Position Summary:

THE CASE AGAINST ISP DNS

ORACLE® + Dyn

dyn.com ☎ 603 668 4998 150 Dow Street, Manchester, NH 03101 USA @dyn

Position Summary:

The Case Against ISP DNS

What Is DNS? Why Should You Care?

The Domain Name System (DNS) is the critical link for network services between human-readable names and computer addresses. DNS outages and misconfigurations cause website outages, email bouncing and the breakdown of your phone system. Many companies undervalue the importance of DNS management and default to bundled DNS services from their Internet Service Provider (ISP). Regrettably, by relying on an ISP for this service, businesses are likely exposing themselves to continuous outages and performance problems that will affect their websites and general accessibility of online services.

Moving DNS to a specialized provider will increase uptime and prevent revenue loss while reducing the hidden costs of DNS maintenance.

The Case Against ISPs

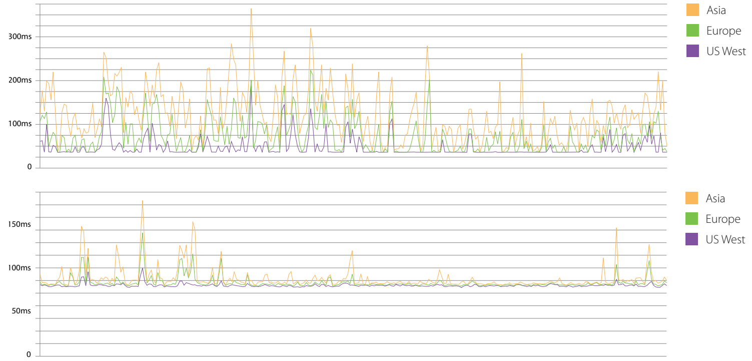
ISPs provide on-ramps for Internet connectivity and make money carrying traffic across their network and connecting their network to other internet networks. ISP sales teams typically lead offers with connection and transport services and then follow initial offers with other ancillary, non-billable services. However, these services (like DNS) are often not within an ISP's core competency.

this rarely translates to expertise in 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 environment where they control everything on their network and often, 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 (DDoS) attacks are more pressing concerns. Constant management is critical to their success and those operating need to be experts in the ever-changing technology of website uptime. Network operators are not necessarily familiar with critical software patches that must be implemented in a timely manner to ensure attackers can be fended off.

Regular Outages

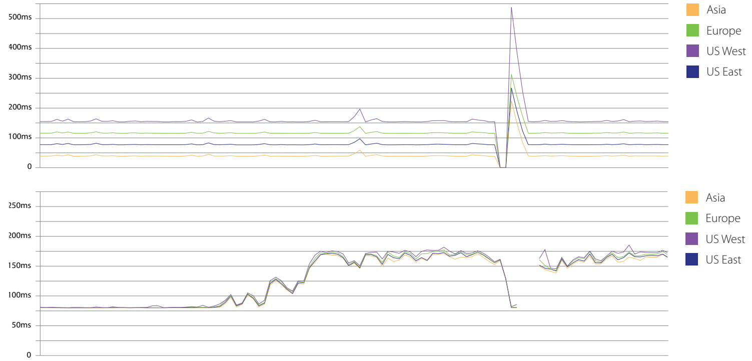
ISPs are excellent at measuring and monitoring within their network as it's their core business. For DNS, this is often insufficient. ISPs generally have extensive monitoring for network connection and transport services but severely lack external monitoring, a key measure in DNS performance. Because of this, ISP-based DNS is subject to regular outages that take a longer time to be identified, mitigated or fixed. ISPs also do not typically provide service level agreements (SLAs) for DNS. Without this customer safeguard, which is designed to protect and guarantee service quality, customers are left with outages and downtime without any recourse.

Figure 1



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

Figure 2



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

What's Going Wrong?

Here are collected samples of DNS performance for two major ISP DNS servers on an average day – one that provides service for nearly 20,000 domains and another 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, California, Chicago, Washington, DC, London, and Amsterdam.

In Figure 1, the US West name server is performing fine although the rest of the servers are struggling while the server in Figure 2 is struggling significantly due to a classic "updates every 12 hours" approach. This severe difference in performance is probably due to an underpowered box that is being overwhelmed by requests. Users will notice the wide variance of response time because the DNS lookup process takes place at the beginning of the website experience.

Regardless of how many load balancers and web servers there are, nothing can immediately speed things up when your DNS lookup is slow. It's an easy fix, but when the ISP is responsible, no one is watching. The aforementioned "updates every 12 hours" approach is faulty because updates require the entire name server to be restarted. This causes an extreme delay 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, resulting in revenue loss because of what you see in Figure 3.

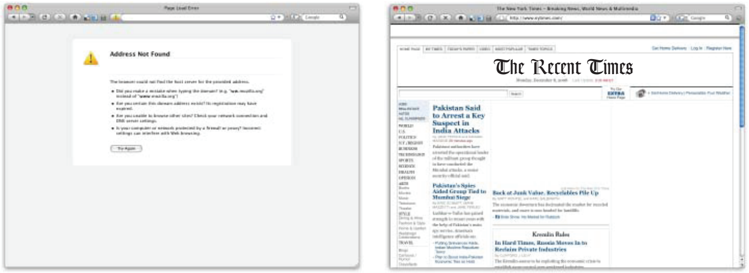
What’s Going Wrong?

Here are collected samples of DNS performance for two major ISP DNS servers on an average day – one that provides service for nearly 20,000 domains and another 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, California, Chicago, Washington, DC, London, and Amsterdam.

In Figure 1, the US West name server is performing fine although the rest of the servers are struggling while the server in Figure 2 is struggling significantly due to a classic “updates every 12 hours” approach. This severe difference in performance is probably due to an underpowered box that is being overwhelmed by requests. Users will notice the wide variance of response time because the DNS lookup process takes place at the beginning of the website experience.

Regardless of how many load balancers and web servers there are, nothing can immediately speed things up when your DNS lookup is slow. It’s an easy fix, but when the ISP is responsible, no one is watching. The aforementioned “updates every 12 hours” approach is faulty because updates require the entire name server to be restarted. This causes an extreme delay 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, resulting in revenue loss because of what you see in Figure 3.

Figure 3


Address Not Found
Try Again
The Recent Times
Pakistan Said to Arrest a Key Suspect in India Attacks
Pakistan's Spies Aided Group Tied to Mumbai Siege
Back at Junk Value, Recyclables Pile Up
Kremlin Rules
In Hard Times, Russia Moves In to Reclaim Private Industries

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.

Using the data from Figure 1, the approximate minimum amount of latency is 50ms, while the average is approximately 120ms. 100,000 users/ day at 70ms of extra latency amounts to 7000 seconds or 2 hours per day. That's a lot of time that people are waiting for your web page to load, all because of faulty DNS. If two hours of downtime disappeared, imagine how much more revenue you could generate and keep because a user didn't leave your site in frustration.

Well Performing Servers

50ms
Approximate Latency Minimum

120ms
Approximate Average

100k
Users/Day at 70ms + Latency

7k
Seconds or 2hrs/Day

There's Help

There DNS is a technical service that is best outsourced to a specialized provider focused on the unique challenges and benefits of enterprise-level DNS management. Dyn Managed DNS eliminates those daily outages and helps you realize a better way to manage your IT infrastructure at an exceptional value. With the top engineering minds in the business, a global anycast IP network and industry-leading uptime, Dyn is the go-to leader in managed/outsourced DNS.

Rethink DNS.

Oracle Dyn is global business unit (GBU) focused on critical cloud infrastructure. Dyn is a pioneer in DNS and a leader in cloud-based infrastructure that connects users with digital content and experiences across a global internet. Dyn's solution is powered by a global network that drives 40 billion traffic optimization decisions daily for more than 3,500 enterprise customers, including preeminent digital brands such as Netflix, Twitter, LinkedIn and CNBC. Adding Dyn's best-in-class DNS and email services extend the Oracle cloud computing platform and provides enterprise customers with a one-stop shop for infrastructure as a service (IaaS) and platform as a service (PaaS).

ORACLE® + Dyn

dyn.com   603 668 4998   150 Dow Street, Manchester, NH 03101 USA   @dyn