td>9%</td>
<td>2%</td>
</tr>
<tr>
<td>Website or application availability or uptime</td>
<td>86%</td>
<td>12%</td>
<td>2%</td>
</tr>
<tr>
<td>Website or application performance</td>
<td>84%</td>
<td>13%</td>
<td>3%</td>
</tr>
<tr>
<td>Cost</td>
<td>75%</td>
<td>19%</td>
<td>6%</td>
</tr>
<tr>
<td>Admin console features or ease of use</td>
<td>61%</td>
<td>29%</td>
<td>10%</td>
</tr>
<tr>
<td>Optional add-on features (e.g., load balancing, DDoS mitigation)</td>
<td>51%</td>
<td>27%</td>
<td>22%</td>
</tr>
</tbody>
</table>

**DATA:** UBM survey of 263 IT and business professionals responsible for DNS or DNS services at organizations that operate a business-critical public website, April 2015
management features. There’s always some grade inflation on questions like this since we didn’t force respondents to rank choices; however, the ordinal rankings of highly rated features are significant, and these show that service availability, uptime, and performance trump all other traffic management bells and whistles. It doesn’t matter how nice the management dashboard and report charts are if a DNS service is slow and unreliable.

We also wanted to understand those attributes respondents find most influential when evaluating and comparing managed DNS services against in-house operations. Again, website availability and performance are important, but security topped the list. This isn’t unexpected since security emerges as a key concern whenever IT pros are asked about outsourcing or cloud services. Yet this concern also presents an opportunity for those DNS service providers that can demonstrate security technology, processes, and auditable results that are as good as or better than those in the typical enterprise. For example, few enterprises can match the best-managed DNS vendors when it comes to DDoS mitigation processes, support for DNS Security Extensions (DNSSEC), or two-factor authentication of DNS administrators.

Although our respondents didn’t highly value advanced traffic management features, we suspect this is primarily due to a lack of information or education about the specific features and their benefits. The data also is skewed by the survey demographics, since smaller organizations with one or two data centers and office locations or a regional customer base may not be as aware as larger organizations of the need for globally distributed load balancing. However, we contend that once an organization goes from one to two data centers, it must have some method for managing traffic to those data centers. DNS is by far the best and easiest way to accomplish that traffic distribution. Smaller companies, in fact, may be employing very simple round-robin DNS traffic management without even realizing it.

**Service availability, uptime, and performance trump all other traffic management bells and whistles for users.**

---

**Figure 7. Of the following website downtime problems, which have you experienced in the past year?**

<table>
<thead>
<tr>
<th>Problem</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outage due to site downtime</td>
<td>57%</td>
</tr>
<tr>
<td>Outage due to single server downtime</td>
<td>39%</td>
</tr>
<tr>
<td>Inadequate performance due to traffic load</td>
<td>35%</td>
</tr>
<tr>
<td>Inadequate performance due to users in other regions</td>
<td>16%</td>
</tr>
</tbody>
</table>

**NOTE:** Multiple responses allowed  
**BASE:** 176 respondents who have experienced website downtime  
**DATA:** UBM survey of 263 IT and business professionals responsible for DNS or DNS services at organizations that operate a business-critical public website, April 2015

---

**Traffic Management 101**

It’s hard to say you need something when you don’t exactly know what it does. We suspect many more enterprises would find advanced site traffic management valuable and cost effective than our survey numbers suggest if they had a full understanding of the capabilities. The following is a summary of key DNS features:
• **Monitoring and failover:** The most basic DNS add-on, monitoring services continually check site or server availability and failover to a backup server, data center, content delivery network, or cloud service provider. The services automatically restore traffic routes to the primary host or site when it comes back online.

• **Global server load balancing:** Simple server load balancing resembles DNS failover. However, there are no active and failover hosts; instead, all hosts distribute traffic equally (round robin) or through weighted distributions (usually an add-on service). Health checks help to monitor each server via timed intervals, and if a health check fails, the load balancer can remove it from the pool while still distributing queries to active servers, ensuring continued website availability.

• **Location-based (geo-IP) routing:** Location-based DNS varies the query response according to a user’s location as approximated by the public IP address. This reduces latency and information relevancy for globally distributed sites by sending users to the closest resource. Location detection and response customization can be quite granular, down to the state, allowing hyperlocal apps, such as local shopping or coupon sites, to send users to the subsite with geographically tailored information.

Although all major managed DNS operators offer some mix of traffic management services, they are usually optional items and are often bundled in higher-cost product tiers. Shoppers should carefully review services offered to ensure that they get the ones they need for a reasonable price.

**Benefits of DNS and Traffic Management-as-a-Service**

Enterprises today have several options when deciding how

---

**7 Must-Have Features for Managed DNS**

Here’s a list of features to look for when selecting a managed DNS provider. Use it to find the right service for you — one that reduces costs and DNS management time while improving performance, availability, and online security.

1. **Availability/reliability:** 100 percent network uptime is the SLA you want. If customers can’t reach your website, they’re not your customers. Insist on highly redundant nodes.
2. **Security:** Non-open source resolvers are less prone to malware, viruses, and phishing. Insist on a provider with built-in DDoS protection, as well as failover to a DDoS protection network. Plus, support for DNS Security Extensions (DNSSEC) guards against cache poisoning and pharming attacks.
3. **Performance:** Fast query resolutions are essential, yes. But also make sure your provider minimizes dropped requests.
4. **Scalability/global network:** More points of global presence mean much faster service for queries bound for servers in Shanghai, Bonn, or Boston. It’s key to sustained growth.
5. **Precision traffic management:** Simple traffic routing services for monitored load balancing and failover are a must for everyone. To further optimize traffic, seek out advanced services that provide the flexibility to direct and customize network traffic for enhanced performance without the need for costly hardware investments.
6. **Ease of use:** A sophisticated platform doesn’t help if it’s hard to use. Be sure you like the portal. It should be simple to access, let you make changes easily, and deliver clear, useful reporting.
7. **Expertise and support:** A simpler word for these is reputation. How long has Provider A been managing DNS? How deep is its expertise, both in technical knowledge and customer support? It pays to check with peers and evaluate their experiences.
to manage their DNS needs: in-house, through their ISPs or hosting providers, or through a managed service provider.

**In-house:** When enterprises manage DNS in-house, it is often with limited expertise and resources. Based on our survey results, a full 41 percent of organizations that managed DNS in-house devote less than one full-time employee to DNS management. What happens when a critical outage occurs? Businesses also tend to lack the network, capacity, and redundancy they need to ensure the uptime and availability necessary when websites are such a critical part of the business. Among the vulnerabilities that increase significantly when DNS is managed in-house are performance, security, and potential outages.

**ISPs:** ISPs relieve some of the issues associated with in-house DNS management, as they tend to have extensive global infrastructures. However, DNS management is not the core function of an ISP, and investments in new features, functionality, and overall improvements will never be an ISP’s top priority. In addition, increased usage of an ISP’s network can lead to congestion and latency issues that tend to impact DNS performance.

---

**Figure 8. Which of your application or workload types are most affected by DNS and address-related traffic services?**

<table>
<thead>
<tr>
<th>Application Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>General business websites</td>
<td>67%</td>
</tr>
<tr>
<td>Business-to-business applications and processes</td>
<td>33%</td>
</tr>
<tr>
<td>Online commerce sites</td>
<td>32%</td>
</tr>
<tr>
<td>Specific marketing and promotions sites</td>
<td>17%</td>
</tr>
<tr>
<td>Location-specific sites</td>
<td>16%</td>
</tr>
</tbody>
</table>

**NOTE:** Multiple responses allowed  
**DATA:** UBM survey of 263 IT and business professionals responsible for DNS or DNS services at organizations that operate a business-critical public website, April 2015

---

**Figure 9. Of the following consequences associated with website downtime, which are of highest concern to your organization?**

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poor customer experience</td>
<td>59%</td>
</tr>
<tr>
<td>Damage to brand reputation</td>
<td>42%</td>
</tr>
<tr>
<td>Loss of productivity</td>
<td>29%</td>
</tr>
<tr>
<td>Increased operational costs (e.g., time spent to resolve issues)</td>
<td>21%</td>
</tr>
<tr>
<td>Loss of revenue</td>
<td>20%</td>
</tr>
</tbody>
</table>

**NOTE:** Maximum of two responses allowed  
**DATA:** UBM survey of 263 IT and business professionals responsible for DNS or DNS services at organizations that operate a business-critical public website, April 2015
Managed service providers: Managed service provider use has continued to increase year over year, but there is still a great opportunity to educate the market on the benefits of outsourcing DNS management. Companies whose websites and online infrastructure are critical to their business should use managed DNS services to eliminate infrastructure costs, reduce management time, improve website performance and reliability, and minimize DNS security vulnerabilities. Due to the mission-critical nature of DNS, most of the world’s largest enterprises and top websites outsource it to managed service providers that have an extensive infrastructure, a reliable network, more expertise, and additional service offerings for advanced support. However, organizations of all sizes should consider managed DNS. Pricing structures tend to be based on usage, so costs can vary based on need — which is a good thing. Managed service providers offer the security, reliability, and performance needed at a cost that is inconsequential when compared to the actual losses incurred when a website is down. Other benefits of managed service providers include:

- Increased performance via distributed, intelligently routed infrastructure (IP Anycast)
- Availability of advanced options like traffic management
- Well-defined service-level agreements
- Enhanced DNS security
- 24/7 service and support
- Added redundancy with no single point of failure
- Scalability

The Neustar Advantage

Neustar UltraDNS provides a secure, managed DNS service to help businesses enable and protect their online infrastructure, ensuring 100 percent website availability and peak performance with built-in security for superior protection.

Availability: Backed by a powerful global directory platform and a highly redundant network of 30 nodes on six continents, Neustar’s extensive global infrastructure provides a 100 percent network availability SLA.

Security: UltraDNS provides comprehensive protection from DNS-based DDoS attacks with Neustar’s cloud-based scrubbing network. Neustar’s non-open source platform is less vulnerable to hijacking, spoofing, and viruses. DNSSEC support helps combat phishing, and name server segmentation further isolates you from threats.

Performance: Neustar’s global Border Gateway Protocol and IP Anycast network manages over 25 billion queries per day with fast, accurate responses and the fewest dropped queries.

Advanced traffic management: Neustar’s advanced traffic management capabilities help to further optimize DNS traffic.

SiteBacker monitors and enables automatic failover of DNS traffic in the event of underperforming or unavailable servers. It provides a variety of monitoring capabilities with customized support and changes propagated globally in near real time.

Traffic Controller controls and optimizes traffic and network performance at the DNS level. It supports both weighted load balancing as well as the traditional round-robin approach, and probe monitoring ensures that resources reaching critical thresholds or becoming unavailable are pulled from the load balancing pool.

Directional DNS sends visitors to specific servers based on their geographic location in order to deliver geographically specific content and images to your end users, improving site performance and the end-user experience. Neustar UltraDNS now supports the EDNS client-subnet to generate more geographically accurate responses for the end user.

Availability:

Backed by a powerful global directory platform and a highly redundant network of 30 nodes on six continents, Neustar’s extensive global infrastructure provides a 100 percent network availability SLA.

Security:

UltraDNS provides comprehensive protection from DNS-based DDoS attacks with Neustar’s cloud-based scrubbing network. Neustar’s non-open source platform is less vulnerable to hijacking, spoofing, and viruses. DNSSEC support helps combat phishing, and name server segmentation further isolates you from threats.

Performance:

Neustar’s global Border Gateway Protocol and IP Anycast network manages over 25 billion queries per day with fast, accurate responses and the fewest dropped queries.

Advanced traffic management:

SiteBacker monitors and enables automatic failover of DNS traffic in the event of underperforming or unavailable servers. It provides a variety of monitoring capabilities with customized support and changes propagated globally in near real time.

Traffic Controller controls and optimizes traffic and network performance at the DNS level. It supports both weighted load balancing as well as the traditional round-robin approach, and probe monitoring ensures that resources reaching critical thresholds or becoming unavailable are pulled from the load balancing pool.

Directional DNS sends visitors to specific servers based on their geographic location in order to deliver geographically specific content and images to your end users, improving site performance and the end-user experience. Neustar UltraDNS now supports the EDNS client-subnet to generate more geographically accurate responses for the end user.
Continued investments in infrastructure and service offerings

Our survey results show the demonstrable business benefits of improved DNS and traffic management. A third (33%) of respondents said DNS or traffic-related problems caused downtime for business-to-business applications and processes, while a like number (32%) reported outages for e-commerce sites.

Anytime the sites customers and business partners use to buy products and complete business processes are down, it costs money. However, direct costs are just the start. Fifty-nine percent of respondents said their biggest concern over site downtime is leaving customers with a poor experience, while 42 percent cited damage to their organization’s brand and reputation. Thus, if downtime isn’t costing you current revenue, it’s likely to cost future business, besides the lost employee productivity.

Most large organizations are better off leaving DNS and traffic management operations for public-facing sites to others.

Considerations and Recommendations

DNS and associated traffic management services are the sort of low-level Internet plumbing that’s easy to ignore. However, as many businesses have found out the hard way, they can have significant ramifications on the bottom line and customer experience. All businesses should carefully review how they manage DNS and evaluate its implications to critical business processes, online sales, customer satisfaction, and company image.

When analyzing the total costs and benefits, we believe most large organizations are better off leaving DNS and traffic management operations for public-facing sites to others. Companies should pay close attention to advanced traffic management services that provide levels of performance and reliability beyond what is typically available from self-operated systems. Small and medium enterprises should strongly consider outsourcing entire website operations to a service provider that includes DNS management (typically sourced through a DNS specialist) as part of a comprehensive suite of website design, management, and deployment services.

Neustar Inc. (NYSE:NSR) is the first real-time provider of cloud-based information services and data analytics, enabling marketing and IT security professionals to promote and protect their businesses. With a commitment to privacy and neutrality, Neustar operates complex data registries and uses its expertise to deliver actionable, data-driven insights that help clients make high-value business decisions in real time, one customer interaction at a time. More information is available at www.neustar.biz.