

High Availability DNS Reduces Downtime Risk and Improves End-User Experience

How Redundant DNS Services Provide Resilience and Improve Application Performance

Introduction

Global DNS performance and availability are critical to user experience. According to Gartner, “DNS is mission-critical to all organizations that connect to the internet. DNS failure or poor performance leads to applications, data and content becoming unavailable, causing user frustration, lost sales and business reputation damage.”¹ But many businesses still rely on a single, often in-house DNS solution that lacks global scale and resiliency. This white paper reviews the business advantages of implementing a high availability DNS architecture using redundant DNS services. You will learn:

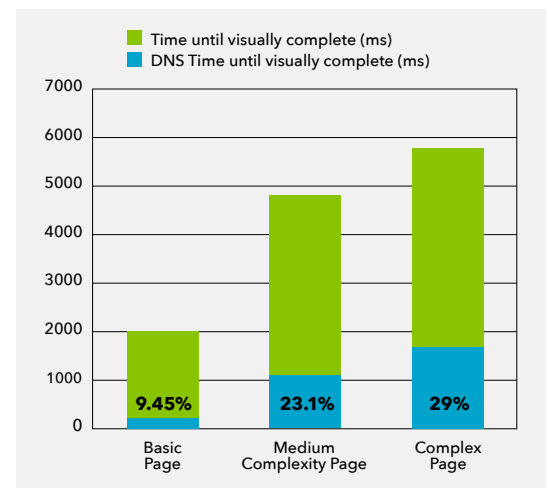
- * The critical role DNS plays in the user experience.
- * The risks of relying solely on a single DNS solution.
- * The added performance and reliability benefits of a high availability DNS architecture with a redundant managed DNS service.
- * Criteria for evaluating a managed DNS service provider.

DNS is Central to the User Experience

Every user's first interaction with your online applications and services begins with a series of DNS queries. The Domain Name System (DNS) is a distributed internet database that maps human-readable names to IP addresses, enabling users to reach the correct destination when entering a URL. DNS mappings are maintained in special-purpose servers called DNS nameservers. When a user enters your company's URL, a DNS query is routed to a DNS nameserver that contains the address mappings for your company's internet domain.

Your online applications, content, data and services may be scattered across the internet. Some of your assets might reside in your corporate data center, some might be distributed across a CDN and some might reside in the cloud. DNS is responsible for steering users to the proper source.

DNS availability and performance are central to the user experience. A contemporary webpage can involve dozens of DNS lookups. For complex webpages, DNS resolution can comprise as much as 29% of initial page load time.²



1 [*If External DNS Fails, So Does Your Digital Business*](#); Gartner, Refreshed 15 September 2016

2 Based on Dyn internal testing

If your DNS solution is unreachable because of hardware failures, network problems or configuration errors, users may not be able to access your assets—regardless of where those assets reside. If DNS responses are sluggish because of internet congestion or latency the user experience will be impaired and your business may suffer.

To make matters worse, research suggests that threats to DNS availability are on the rise. For example, infrastructure layer (layers 3 & 4) Distributed Denial of Service (DDoS) attacks increased by 151% year-over-year.³ While a recent Aberdeen Group report found that 78% of enterprise organizations surveyed experience four or more website disruptions per month at an average cost of \$1,000 per minute of downtime.⁴

In-House DNS Solution Constraints and Risks

Many businesses rely solely on in-house DNS solutions that don't deliver global reach, availability or performance. Creating a highly scalable, reliable and efficient DNS service requires time, money and know-how. Most businesses lack the expertise, financial wherewithal and focus to build out, support and safeguard global DNS infrastructure on their own.

Most in-house DNS solutions consist of a relatively small number of DNS nameservers deployed in one or two data centers in a unicast delegation pattern. Relying on a single DNS solution with a small footprint is inherently risky and inefficient. Concerns include:

- ★ **Availability constraints:** If your DNS solution is unreachable for any reason (disaster, equipment failure, networking outage) users may not be able to access your website or web-based applications—regardless of where your content or services are hosted.
- ★ **Security vulnerabilities:** In-house DNS solutions are particularly vulnerable to DoS/DDoS attacks. Hackers can impair your DNS service by overwhelming or incapacitating your nameservers or, more commonly, the bandwidth to reach them. Most in-house IT teams lack the time and resources to keep pace with ever-evolving and increasingly sophisticated security threats.
- ★ **Performance limitations:** DNS queries and responses are subject to network transmission delays and propagation delays as they make their way across the internet and traverse intermediary routers. Most in-house DNS solutions are based on a small number of nameservers deployed in a limited number of sites many hops away from most global users.

Boost Performance and Resiliency with a High Availability DNS Architecture and a Redundant Managed DNS Service

You can improve the performance, security and reliability of your DNS infrastructure by adding a managed DNS service to your IT environment. Best-of-breed managed DNS service providers have the global DNS infrastructure and deep DNS expertise to ensure your success.

Adding a redundant DNS service provides resiliency at the DNS layer. If your primary DNS service suffers an outage or is attacked, the redundant service remains fully operational (leading providers offer 99.999% availability commitments). Adding a secondary, global DNS service can also help you deliver consistent, high-quality user experiences across the world.

³ [*Akamai State of the Internet Report*](#); Q2 2016 vs. Q2 2015.

⁴ [*Constant Website Disruptions Demand a New Kind of Performance Management*](#); Aberdeen Group, July 2016.

Advantages of adding a redundant DNS service include:

- ★ **Global scalability:** Leading DNS service providers operate large-scale anycast networks with multiple PoPs across the globe. Global anycast networks accelerate DNS resolution by automatically steering DNS queries to the closest PoP, minimizing internet latency. In addition, some leading DNS service providers connect directly to Tier 1 internet transit providers, reducing intermediary hops.
- ★ **High availability:** Best-in-class DNS service providers operate out of geographically distributed PoPs on separate power grids, floodplains and fault lines to protect against disasters. They employ fully redundant server configurations to protect against hardware failures. And they connect to multiple Tier 1 transit providers at each PoP for resiliency.
- ★ **Strong security:** Best-of-breed DNS service providers employ a variety of security measures to establish trust, defend against threats and malicious attacks, and mitigate risk. They retain dedicated security experts who closely monitor industry trends and proactively update data center systems and practices.
- ★ **Rapid record propagation:** Best-in-class service providers globally disseminate DNS record changes in less than a minute.
- ★ **DNS expertise and support:** Leading DNS service providers employ full-time DNS experts and offer 24x7x365 technical support to help you keep your website running smoothly around the clock.

A complementary managed DNS service is a great way to protect and extend your previous DNS infrastructure investments. You can evaluate, pilot and implement a redundant service without introducing risk or disrupting your current DNS infrastructure.

Unicast Addressing vs Anycast Addressing

Distributed DNS networks can be implemented using two distinct standards-based IP addressing schemes: unicast addressing or anycast addressing. The unicast approach is far simpler to implement, but the anycast approach offers significant performance and resiliency benefits.

Unicast addressing delivers unpredictable results

*The DNS request may be answered by **any** Point of Presence (PoP) and potentially increasing latency.*



With a unicast approach each of your company's DNS nameservers (or server clusters) is assigned a unique IP address which resolves to a single (thus uni) physical location. The recursive DNS nameserver (typically owned by the user's ISP) maintains a table of your domain's nameservers and their corresponding IP

addresses. When a user enters your company's URL, the recursive server arbitrarily⁵ performs a request to the IP address of one of your DNS nameservers which then returns the IP of the asset the user is trying to reach. You have no control over which of your nameservers the recursive server selects. A user in China could be served by a nameserver in North America. And a user in the U.S. could be served by a nameserver in Europe.

Anycast addressing optimizes DNS performance, enabling consistent user experiences across the globe.



*The DNS request is answered by **the closest** Point of Presence (PoP) for the fastest possible DNS performance.*

With an anycast addressing scheme, all your DNS nameservers are broadcast from many locations around the globe from a each IP. When a user enters your URL, the recursive DNS nameserver resolves to the closest location of your DNS nameservers. The IP network automatically routes queries to the “closest” nameserver using BGP.⁶

The anycast approach offers a variety of advantages:

- ★ **Better performance:** Anycast accelerates DNS resolution by automatically directing DNS queries to the “closest” DNS nameserver, minimizing internet latency. Anycast also enhances the performance of your overall DNS infrastructure by increasing its global footprint.
- ★ **Greater resiliency:** Anycast provides predictable and more efficient failover mechanisms. With the unicast approach, you must rely on resolvers failing over through the nameserver list when there is a DNS timeout. With the anycast approach, should a location become unavailable, that announcement would drop from BGP, and queries are deterministically directed to the next “closest” active server.
- ★ **Stronger security:** Anycast provides fundamental security advantages over unicast. Unicast exposes the IP addresses of individual servers. Hackers can initiate targeted DoS/DDoS attacks against specific physical servers or virtual machines. This could cause normal traffic to divert to suboptimal servers around the world, causing even further disruption. Anycast reduces security threats by concealing the addresses of individual servers and by automatically dispersing DDoS attacks across collections of compute resources behind the anycast IP address.

⁵ Initially, this is arbitrary. Over time, recursives will store response information to make this less arbitrary directing queries to preferred nameservers. However the initial responses to the sub-optimal nameserver, as well as daily checks, would still be performed. This is known as Round Trip Time (RTT) banding (see: dyn.com/blog; May, 2012)

⁶ BGP directs the query to the DNS nameserver with the lowest hop count.

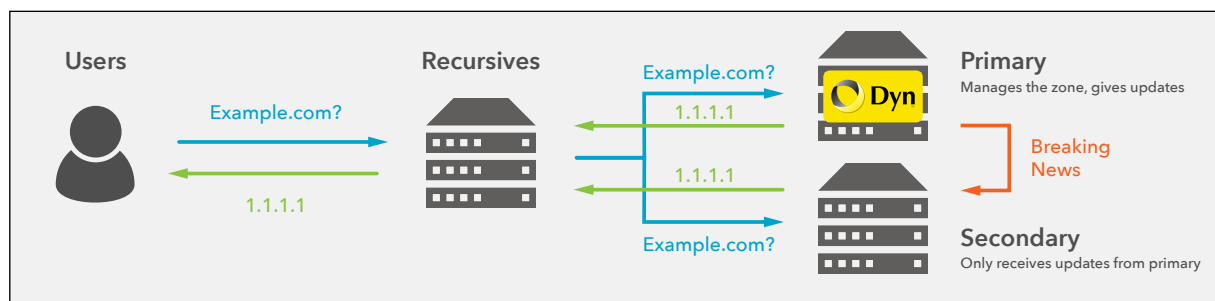
Multi-DNS Deployment Options

There are various ways to add a redundant DNS service to your existing DNS infrastructure. Each option offers unique advantages and drawbacks.

Traditional Primary-Secondary Option

The existing DNS solution acts as the primary DNS service from a DNS records management perspective. Record updates are made to the primary service using established tools and practices. The primary service automatically updates the secondary service. Both services respond to DNS queries.

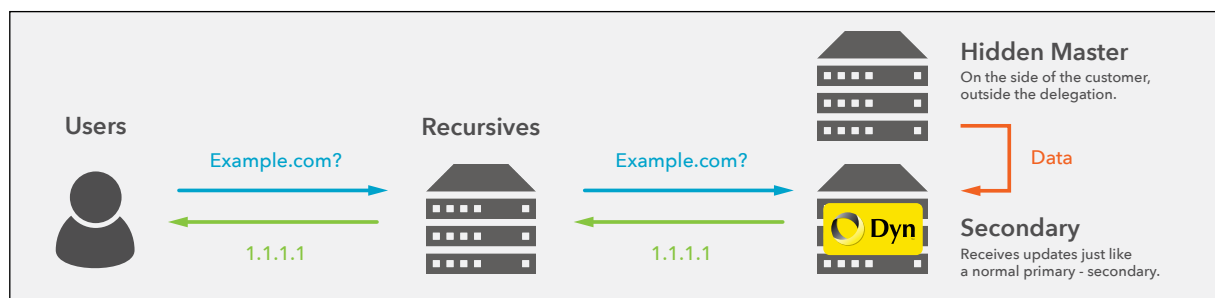
- ★ **Pros:** Easy to deploy. Increased redundancy with multi vendor strategy.
- ★ **Cons:** You cannot take advantage of advanced features such as end-user traffic steering and load balancing; if the primary service suffers an outage, ability to update records is lost. If the primary is internal, your edge is still exposed to attack and contributes to poor global performance.



Hidden Master-Secondary Option

The existing DNS solution is deployed behind the corporate firewall and acts as the primary DNS service from a DNS records management perspective. Record updates are made to the primary service using established tools and practices. The primary service automatically updates the secondary service. Only the distributed edge takes traffic. Often this process is then repeated with a second secondary solution to have two vendors in delegation, with the master safely calling the shots.

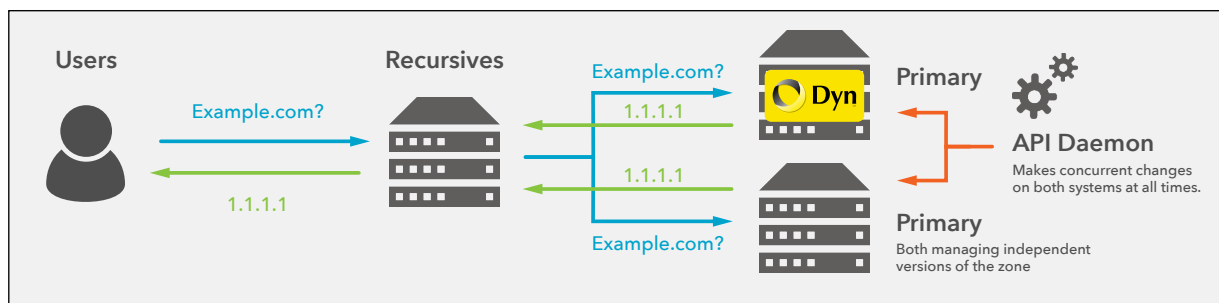
- ★ **Pros:** Provides added security (only supplementary DNS service is visible to the outside world). Greater performance with a distributed anycast edge. Keep existing workflows and set up easily.
- ★ **Cons:** You cannot take advantage of advanced features; if the primary service suffers an outage, ability to update records is lost.



Primary-Primary Option

Each DNS service is updated independently. Records are automatically synchronized across services manually, with the API, or via an external application. Both services respond to DNS queries.

- ★ **Pros:** You can take advantage of advanced features so long as both providers support them; you can update DNS records from either service; you can still update DNS records if one of the services fails.
- ★ **Cons:** More complex to successfully deploy or administer (you'll need to manually update both services or write an application to sync records across services). Costs of advanced features increases as a multiple of number of providers.



Choosing the Right Managed DNS Service Provider

Not all managed DNS services are the same. Don't be fooled by free DNS services offered by your ISP or hosting provider, or by cloud providers or CDN providers that offer adjunct DNS services. Go with a service provider that lives and breathes DNS. Best-in-class managed DNS providers have the worldwide DNS infrastructure, experience and resources to ensure your success.

Supplementary Managed DNS Service Provider Checklist:

- ★ DNS expertise and focus
- ★ Global anycast DNS network with PoPs across the world
- ★ High availability DNS solution with fully redundant DNS constellations and multiple Tier 1 transit providers per PoP
- ★ Advanced features like end-user traffic steering and load balancing
- ★ DNS-based DDoS protection and in-house security experts
- ★ Open APIs
- ★ Easy-to-use reporting and management tools
- ★ 24x7x365 customer service

Conclusion: Deliver Legendary User Experiences with a High Availability DNS Architecture with Redundant DNS Services

DNS speed and reliability are fundamental to the performance of your web-based applications, services and data, and are essential to your business. You can improve user experiences and boost business results by adding a redundant managed DNS service to your IT infrastructure.

You'll gain a variety of benefits, including:

- ★ **Global performance:** Deliver consistent, high-quality user experiences across the world with a global DNS footprint.
- ★ **Greater peace-of-mind:** Enjoy the resiliency and security advantages of a worldwide anycast DNS network backed by DNS experts and stringent SLAs.
- ★ **Better business results:** Superior DNS performance translates directly to better user experiences, improved customer satisfaction, lower website abandonment and greater revenue.

About Dyn

Dyn is a cloud-based Internet Performance Management (IPM) company that provides unrivaled visibility and control into cloud and public internet resources. Dyn's platform monitors, controls and optimizes applications and infrastructure through Data, Analytics, and Traffic Steering, ensuring traffic gets delivered faster, safer and more reliably than ever.

Dyn is the leading IPM provider to the largest enterprises and most visited web properties in the world, including eight of the top 10 internet services and retail companies, and six of the top 10 entertainment companies, in the Fortune 500. Dyn helps everyone from startups to companies like Pfizer, Netflix and Twitter solve the challenges associated with Internet scale, complexity and volatility. Dyn is Internet Performance. Delivered.

[learn more](#)

Contact Dyn today to learn how a redundant DNS service can help you optimize DNS performance, improve user experiences and boost business results.