DNS THREATS TO NETWORK AVAILABILTY

By Jo Van Schalkwyk, Men & Mice

Network availability happens when IP meets DNS

What's your IP address? Chances are you don't know, but without your IP address contacting the IP address of the domain hosting this content, you and I won't be having this conversation. IP addresses, in short, are the phone numbers of the internet.

Since most people aren't that good at remembering large numbers, let alone the 32-bit (IPv4) or 128-bit (IPv6) numbers denoting IP addresses, the internet's forefathers were wise enough to devise a system translating alphabetic names into numerical IP addresses. So to catch up on the latest White House scandal, we can just enter the easy-to-remember name bbc.com into our web browser, instead of using the hard-to-remember IP address 212.58.244.71. The browser will automatically look into the internet 'directory' to figure out the correct IP address to 'call'.

This almost instantaneous IP address lookup is performed by the Domain Name System (DNS), which, for IP Addresses, works like a large and distributed directory. Whenever any of the billions of daily online requests for information or services are made, appropriate DNS servers spring into motion and answer queries, resolving IP addresses to names and establishing critical connections between those who provide products and services and those who use them.

When DNS fails

But what happens when DNS becomes unavailable? Well, quite simply, to the user it will appear as if the service they're trying to reach has vanished off the internet. Which, in its turn, can lead to absolutely disastrous repercussions for the providers of products and services. The hard costs of DNS failure, depending on aspects such as your organizational size, type of operations, critical data, backup and recovery systems and number of employees affected, can run up to anything between $55,000 in lost revenue per year for small enterprises, to upwards of $1,000,000 for large companies. The soft costs, such as loss of reputation and customer churn rate, can be just as devastating.

Critical as it is, DNS is also a remarkably vulnerable system, which makes it an attractive target for cyber criminals, often in the form of distributed denial-of-services (DDoS) attacks. A DDoS attack occurs when multiple compromised computer systems flood a server, website or other network resource with messages, connection requests or malformed packets. This slows down, or even crashes the service, rendering it useless for legitimate users or systems.

Late October 2016, Dyn, provider of DNS to high-traffic domains such as Twitter and Netflix, fell victim to the biggest DDoS attack to date. Making headlines everywhere, Dyn's devastating encounter with, amongst others, the Mirai botnet literally led to every IT team and their data center rethinking how they do DNS, and for good reason - Dyn had enjoyed a whole 8 years of 100% uptime before the 21st of October 2016.

DDoS attacks may be unpredictable, nasty and expensive, but they are not the greatest threat to network availability. Networks are still most vulnerable to simple human and mechanical error, a situation made worse by poor network architecture design and the lack of well-constructed and well-tested disaster recovery plans. Additionally, as technological disruption accelerates, the complexity of systems becomes inflated, requiring both a superior skilled workforce as well as increasingly sophisticated equipment.

In May 2017, British Airways (BA) discovered the glaring gaps in their network management the hardest way when a power outage at their main Heathrow data center left 75,000 passengers in 170 countries stranded for days. What most surprised people in the IT industry, and not the least BA themselves, was the complete failure of their back-up system to kick in.

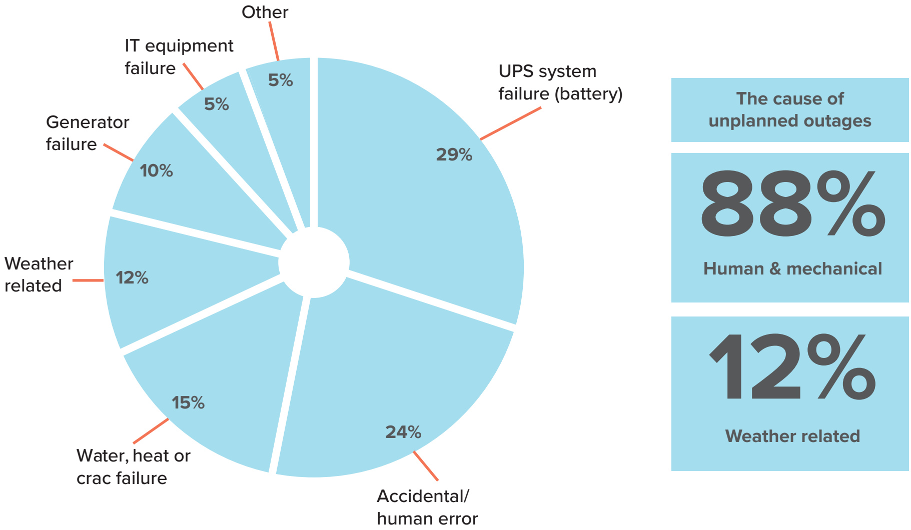

Figure 1 – The primary root causes of reported unplanned outages (source: data from Vertiv, formerly Emerson Network Power)

BA's woes serve as an unpleasant, but urgent, reminder that the way we back up our systems is sometimes even more critical than how we run it day-to-day. As it goes with life insurance or a last will and testament, there's no point in waiting until your plane goes down (or fails to go up) before you start getting your house in order.

Keeping your DNS up and running, always

In the last decade or so, the creation of anycast technology and large-scale cloud services have allowed companies to transfer the risk and complexity of running their own DNS, to the generally much better network availability, load distribution and systems back-up of highly specialized DNS service providers.

Yet, as seen in the case of Dyn, putting all your DNS availability eggs in one DNS basket, however specialized it is, is not necessarily the most secure solution. Looking at the odds and costs of outages, many enterprises are now opting to bring in a second, or even a third, DNS service to hold copies of critical DNS master zones. That way, if your sole source of external DNS is knocked out due to power failure, human error or malicious cyber activity, this critical service is still active, ensuring service continuity and retaining critical operational data – and if you're BA, keeping your passengers happy in the air, instead of sleeping on yoga mats in conference centers.

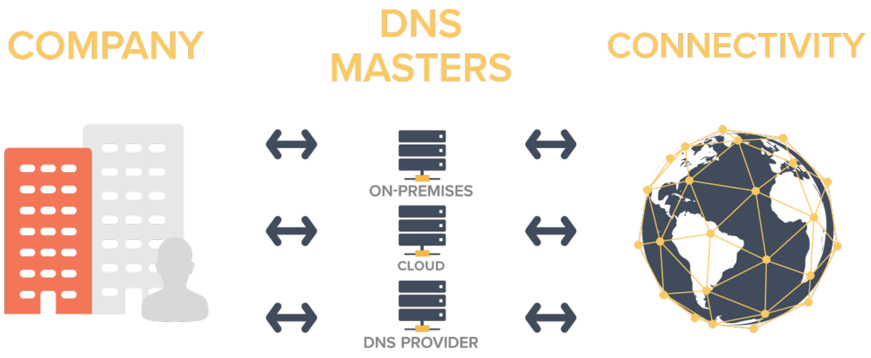

Figure 2 - External DNS redundancy

This system of external DNS redundancy boosts DNS availability by:

1. removing the danger of exposure to a single point of DNS failure.
2. reducing traditional master-slave DNS redundancy vulnerabilities, where slave zones can't be changed if the master becomes unavailable.
3. improving infrastructure resilience by hosting critical zones with multiple providers, ensuring continued service availability and updates of changes if one DNS service provider becomes unavailable.

Additionally, maintaining redundant DNS at more than one provider helps you to avoid the pitfalls of vendor lock-in.

How to multi-DNS: Think compatibility across platforms, think automation

In theory, DNS redundancy across multiple DNS service provider platforms should be the best solution for optimal DNS high reliability, high availability and high performance. In practice, however, the complexity of tasks and scope for error involved in replicating and maintaining identical DNS zones on multiple platforms pose additional threats to DNS availability. The situation is made worse by:

- A lack of centralized views
- A lack of workflow automation
- The difficulty of coordinating multiple platform APIs

Maintaining and keeping DNS records in sync in multiple host locations is complicated, but can be done using APIs or custom applications. However, it's important to choose DNS service providers that offer similar functionalities and are able to operate in a collaborative setting. Also consider the global points of presence (PoP) of the providers, the quality of their APIs and reporting tools and their performance in different locations and under varying server load. You want to be able to deploy your multi-DNS on different networks - your service providers should be capable of seamless integration through APIs or custom programs. To reduce complexity and ease the replication and synchronization of data across multiple DNS platforms, it also pays to explore third-party solutions such as Men & Mice's xDNS redundancy.

The bigger picture

Apart from covering all your bases by deploying well-architectured multi-DNS, it's worth taking a look at other ways of mitigating DDoS and preventing DNS failures at large. Geoff Huston made an impassioned plea for stepping up DNSSEC deployment at RIPE 73 and DPRIVE, the DNS PRIVate Exchange Working Group, is working on developing mechanisms to enable the confidentiality of DNS transactions. Other groups, such as the Internet Society, are charting a number of initiatives, aimed at, for instance, creating a more secure environment surrounding the Internet of Things.

It is said that the price of freedom is eternal vigilance. Making the internet more secure, but keeping it an open and free network of networks, without any single entity exercising centralized control, will require collective solutions and a collaborative security effort. We better get started, if we haven't already.