



# The Case Against Free ISP DNS

*Something this important is worth paying for.*

Your enterprise knows that its web presence is business critical. Why do you trust the reliability of that presence to a company that far from specializes in it? Your DNS management is critical to the reliability, speed and safety of your company. That is something worth paying for.

The Domain Name System (DNS) is the critical link for network services between human names and computer addresses. DNS outages and misconfigurations cause website outages, email bouncing, and the breakdown of your phone system. Many companies ignore the importance of DNS management and leave it to their Internet Service Provider (ISP). By relying on your ISP for this service, you are unknowingly exposing yourself to continuous outages, affecting your website and the general accessibility of your online services. Outsourcing DNS to a specialized provider will increase your uptime and revenue while reducing the hidden soft costs of DNS maintenance.

## Why are ISPs Bad at DNS?

ISPs provide pipe services, Internet connectivity. They have set up their business to ensure they can carry packets across their network. That's what they lead with when they are out making a sale. Sometimes they happen to offer other ancillary services that they cannot bill, but these services, like DNS, are not specialties or areas of expertise. They are theoretical *value-adds*.

As a network operator, providing a highly available service such as DNS is not their core competency. Managed services like DNS are different from network engineering. While network services require their own expertise with routers and switching, this expertise rarely translates to expertise in services like DNS. DNS and other managed services are not only focused on the network availability but also server operating systems, software updates, load-balancing, customer interfaces, and physical server limitations.

Network operators work within an entire environment where they control everything on their network. Often times these operators are not familiar with the unique problems associated with DNS and other services. Online applications like DNS are world-facing by design and both security and denial of service attacks are more pressing concerns. Constant management is critical to their success, and those operating it need to be well versed in the appropriate techniques. Network operators, for example, are not necessarily familiar with critical software patches that must be implemented in a timely manner to ensure attackers can be fended off.

## No One is Watching

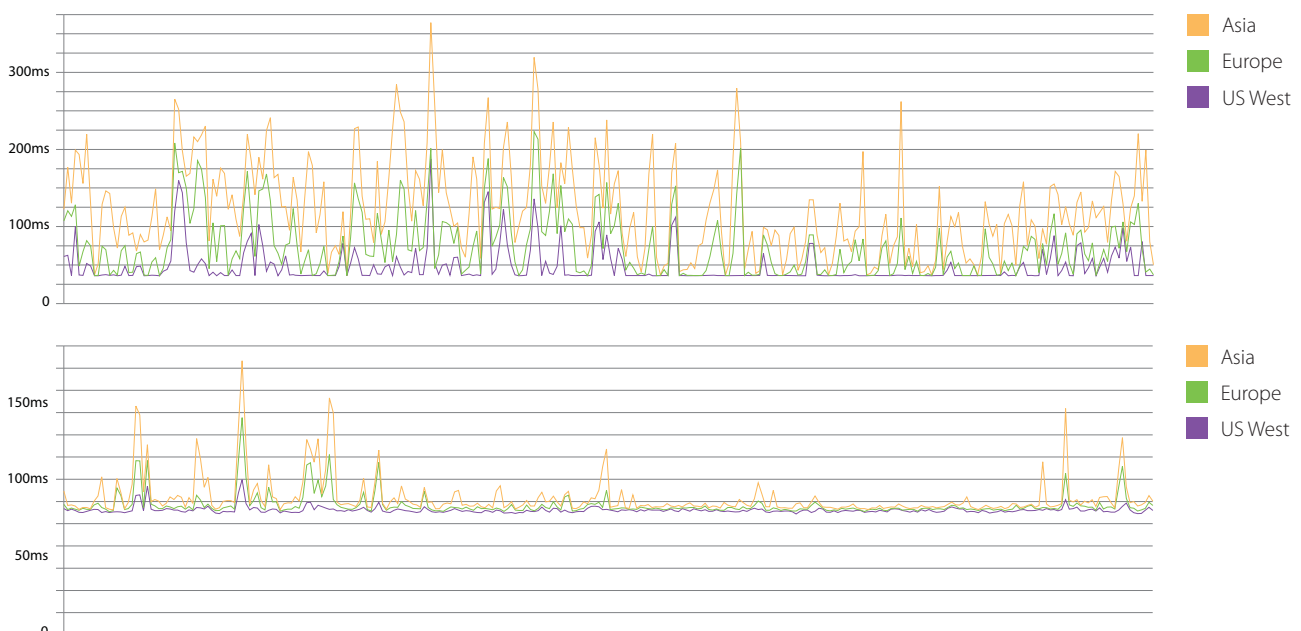
ISPs are excellent at measuring and monitoring within their network. It is their core business. But for DNS, this is often insufficient. ISPs generally have extensive monitoring for network pipe services but severely lack external monitoring, a key measure in DNS performance. Because of this, ISP-based DNS are subject to regular outages that take quite some time to be fixed.

ISPs also do not typically provide service level agreements (SLAs) for DNS. Without this customer safeguard, designed to protect and guarantee service quality, customers are left with outages and downtime without any recourse. ISPs seem to think that even a number of DNS outages will not make customers change who their network service provider is.

## What's Going Wrong?

Below you will find collected samples of DNS performance for two major ISP DNS servers, one that provides service for nearly 20,000 domains and the other that manages over 60,000. This monitoring was collected over several months for multiple transit providers and from multiple locations including Hong Kong, Palo Alto, Chicago, Washington DC, London, and Amsterdam. Represented here is an average day.

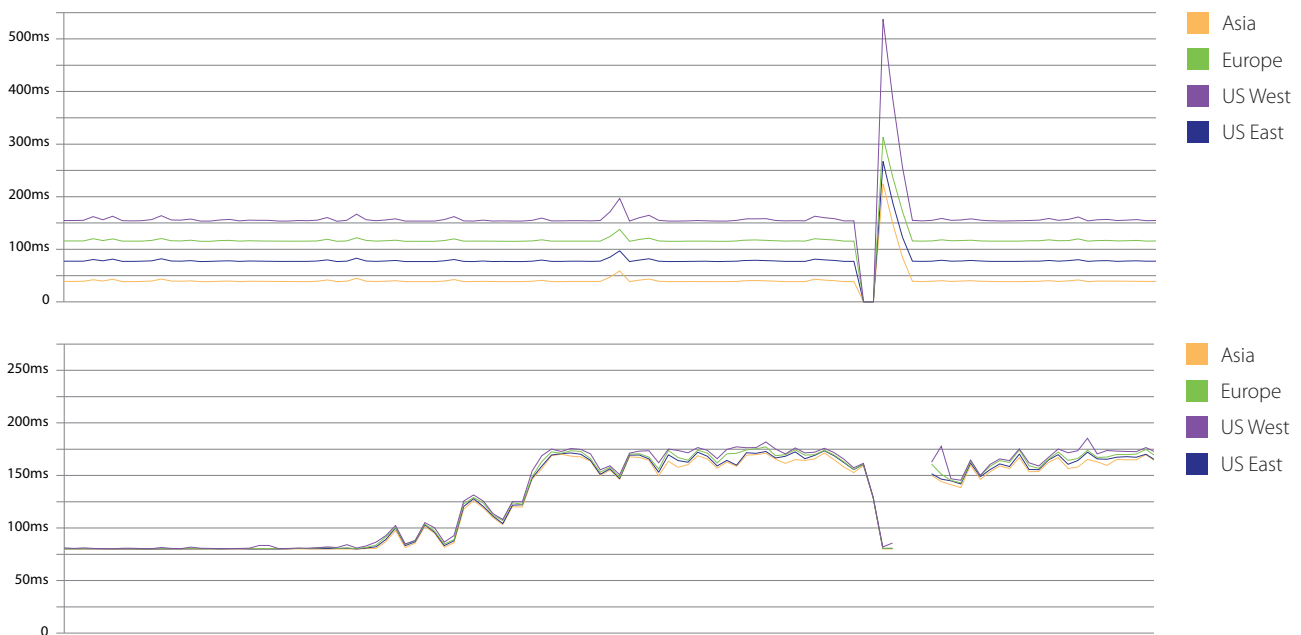
Looking at the graphs in *Figure 1*, one name server appears to be performing well while



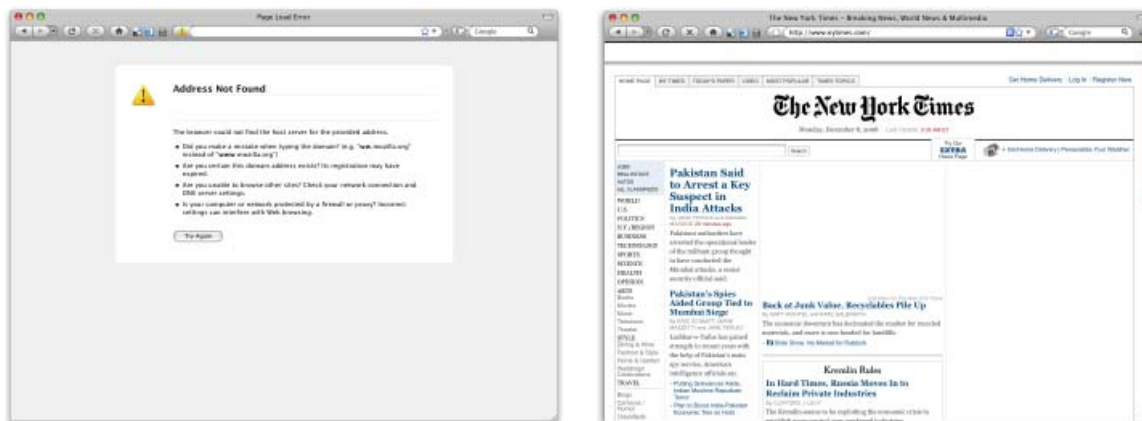
**Figure 1** – The data shows struggling performance, suggesting an under-powered box overwhelmed by requests.

the other struggles significantly. This severe difference in performance is probably due to an under-powered box overwhelmed by requests. Because of the wide variance of response time, users will notice. The DNS lookup process takes place at the beginning of the website experience, making it a critical component. Regardless of how many load-balancers and web servers there are, if your DNS lookup is slow, there is nothing to speed it up. It's an easy fix, but when the ISP is responsible, no one is watching.

The other provider in *Figure 2* has the classic *we-only-make-updates-every-12 hours* setup.



**Figure 2** – The name server restart causes an extreme increase in load speeds for the 5-10 minutes after each restart.



**Figure 3** – The results of ISP DNS. (left) A “404 Not Found” page displays because the name server is being reset, (right) nytimes.com loads slowly due to the restart of the name server.


Because of this, updates require the entire name server be restarted. This restart causes an extreme increase in load speeds for the 5-10 minutes after each restart as it unnecessarily reloads every single domain. While it is doing this, the average DNS response takes several seconds. That limit is far beyond the amount of time most users will wait on a search result page and causes potential customers to go on to other websites.


The results (See *Figure 3*) of either of these cases can cause the loss of revenue. Based on the data from *Figure 1*, the approximate minimum amount of latency is 50ms, while the average is approximately 120ms. Figure 100,000 users/day at 70ms of extra latency amounts to 7,000 seconds or 2 hours/day that people are waiting for your web page to load, all because of DNS. If that went away, imagine how much more revenue you could generate just because a user didn't bounce to another website.

## Off Net is Safer

Companies who earn their revenue online would be wise to consider having their DNS separate from their ISP network. DNS directs end-users and customers to important online systems. If the ISP hosting those services and providing DNS services has an outage, you would be unable to implement any high-availability or disaster recovery plans to route around outages.

## Not Customer Centric

With ISPs, DNS settings are often only loaded once or twice a day. This means that if an outage occurs on your network at 9:00am, it may not be fixed until noon.  With the *twice-a-day* update, the act of fixing that outage actually causes continued problems as the name server is restarted, problems and delays for both you and every other domain on that server.

Security for DNS changes is critical. Your domain name is a sacred piece of your Internet presence and the redirection of that domain name should be handled securely.  With ISP-based DNS management, this is not the case. The process for making these changes is lax and ripe for unauthorized individuals to make updates and cause outages. Some providers merely use web forms to submit a request or even tell their customers to email the changes. With this process, there is no way to verify changes are correct or authorized before they are implemented. If someone makes a mistake, they have to wait another 12 hours for the next reload.

## A Better Way

DNS is a technical service that is best outsourced to a specialized provider focused on the unique challenges and benefits of well-balanced DNS management. The Dynect<sup>SM</sup> Platform can eliminate those daily outages and help you realize a better way to manage your IT infrastructure at an exceptional value.

For more information about The Dynect Platform, please call a member of our sales team at 1-888-840-3258 or email us at [sales@dynect.com](mailto:sales@dynect.com).

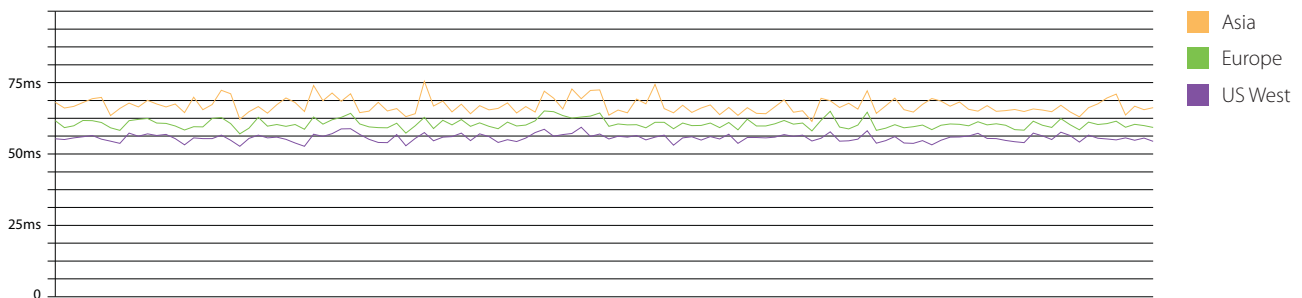


Figure 4 – Properly managed DNS name servers by Dynamic Network Services Inc.

