IBM NS1 Connect

The need for speed

Why you should give your network's DNS performance a closer look

IBM

catchpoint

Table of contents

Introduction

Nearly everything on the internet depends on the Domain Name System (DNS) to function as intended and expected. DNS is fundamental to every website or application connection. It's what translates and connects domain names to the web of unique Internet Protocol (IP) addresses, so browsers can load the internet resources that provide the user experience.[1] DNS is the protocol that tells your device where an application lives on the internet. Every connection your phone, laptop or tablet uses to collect information—including this piece you're reading right now—starts with a DNS connection.

We see applications and websites as fully formed pieces of content that sit in a single location—Google.com or the Yelp app, for example. The reality is that underneath that unified user experience there are often hundreds of DNS connections happening at any given moment. When you access a website or application, it's probably delivering things like photos, advertisements, headlines, graphics and videos—all from different places. DNS is what makes those connections happen. For an optimal experience, the user should remain blissfully unaware of all that activity.

The speed of DNS connections is a critical factor in the performance of applications and websites we use every day for work and play. Given the importance of DNS performance to companies around the globe, IBM collaborated with internet performance monitoring experts, Catchpoint Systems, Inc., to measure the speed of DNS connections to over 2,000 of the most visited websites. Our goal was to compare the performance of authoritative DNS providers.

Using a meticulously designed series of tests, we measured the performance of the top websites during peak season for internet traffic. We found a significant difference between DNS providers. Self-hosted authoritative DNS architectures were significantly slower than managed DNS options. We also found major differences between the performance of managed DNS providers, with one product providing a significant boost over competitive offerings.

Performance starts with DNS

Tracking the business impact of poor DNS performance

When you see that spinning wheel or hourglass icon in an app or on a website, how long does it take you to click away? Studies reveal it's a matter of seconds. Collectively, our patience with slow-loading websites and applications is wearing thin.

Time can cost revenue—and reputation

There's a direct correlation between poor website or application performance and revenue:

- A study from Portent found that B2B sites that load in 1 second have a conversion rate 3 times higher than sites that load in 5 seconds.[3]
- Looking specifically at application performance, Deloitte found that just a 0.1 second improvement in application response times led to 10% sales growth.[4]

Not only is revenue directly impacted, but brand reputation is also connected to application and website performance. According to WebsiteBuilderExpert, 64% of shoppers won't visit a slow website again[2]—a blow not only to the company's bottom line, but also to its perceived value. This kind of reputational damage can be far more costly over time than the immediate loss in revenue.

The where and the how of DNS

DNS not only locates *where* to make a connection, but also dictates *how* that connection actually comes about. Left to its own devices, DNS will make a connection but not always the best connection for the technology profile of a specific business. Alternatively, you can make a deliberate choice to send DNS to the best available back-end resources at any given moment.

> One in four website visitors leave a site that takes more than 4 seconds to load, and every 1 second delay in website load times reduces user satisfaction by 16%.[2]

Of course, the very idea of the "best connection" varies from business to business. In some markets like retail or e-commerce, the speed of a connection is the most important factor. In others, like banking, reliability or resilience is more important. Still others prioritize the cost of delivering content to users.

In a nutshell, the architecture and deployment of DNS determines how a business makes any connections to its customers and users. All of those statistics about speed and how it impacts revenue often come down to how a business deploys its DNS.

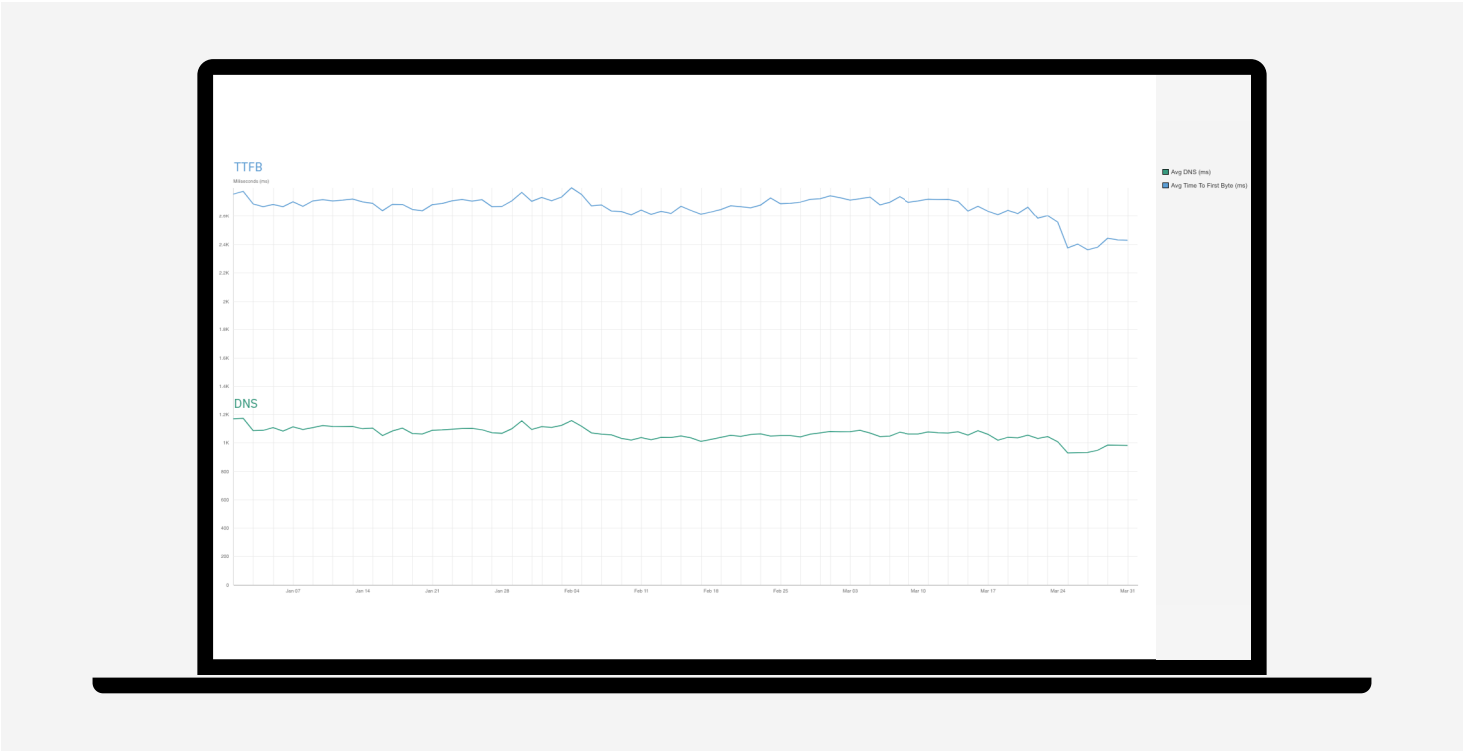


Figure 1. The average TTFB, tracked over a 90-day period, of a large software company's website

How page load times can impact SEO

DNS also plays a key role in search engine optimization (SEO)—the rankings that help determine how easy it is to find a business' content on the internet. It's common knowledge among industry experts that page load times factor into page search engine rankings.

The quantity and quality of DNS connections play a large role in page load times. Some businesses try to reduce page load times by eliminating unnecessary DNS lookups, but there will always be a core set of DNS queries that just have to happen. When the underlying connection is necessary, the only option is to reduce how long it takes to resolve.

To illustrate this connection between DNS load times and SEO metrics, in October 2023 we performed an analysis of a large software company's website using data from Catchpoint's web test and Google's PageSpeed Insights. See figure 1.

The average time to first byte (TTFB) of the software company's website, measured over 90 days from 11 November 2023 through 11 February 2024, was 2,699 milliseconds, about 2.7 seconds. A substantial portion of this can be attributed to the DNS lookup, which averaged 1,083 milliseconds, about 1.1 seconds.

This rather long DNS connection time directly impacts TTFB, which in turn influences both the website's overall performance and its SEO ranking. We can see this impact in the resulting SEO score in Google PageSpeed Insights, shown in figure 2. If the software company were to optimize its DNS resolution time by reducing TTFB, its performance and SEO standing would improve.

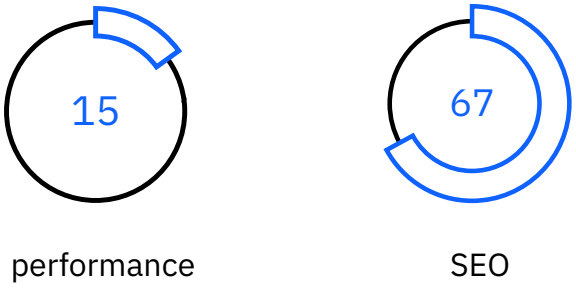


Figure 2. The large software company's SEO score in Google PageSpeed Insights

The challenges in measuring DNS performance

Given the critical role of DNS in practically every application and website worldwide, one might expect there to be abundant data illustrating the performance of various DNS solutions. Unfortunately, comprehensive and precise data on DNS performance can be hard to find, largely because it's incredibly complex to measure DNS performance as real-world DNS connections are influenced by many potential variables, including:

- **Local ISP connection.** The performance of DNS is directly impacted by the quality and speed of the user's internet connection, which varies significantly by provider and geography.
- **Distance.** The further the geographical distance between the user and the server, the longer the DNS response time.
- **Routing.** The number of "hops" and the distance between them can impact DNS response times. Inefficient routing between host servers and users introduces delays and impacts the overall speed of DNS resolution.
- **Resolver proximity.** When users are far away from intermediate resolver resources in the recursion chain, this often results in slower DNS resolution times.
- **Third-party tools.** Many do-it-yourself (DIY) measurement tools don't have a reliable or consistent approach, making it challenging to use them for benchmarking.

These variables encompass a range of factors influencing DNS performance, and each plays a crucial role in determining how efficiently DNS queries are resolved. It's important to recognize and understand the variables to interpret DNS performance data accurately.

Because of the complexity these factors introduce, businesses tend to overlook DNS as a critical component of their success in the marketplace; it's difficult to measure in objective terms. In the absence of standardized metrics, businesses tend to invest in basic, "good enough" solutions that answer queries reliably but not optimally.

Furthermore, many companies build their own DNS architecture with open-source tools and servers they deploy around the world. This DIY, self-hosted approach to DNS can seem like a good solution, because it allows companies complete control over their DNS and naturally appeals to network engineers who prefer to build things themselves. But as this report will show, there are operational consequences that flow from the decision to self-host.

What we studied

Recognizing both the importance of measuring DNS performance and the lack of reliable metrics network operators can use to benchmark their own applications, IBM joined forces with Catchpoint to perform a study of DNS performance worldwide. Our goal was to put some concrete numbers behind the various options for DNS management.

We paired public data about the DNS architectures of the most visited websites in the world with Catchpoint's deep insights into application performance to produce a comparative look at how DNS performs in real-world situations. Catchpoint was the perfect collaborator for this effort because of their unequalled global observability network[5] and powerful DNS monitoring capabilities.

> Monitoring and fine-tuning DNS resolutions can prove instrumental in navigating the complex web of dependencies and enhancing overall web page performance.

What makes Catchpoint's observability network stand out is its unparalleled scale, featuring a vast, global and strategically positioned network infrastructure; extensive coverage, encompassing diverse locations and major internet hubs; and advanced data processing capabilities. Taken together, this enables the Catchpoint internet performance monitoring (IPM) platform to provide an unparalleled understanding of internet and DNS performance in real situations. The platform not only captures data comprehensively but also analyzes it effectively, making it an invaluable asset for studies of this nature.

The methodology behind measuring true DNS performance

We compiled a list of the most visited websites across the world that totaled 2,271 websites, then conducted the tests in the most active time of the year—the peak holiday shopping season of November and December 2023. All of our data was collected on weekdays to capture, as best we could, a consistent sample of "typical" traffic.

Catchpoint was the perfect collaborator on this analysis, as they operate an industry-leading Internet Performance Monitoring Platform, known for its expansive global observability network. Catchpoint offers solutions like Synthetic Monitoring, Real User Monitoring (RUM), and Endpoint Monitoring to provide deep insight into internet performance across diverse environments—making it the ideal platform from which to conduct these DNS test.

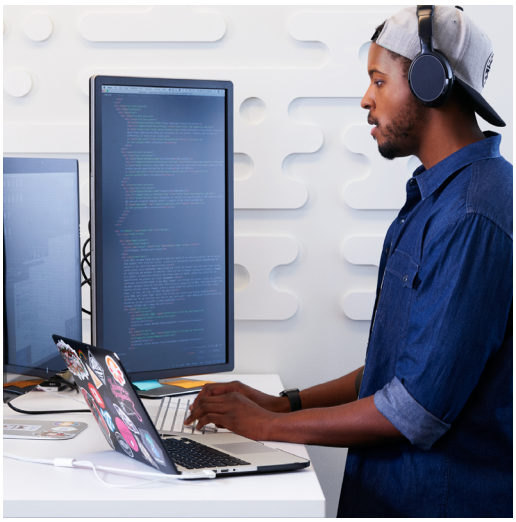
We conducted DNS lookups for the corporate websites of all our target dataset, correlating the nameserver addresses with known DNS providers. Throughout this report, we refer to "premium DNS" services as a category of solutions which deliver enterprise-grade managed DNS services. We use the term "premium" to distinguish these solutions from the basic DNS services provided by domain registrars. In this report, we put the following solutions in the "premium" category: IBM NS1 Connect, Vercara UltraDNS + CSC, Cloudflare DNS, AWS Route 53, Akamai Edge DNS.

Some DNS providers offer their services through third parties, such as registrars. When these connections were known, we added them together. A handful of premium DNS providers, including Domain Control, DNS Made Easy, Azure DNS and Google DNS, weren't well-represented in our sample, so we decided to exclude them from our analysis rather than draw conclusions from insufficient data.

When a nameserver record didn't indicate a known managed DNS provider, it was categorized as self-hosted. In some cases, this approach probably resulted in categorizing some second-tier DNS providers as self-hosted, but we were unable to find an easy way to weed those out using public data.

The table shown provides the sample sizes for the major DNS providers included in this study, where *n* represents the number of nameservers sampled per provider.

DNS provider	*n*
IBM NS1 Connect	309
Vercara UltraDNS + CSC	242
Cloudflare DNS	289
AWS Route 53	108
Akamai Edge DNS	281
Self-hosted	1,042
Total	**2,271**



Test design

Because our goal was to compare the performance of authoritative DNS options, we had to eliminate the influence of other factors which might have skewed the results. For this reason, we deliberately conducted tests without leveraging any additional internet capabilities that could potentially accelerate performance. We made this decision to establish a valid technical baseline, eliminating extraneous variables and providing a set of control data that reflects a level playing field.

Specifically, we opted not to dictate the use of specific accelerated DNS services, such as Cloudflare DNS or Google DNS. Instead, we allowed the resolvers to autonomously choose the best nameservers. This decision aligns with the reality that a significant portion of users rely on their local ISP resolvers; the majority don't actively spend time configuring alternative DNS services like Google or Cloudflare.

The rationale behind this approach was to help ensure a realistic representation of DNS performance under typical user conditions, acknowledging that many users default to their ISP's resolvers. This design choice addresses concerns about skewing the data collected from widely known, high-performance DNS services, which would artificially inflate performance. By allowing the resolvers to make autonomous choices, our study captures a more authentic reflection of DNS performance in real-world scenarios.

Designing the DNS tests

What constituted our DNS tests?
A DNS test involves querying DNS servers to measure their response times and assess their overall performance. Specifically, we focused on direct DNS tests, which entailed sending DNS queries directly to authoritative DNS servers. Authoritative DNS servers are responsible for providing the official responses to DNS queries for specific domain names.

In our testing methodology, we sent DNS queries directly to authoritative DNS servers to gauge their efficiency in responding to these requests. The *response time* metric, a key aspect of our analysis, measures the time taken by the authoritative DNS server to respond to the query. This metric is crucial for understanding how quickly a DNS server can provide accurate and reliable information and thereby influence the overall performance of web applications and services.

Testing types and why they matter
The difference between synthetic tests and "real" or instant tests lies in their nature and purpose. The choice between synthetic tests over an extended period and instant tests is driven by the specific goals of the assessment.

- **Synthetic tests:** These tests involve the simulation of user interactions with the DNS server. These tests are scripted to mimic specific actions a user might take, providing controlled and predictable scenarios. Synthetic tests are designed for proactive monitoring and performance optimization and can help identify potential issues before they impact real users by offering insights into baseline performance and potential bottlenecks.

  This approach provides a more comprehensive and accurate assessment of DNS performance by capturing variations and trends over an extended period. It offers a holistic view, allowing for the identification of patterns and potential issues that might not be apparent in a single-instant test.

- **Instant tests:** "Real" or instant tests represent a snapshot of the current state of DNS server performance at a particular moment. These tests reflect the actual conditions and responses at the time of execution.

  These kinds of tests are valuable for immediate data collection and troubleshooting and can be useful for diagnosing issues quickly but might not provide a comprehensive view of overall performance trends. Relying solely on instant tests might not allow you to capture the broader trends or variations in DNS performance; therefore, you might miss underlying issues that become evident only over time.

Running the DNS tests

Tests we ran
We ran DNS tests using a representative sample of 216 backbone nodes, strategically positioned to represent major ISPs worldwide. These nodes, strategically stationed in Tier 1 data centers, establish a direct connection with major internet providers, adopting a single-homed configuration. This setup allows for the meticulous isolation of performance metrics by ISP. Within these backbone nodes, local DNS resolvers are deployed, colocated in the same data center and ISP infrastructure, helping ensure precise DNS performance data for each geographical location.

Backbone nodes are important to our testing methodology because of their ability to provide granular insights into baseline performance expectations for users in a specific region. By excluding the variability introduced by users' individual ISPs and networks, backbone nodes offer a clear and standardized perspective. In most monitoring scenarios, the inclusion of backbone nodes is imperative, because they contribute invaluable data toward understanding the foundational performance levels that users can anticipate, irrespective of the intricacies of their own ISPs and network configurations.

Scope of Catchpoint locations
The locations chosen for assessment spanned Asia, Europe, North America, Oceania and South America, offering a global perspective on DNS performance. To create a focused and comprehensive analysis, some ISPs were deliberately repeated across multiple locations. For instance, Verizon may appear in both San Francisco and New York, reflecting its availability and presence across the US. Although the list of backbone nodes specifically mentioned the ISPs, it's essential to note that the 216 nodes encompassed this intentional repetition. In this way we were able to capture performance across various regions and help ensure a thorough examination of DNS performance expectations for users, while accounting for the widespread availability of certain ISPs in multiple locations.

List of backbone nodes:

- **Asia:** Airtel, Tata, Jio, Vodafone, ACT, Singtel, Starhub, KDDI, PCCW, Emirates Telecomm
- **Europe:** Telia, Vodafone, BT, Orange, Swisscom, DTAG
- **North America:** AT&T, Verizon, Comcast, GTT, Level 3, Bell Canada, Rogers
- **Oceania:** Telstra, Vodafone, Optus, Vocus
- **South America:** Telefonica, Giga, Entel

Testing timeframe
We opted to conduct synthetic checks over 48 hours with a frequency of one run per minute instead of using instant tests. By choosing this testing approach, Catchpoint helped ensure a thorough and in-depth evaluation of DNS performance, providing a more nuanced understanding of how the servers behave over different conditions and usage scenarios.

Conducting synthetic checks over an extended period, we gathered 13 samples from each ISP's backbone nodes, resulting in an overall sample of 2,880 runs for each DNS test. This extended-testing approach allowed us to capture variations and trends in DNS performance over time, providing a more accurate and holistic assessment.

Assessing DNS performance

How we benchmarked performance

In evaluating DNS performance, we focused on the critical metric of *response time*: how swiftly the DNS server responds to queries. Although there are additional metrics, such as resolution accuracy, reliability and geographic reach, we deliberately chose to prioritize real-world user scenarios in our analysis. Recognizing that in practical terms users seldom concern themselves with the specific nameservers, their resolution accuracy or the geographic locations involved, we opted for a direct DNS test approach to mimic the actual behavior of users connecting to a website.

Our decision not to cover resolution accuracy, reliability and geographic reach in this study doesn't diminish their significance. In cases where organizations are dealing with challenges related to these aspects, Catchpoint's "DNS experience" test type provides a specialized examination. This test allows us to probe into the complexities of DNS resolutions, latency variations at different levels and other factors impacting accuracy, reliability and global reach.

The *response time* metric served as the primary criterion for categorizing DNS performance into *good, better* and *best* classifications. Servers falling within an acceptable range were classified as *good*, those demonstrating notable efficiency as *better* and those exhibiting exceptionally prompt response times as *best.*

Geographic factors

Geographic factors impacting DNS performance often revolve around infrastructure, network connectivity and server distribution. North America and Europe generally show better performance due to:

- Infrastructure density: higher concentration of data centers and DNS servers
- Network connectivity: robust internet backbones and connectivity between major cities
- Server proximity: closer proximity to DNS servers, resulting in lower latency

Conversely, Asia and Oceania often face challenges due to longer network distances, less-dense server infrastructure and regulatory constraints—thus impacting internet access or DNS resolution paths.

The specific challenge of China

China presents special challenges due to its unique internet architecture and regulatory controls. DNS resolution within China can be slower due to government regulations and the rerouting of traffic through specific gateways. As a result, accessing DNS servers outside China might face increased latency, impacting overall performance. To address this challenge, optimizing DNS within China and using China-specific DNS services or content delivery network (CDN) providers becomes crucial.

Catchpoint boasts the highest node presence among major ISPs in China, providing a comprehensive view of DNS performance within the country. This extensive network presence allows Catchpoint to monitor and analyze DNS performance intricacies far better than any other service and offer valuable insights into the unique complexities of DNS resolution within China. These insights can offer a comprehensive understanding of how Catchpoint assesses DNS performance, compares measurements and navigates geographic challenges across the globe, especially in regions like China. Adjustments or further details can be added based on the specific data or insights available from Catchpoint's analyses.

The bottom line

Many network teams will look at the response times in this report and wonder, "Why are they so slow?" While this may appear to be the case at first glance, the purposeful methodology and test design ultimately helps ensure the validity and relevance of the results within the context of diverse user behaviors and preferences.

The bottom line: our tests were designed to compare the relative performance of different authoritative DNS providers, not to provide an assessment of typical DNS connection performance as a user would experience it.

What we found

Global average
The average DNS response time across the websites we studied was 263 ms. This is a global average, measured across geographical regions, local ISPs and authoritative DNS providers.

Regional variations
There's a lot of regional variation in that number; response times in Europe and North America are significantly faster than in other regions. Much of that variation can be attributed to the sheer density of DNS servers in both regions, which are positioned to serve the needs of the largest players in the world economy.

Geography is also a factor. The distance that a query needs to travel in Asia, South America and, especially, Oceania, is farther than in North America or Europe. That fact naturally adds to the response times from these regions.

The variation in response times from different DNS providers was generally consistent across regions. As you can see in figure 3, the different categories of DNS providers showed similar patterns.

Self-hosted DNS performed a bit worse in Asia, South America and Oceania. This pattern squares with the greater distances queries need to travel in those regions—travel time to the nearest point of presence is longer. This is especially true for self-hosted DNS systems, which tend to have fewer points of presence.

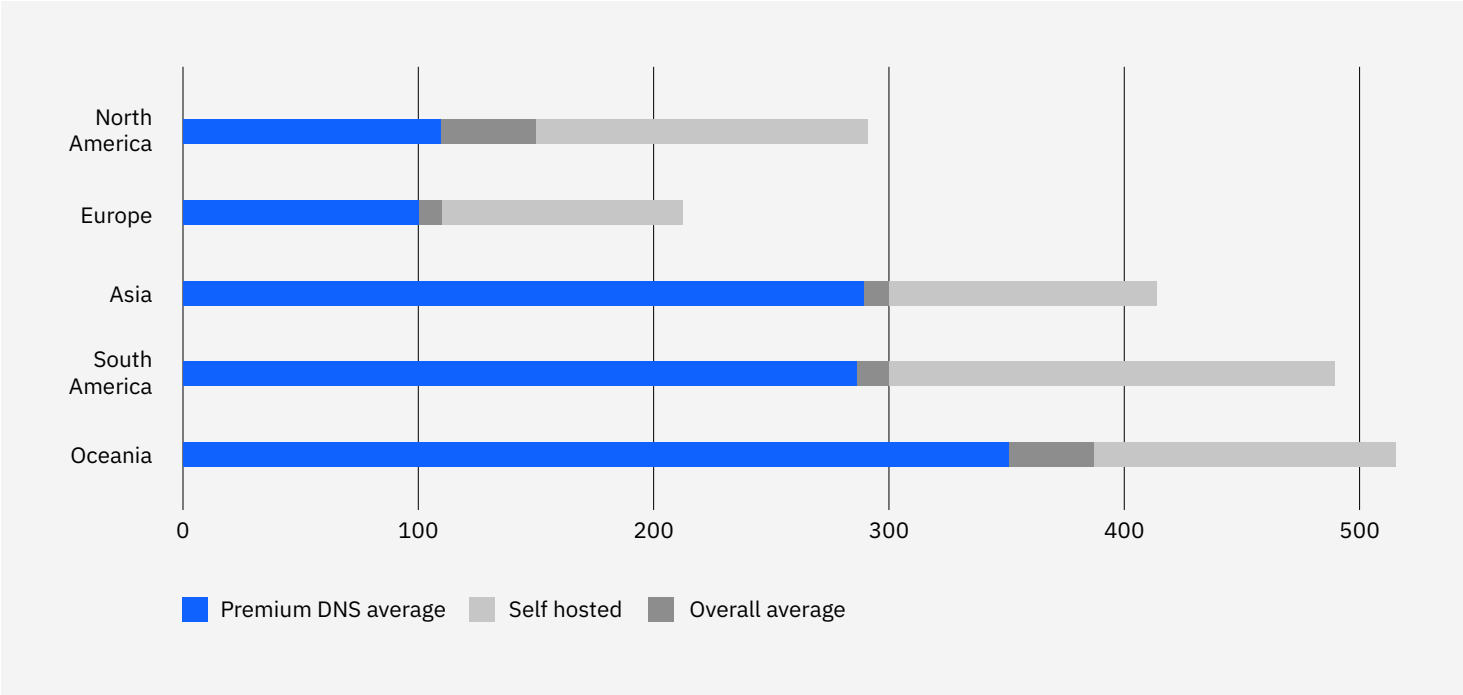


Figure 3. Average DNS response times by region, in milliseconds, with the average speeds of the premium DNS providers faster across the regions

Variations by DNS provider type

We found a significant difference between the performance of companies that self-host their DNS and companies that use a premium managed DNS service.

Self-hosted DNS response time was 35% slower than the average global response time in our tests, as shown in figure 4. That's an average difference of 141 ms, which a user would certainly notice when compounded across all the DNS queries it takes to load the typical website or application.

The gap is even larger between self-hosted and premium DNS providers—self-hosted is 41% slower, with an average lag of 161 ms. The difference is even more telling between self-hosted DNS and IBM NS1 Connect—self-hosted is 60% slower, a whopping 244 ms difference.

Many companies decide to self-host their DNS to control everything about their connections, but our numbers clearly show that the investment isn't paying off when it comes to performance.

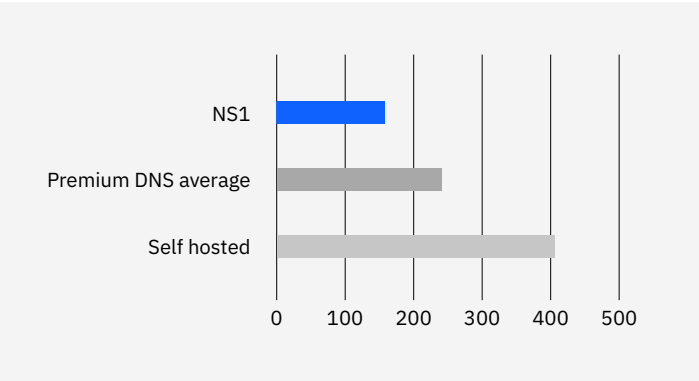


Figure 4. Average comparative global DNS response times, in milliseconds, with NS1 outperforming the self-hosted and peer premium DNS providers

Variations by managed DNS provider

There's a fairly clear difference between premium and self-hosted DNS services. But what about the differences between DNS providers themselves? It turns out that the performance of managed DNS providers can vary significantly, also, as you can see in figure 5.

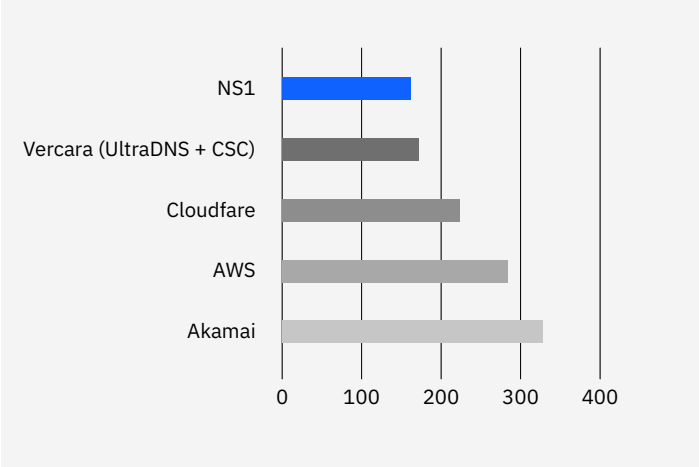


Figure 5. Average global response times, in milliseconds, for the five top-performing premium DNS providers studied

NS1 Connect emerged as the fastest premium DNS provider, with an average response time 39% faster than the global average. Close behind was Vercara UltraDNS, with 35% faster connections than the global average, and Cloudflare DNS was in third place, with 16% faster connections than the global average.

Two of the remaining premium DNS providers we researched came in below the global average. AWS Route 53 delivered response times 9% slower than the global average—not a gigantic difference, but certainly noticeable when compared to the faster premium DNS providers. Akamai Edge DNS proved to be the worst-performing premium DNS provider, with 24% slower connections than the global average and 51% slower connections than NS1 Connect.

Variations by traffic volume

IBM and Catchpoint compiled a list of the most-visited websites in the world. We looked at the distribution of DNS response times by the amount of traffic a company receives. Our expectation was that those that receive the most traffic tend to have the most sophisticated networks and would therefore be much faster than enterprises further down the list.

The distribution was more evenly distributed than we anticipated—the pattern of DNS response times was roughly similar across the most-visited websites. There was a small cluster of companies that did extremely well, but even among the top 100 there were some outliers with comparably poor performance. On the other end of the spectrum, companies near the bottom often did quite well with their DNS connection times.

Just 23 companies reporting had DNS connection times slower than 1,000 ms. Extreme outliers were found just about equally at any point across the spectrum. Tellingly, all but three of these companies experiencing slow DNS connection times used a self-hosted DNS.

What it all means

Monitor your DNS performance
The significant differences in authoritative DNS performance demonstrated in this report show that monitoring DNS performance is crucial for maintaining a healthy and optimized online presence.

Why monitoring DNS performance matters
- Early issue detection. Identifying DNS issues early can prevent potential service disruptions or slowdowns for users.
- Optimization opportunities. Monitoring helps pinpoint areas for DNS infrastructure improvement, leading to faster load times and better user experiences.
- Geographical insights. Understanding regional variations aids in optimizing DNS configurations to ensure consistent performance across diverse locations.

The benefits of using Catchpoint for DNS monitoring
- Real-time visibility. Continuous monitoring provides real-time insights into DNS performance, enabling prompt action when anomalies are detected.
- Global perspective. Monitoring from various global locations offers a comprehensive view of DNS performance, minimizing blind spots and helping ensure optimized user experiences across regions.

Example use case
Consider the case of a large news media company's website that attracts a significant volume of user traffic. Looking at the company's website data from October 2023, we found that it loaded a staggering 692 items on a single page, ranging from HTMLs to images, scripts and font files.

Investigating deeper into the intricacies of web page loading, 238 hosts (that is, domains) were involved in creating new connections, necessitating DNS requests. Surprisingly, the overall web page response time clocked in at 20,533 ms, about 20.5 seconds, with a significant portion—11,353 ms, about 11.3 seconds—dedicated solely to DNS resolutions. This vivid example underscores the critical role of DNS performance, not only for your main domain but also for the countless dependencies entailing diverse hosts.

A WebPageTest analysis of the diversity of requests made by the same large news media company's website. Spanning advertising, content and publishing, CDNs, social, developer utilities, marketing, analytics and more, the test showed that optimizing DNS performance emerged as a paramount concern for a seamless and efficient user experience. Monitoring and fine-tuning DNS resolutions can thus prove instrumental in navigating the complex web of dependencies and enhancing overall web page performance.

How does a single web page of a large media company take over 20 seconds to load?

692
items load per page.

238
hosts necessitate DNS requests.

11
seconds are dedicated to DNS resolutions.

Choose your authoritative DNS provider wisely
Our study also demonstrated that the performance of authoritative DNS providers varies greatly. Specifically, it showed that self-hosted authoritative DNS offers significantly poorer performance than using a managed provider for authoritative DNS. The global reach, performance-enhancing feature set and reliability of a managed DNS service clearly trumps even the best self-hosted authoritative DNS option.

Even within the category of managed DNS providers, we found a significant difference in performance. Some managed providers actually delivered performance that was worse than the global average. Others, like NS1 Connect, outperformed their peers, delivering consistently faster performance around the world.

As noted at the outset, the choice of authoritative DNS provider isn't merely academic. It has real-world consequences for application performance, SEO, brand reputation and, ultimately, revenue.

How our tests compare

There are, of course, other DNS performance measurements in use today. DNSperf is a website that compares the performance of authoritative DNS providers and is often used as a performance benchmark by network teams and application owners. If you compare the performance metrics on DNSperf with the performance metrics in this paper, you'll notice a significant difference. Which one should you trust? Which one is more accurate?

When evaluating DNS performance, the testing infrastructure plays a pivotal role in helping ensure real-world relevance and comprehensive insights. Catchpoint's approach distinguishes itself through a diverse set of testing nodes and backbone nodes strategically positioned in Tier 1 data centers to best reflect real-world performance expectations.

In addition to the Tier 1 data center backbone nodes, Catchpoint extends its testing capabilities with nodes strategically hosted close to last-mile ISPs, providing insights into performance variations experienced by users. Our testing network also includes nodes hosted in public cloud environments to address the growth of cloud-based DNS services. Catchpoint's commitment to diverse testing nodes helps ensure a holistic assessment that mirrors the complexity of real-world DNS scenarios.

Catchpoint's assessment covers a wide spectrum of performance indicators from diverse global locations—more than 2,600 worldwide compared with 200-plus for DNSperf—enabling a comprehensive evaluation of DNS performance for different scenarios and conditions. DNSperf has not disclosed their server locations, which raises significant questions about how closely its testing environment aligns with real-world conditions.

Note also that, as outlined earlier, our test deliberately didn't leverage any additional internet services such as Cloudflare DNS or Google DNS that could potentially accelerate performance. This deliberate choice was made to establish a valid technical baseline, eliminating extraneous variables and providing a set of "control" data that reflects a level playing field. Measuring DNS performance from a DNS server hosted in the cloud doesn't always accurately capture the experience of users, who don't originate their web browsing from cloud servers. DNSperf includes these third-party internet services in their calculations by default.

About IBM NS1 Connect and Catchpoint

IBM NS1 Connect offers premium, authoritative DNS and advanced traffic steering to deliver the high-performance, reliable, secure network connectivity that businesses need to meet increasingly sophisticated customer expectations. NS1 Connect leverages its global anycast network to provide the massive capacity and scale needed to keep users reliably connected across the world. An API-first architecture empowers teams to embrace automation and streamline DNS management. Enterprises with complex network infrastructures can take performance to the next level with sophisticated traffic steering capabilities and real-time reporting on DNS observability data.

Learn more about IBM NS1 Connect →

Request a live demo →

Catchpoint Systems, Inc., is the industry-leading IPM platform renowned for its expansive global observability network—the largest of its kind worldwide. With a suite of comprehensive solutions, including Synthetic Monitoring, Real User Monitoring (RUM) and Endpoint Monitoring, Catchpoint's IPM platform provides deep insight into internet performance across diverse digital environments. In short, it was the ideal platform from which to conduct these DNS tests. Beyond testing, monitoring DNS performance is essential to maintaining optimal website and application performance and delivering a seamless user experience. Catchpoint DNS monitoring can actively monitor the speed, availability and security of the DNS infrastructure in real time to ensure that it's operating optimally and safely. In addition, Catchpoint offers a proactive approach to keeping organizations' DNS services running smoothly by enabling them to configure tests that can identify problems before they occur.

Learn more about Catchpoint →

Request a live demo →

1. What is DNS | How DNS works, Cloudflare, Inc., 2024.
2. Website Load Time Statistics: Why Speed Matters, Marketing VF Ltd., 27 November 2023.
3. Site Speed is (Still) Impacting Your Conversion Rate, Portent, 20 April 2022.
4. Milliseconds make Millions: A study on how improvements in mobile site speed positively affect a brand's bottom line, Deloitte Ireland LLP, 2020.
5. The world's largest, most reliable observability network, Catchpoint Systems, Inc., 2024.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
July 2024