THE UTILITY OF DNS TRAFFIC MANAGEMENT
About DNS

The domain name system, or DNS, is a protocol that translates user understandable names (like domain names – for example, .co, .biz, .au) and labels (like website addresses – for example, www.neustar.biz) into IP addresses that are understood and accepted by computers and routers to move and direct packets around the Internet.

As the first step in almost every transaction on the Internet, DNS is well positioned to deliver traffic management capabilities, or to redirect traffic on the Internet based on conditions other than the standard routing protocols. But not every company is maximizing their DNS’ potential.

With more than three billion people now1 accessing the Internet, there’s a true tension between managing website traffic, delivering a consistent user experience, and securing web applications. Failure to properly align these priorities could negatively affect website availability and cause irreparable brand damage.
DNS Traffic Management

So What's A Business To Do?

Since a flawless website experience is a must, some organizations are relying on multi-vendor hosting and/or delivery solutions – cloud delivery networks (CDN) or cloud computing services – to balance incoming traffic requests. Whether on-premise or in the cloud, these solutions can be helpful — and expensive. It's no surprise that higher performance usually comes at a higher cost. Also, essential tasks like moving from degraded servers to ones that are functioning properly heavily depend on budget, time and availability.

Seeking to balance efficiency with finances, companies often use an array of cloud vendors in different regions of the world, exponentially increasing user demand and traffic. In one region, a less expensive provider with adequate performance may suffice, while in another region of the world, superior service - despite the premium cost - may be necessary.

In other words, it can get complicated. Good thing there's a built-in way for you to complement your current traffic management solutions, keep a close eye on global traffic, deliver a consistent user experience, and even strengthen security. The answer consists of three letters: DNS.

Nobody likes to wait. Whether it’s at a theme park or on the Internet.

DNS traffic management strategies and tools optimally direct user traffic to the correct destination, which can be defined by geographic location, Internet location, server availability, or traffic distribution. DNS also involves the re-routing of traffic when networks or servers require maintenance or incur incidents, making service unavailable. Traffic management helps to ensure websites and applications are always available and working at peak performance.

DNS queries can provide a lot of information about a user before their browser even connects to your website. From the user’s geographic region and internet service provider (ISP), down to the specific location when their provider supports advanced DNS features, you can learn a lot about a user based on the DNS query.

Combining information on the performance and availability of your server resources allows you to make intelligent decisions about how you want to direct traffic and deliver the best user experience.

TO THE CLOUD!

Opting for cloud-based DNS traffic management is less expensive than maintaining on-site hardware, and it’s easier to update. Cloud DNS also offers advanced traffic management capabilities that result in cost-savings, improved scalability, and better performance and managed security over a wider footprint.
Monitoring and Failover

When Downtime is NOT an Option

Congratulations! Your marketing team did a fantastic job of driving traffic to your website, but do you know how much load the network can support? Is there a contingency plan just in case one of your servers goes down? One of the core tenets of having a website is ensuring its availability. Guessing won’t suffice; you need proactive monitoring and standby services to ensure high availability and exceptional response time to provide a good user experience.

Proactive monitoring leverages probes to test the availability and performance of the applications. Based on the results, you can now decide how to best redirect and manage traffic to the application.

Standby or failover refers to the ability to seamlessly direct user sessions to an alternative, standby or redundant application instance when the primary server has failed or has been taken out of service. Failover can also allow you to direct traffic to another server in the event of an emergency, such as when your primary network is undergoing routine maintenance, or if you’re being hit with a distributed denial of service (DDoS) attack.

By delivering monitoring and failover services at the DNS level, you now have added availability. A plan B is a beautiful thing.
Traffic Management Monitoring Probes

Traffic management services may use multiple types of probes to verify that servers and applications are reachable from several locations. This information is then used to determine which resources to announce via DNS, enabling automatic failover between primary and standby resources. It also enables intelligent load balancing among multiple active resources.

The available probes range from very simple (PING) to more complex transaction based probes (HTTP/HTTPS).

**PING Probe**
PING is the simplest and most commonly used probe. It sends an ICMP packet and measures whether a server is reachable in a defined timeframe. Although the PING probe is frequently used, it is the least reliable indicator of system availability.

**DNS Probe**
DNS probes are used when an organization is layering cloud-based traffic management services with hardware load balancers that they have deployed. A probe is sent to the hardware load balancer, where it searches for a valid DNS reply. The probe allows for traffic management configurations, which leverage multiple deployments of load balancing hardware, to fail between or distribute traffic amongst them.

**FTP Probe**
This is used by organizations that maintain file transfer protocol (FTP) servers to allow the distribution of files. The FTP probe verifies an FTP service by logging into an FTP session.

**SMTP Availability Probe**
The SMTP probes verify that a mail server is reachable and active.

**TCP Probe**
TCP probes attempt to connect to a specified TCP port. TCP probes are used by organizations that wish to test the availability of applications that are not using HTTP/HTTPS and are using non-standard TCP ports. This probe verifies that the specified port is reachable.

**HTTP/HTTPS Probe**
The HTTP probe is the most common probe used in traffic management services. It verifies an HTTP service by making a request to a web server and testing the response. A correct response can be as simple as a valid HTTP response code, but typically these services are configured to look for a specific page on the host and search for a specific string of text. In doing so, the service verifies not only that the server is available, but that the web application is up and responding. Many services also provide the capability to build multi-step transactions using a series of HTTP(S) GETs and POSTs. This is the most robust traffic management probe and, as such, it is the most utilized.
Global Load Balancing and Traffic Distribution Methods

Investing in redundancy is an excellent step towards ensuring a constant website presence, but it doesn’t guarantee the maximum use of all of your server resources. If your website suddenly receives a surge in traffic, some users could experience sluggish wait times - if they can even reach your site.

To guard against this potentially brand-damaging event, DNS offers the ability to load balance incoming traffic. With load balancing, you now have several ways to direct and distribute traffic across multiple servers, ensuring optimal website performance and minimizing the risk of downtime.

Some of the different approaches to DNS load balancing:

**Priority Hunt**
Directs traffic to a specified sequence of servers and returns to the top of the prioritized hunt list to select the first available server when the current server is unavailable.

**Random**
Traffic is distributed randomly between destinations.

**Round Robin**
Spreads traffic between the probe results of multiple configured servers.

**Weighted Load Balancing**
Traffic is managed based on a specified percentage that is sent to each server. Whether the ratio is 50:50 or 70:30, weighted load balancing allows you to distribute traffic based on the characteristics of each application server.

**TIP:** Weighted load balancing allows you to take control of your website’s performance. Since you have the ability to manage the traffic routed to each server, it allows for proper allocation resource and a flawless website experience.
The Utility of DNS Traffic Management

GLOBAL LOAD BALANCING

<table>
<thead>
<tr>
<th>TRAFFIC DISTRIBUTION METHOD</th>
<th>ACTION UPON FAILURE</th>
<th>TRAFFIC DISTRIBUTION FOR SERVERS A, B, C, D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weighted</td>
<td>Next available server based on load</td>
<td>A: 40%; B: 60%</td>
</tr>
<tr>
<td>Round Robin</td>
<td>Next server in list</td>
<td>ABCD; ABCD; ABCD</td>
</tr>
<tr>
<td>Random</td>
<td>Next random server</td>
<td>D, A, C, D, B, B, A, C</td>
</tr>
<tr>
<td>Priority Hunt</td>
<td>Next available server in list, starting from top/priority on the list</td>
<td>A, B, C, D</td>
</tr>
</tbody>
</table>

*A is the priority*
Origin-Based Routing

Origin-based routing allows you to see where a user is accessing your website—be it geographical or network—and route them to the appropriate resource to deliver maximum performance and/or tailored content. From the time they connect to the Internet, every user has an assigned IP address that can be viewed and analyzed. But not every DNS provider has quality IP intelligence data and the ability to set rules to provide an appropriate level of routing. Accurate IP intelligence is crucial if you have regional restrictions or offers.

Not only is authentic IP intelligence a great way to serve your clients, it also allows you to identify and guard against security threats at the country, region and state level. As cyber attacks continue to cross borders and territories, authentic IP intelligence allows you to block access to your site based on the origin of the IP. And with proper traffic management that updates its IP intelligence files on a daily basis, you can proactively identify and stymie breaches before they occur.

**BUT:** Not all IP intelligence solutions are created equal. Top-tier solutions continuously cleanse and append their data to provide accuracy and detail down to the state level for every country in the world.

**TIP:** Support for EDNS0-Client-Subnet improves routing accuracy by identifying the geo-location of end users, enabling faster response times.
Combining Capabilities for Improved Performance

88% of consumers distrust a brand if the website is off-line and unavailable
Source: Ponemon Institute/Neustar Study: What Erodes Trust in Digital Brands

As the old adage goes, you never get a second chance to make a first impression. In this always-on and interconnected world, the Internet never sleeps. If your website is slow, unresponsive or down, it can quickly lead to skeptical customers, missed sales opportunities and brand damage.

But that doesn’t have to happen.

You can achieve maximum website performance by combining traffic management services through a cloud-based managed DNS service that provides added flexibility and customized solutions for business applications. By using a solution that combines traffic distribution, monitoring and failover, load balancing, and origin-based routing, you can feel confident that you have the best assurance for website availability that is capable of providing a flawless customer experience.

And much like a cell phone or radio tower, DNS is best served from the nearest, highest performing delivery node. As website traffic increases, it is important to have a scalable cloud and managed DNS service that is capable of improving performance and providing a seamless user experience.

**Key Takeaways:** Most organizations do not understand nor realize the full set of capabilities that DNS can provide.

By leveraging the benefits of DNS-based traffic management, you can:

- Increase redundancy via monitoring and failover
- Implement global load balancing to distribute global traffic more efficiently
- Optimize performance and improve end-user experience
- Prevent costly downtime
- Support disaster recovery and business continuity plans
- Protect your infrastructure from cyber attacks
- Obtain user location information
- Reduce and cap operation costs (no hardware required!)

More than just a way to connect users to a website, DNS offers dynamic traffic management capabilities that can augment existing services, and in some cases, save money and time. If properly utilized, DNS can dramatically transform the website and user experience for you as well as your customers.
Neustar UltraDNS is a cloud-based, authoritative managed DNS service that helps businesses with critical online infrastructure connect and stay connected to the internet—ensuring better website availability, improved security, and faster performance for their users. To further increase website reliability and performance and ensure a flawless end-user experience, Neustar UltraDNS offers Advanced Traffic Management services. With 24/7 support and over 16 years of industry experience, Neustar fully manages your DNS so you can focus on other core initiatives.

Learn more at [neustar.biz/dns](http://neustar.biz/dns)

Endnotes

1. InternetLiveStats.com