xDNS

MEN&MICE

SECURE YOUR DNS ACROSS MULTIPLE DNS SERVICE PLATFORMS WITH MEN & MICE xDNS REDUNDANCY

White Paper

INTRODUCTION

What happens when DNS becomes unavailable?

Quite simply, to the user looking for a product or service, it will appear as if the company they're trying to reach has vanished off the face of the earth. In this customer-oriented era, where companies are becoming utterly dependent on the speed and convenience of eternal connectivity, being unexpectedly off-line can equal digital death and lead to significant business disaster.

THE DNS CHALLENGE

DNS (Domain Name System) is the most critical aspect of any network's availability. When DNS services are halted, or slowed down significantly, networks become inaccessible, leading to damaging losses in revenue and reputation for enterprises.

To ensure optimal network availability, many enterprises depend on top-tier managed DNS service providers for their external DNS needs. The basic "table stakes" characteristics of an enterprise-class managed DNS service are high reliability, high availability, high performance and traffic management. However, even the most robust DNS infrastructure is not immune to outages.

Outages may be localized, in which only certain DNS servers in the network are not responding, or, less commonly, system-wide. A system-wide DNS failure can take an entire business off-line - the equivalent of power failure in every one of their data centers.

To prevent this, top-tier managed DNS systems have a great deal of built-in redundancy and fault tolerance, yet the danger of a single point of failure remains for enterprises that rely solely on a single-source DNS service.

If no system of DNS is failure proof, this begs the question: what should an enterprise do about it?

USING MULTIPLE DNS SERVICE PROVIDERS FOR ULTIMATE DNS REDUNDANCY

DNS availability statistics for managed DNS providers show that the industry norm exceeds 5 nines (99.999%) uptime. This is the equivalent of about 5 minutes per year downtime. However, this top line number does not provide any detail on the impact of degraded performance, or the cascading effect of a system-wide outage of various duration, on individual enterprises.

To discover the true impact of a potential loss of DNS availability, enterprises need to properly assess the business risk associated with relying on a sole source provider, and compare that with the cost of a second source DNS service. What would a 30-minute loss of DNS cost the business in terms of revenue loss, reputation damage, support costs and recovery? What does it cost to maintain a second source DNS service?

Research amongst enterprises for whom online services are mission critical generally concludes that the cost ratios are in the range of 10:1 – one order of magnitude. Put another way, the cost of one outage is roughly estimated to be ten times the annual cost of a maintaining a second service. A business would have to have second source DNS for ten years to equal the cost of one major DNS outage.

Looking at the odds and costs of outages, many enterprises are opting to bring in a second, or even a third, DNS service to hold copies of critical DNS master zones (Diagram 1). 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.

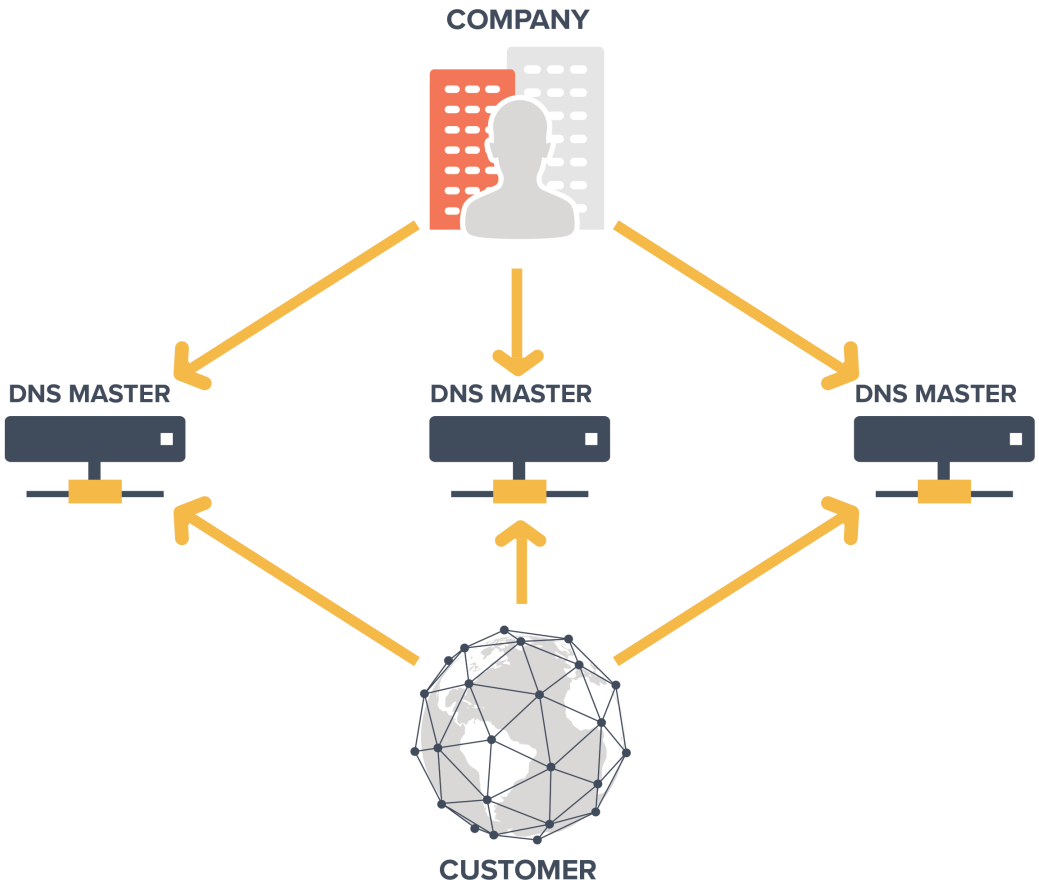

Diagram 1: External DNS redundancy

THE RISKY BUSINESS OF MAINTAINING DNS REDUNDANCY ACROSS PLATFORMS

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

This inability to view, synchronize and update identical zones' data simultaneously can, in itself, lead to errors and conflicts in DNS configuration and result in a degradation of network performance, or even a network outage – the very events that multi-provider DNS redundancy is intended to prevent.

PROTECT YOUR DNS ON MULTIPLE PLATFORMS WITH MEN & MICE xDNS REDUNDANCY

Breaking new ground in the battle against DNS disruption, the Men & Mice xDNS redundancy feature provides the abstraction level necessary to replicate and synchronize critical DNS master zones across multiple DNS service provider platforms, on-premises, in the cloud, or in hybrid or multi-cloud environments.

Men & Mice xDNS provides a unified view and centralized management of DNS data, regardless of the DNS service provider platform. Network administrators and other authorized users can use xDNS to perform necessary updates to their network's DNS, as well as benefit from building automation with the powerful Men & Mice API, instead of having to dig around in different DNS platforms and deal with coordinating conflicting APIs.

Combined with the flexibility of building automation on top of the Men & Mice Suite, xDNS offers you the freedom to better distribute your DNS load based on zone priority, performance requirements and accompanying costs. With xDNS, you are better equipped to steer the tiered price points of externally hosting, for example, critical high-performance or less essential low-performance zones, and utilize the DNS service best suited to your situation at a given time.

HOW xDNS REDUNDANCY WORKS

Using the Men & Mice xDNS feature, create a zone redundancy group by selecting critical zones from DNS servers and services such as BIND, Windows DNS, Azure DNS, Amazon Route 53, NS1, Dyn and Akamai Fast DNS.

Once an xDNS zone redundancy group has been created, xDNS assists the administrator in creating identically replicated zone content, resulting in multiple identical master zones. Additional zones can be added or removed from the xDNS group as required.

All changes initiated by the user through Men & Mice, both the UI and API, will be applied to all selected zone instances in the group, as configured in the sync policy. All changes made externally to the selected zones existing in the xDNS group, will be synchronized to all zones in that particular xDNS group. However, zones that are not selected will act as "read only" and only receive updates done through the Men and Mice Suite or when the zone itself is modified externally, for example through its corresponding cloud portal. Additionally, if DNS record conflicts arise, xDNS will alert the user and provide an option on how to resolve conflicts before the group is re-synced.

If an xDNS zone is not available for updating, for instance if one DNS service provider experiences an outage, that zone will be marked as out-of-sync. Once the zone becomes available again, it will be automatically re-synchronized and will receive all updates that were made while the DNS service was unavailable.

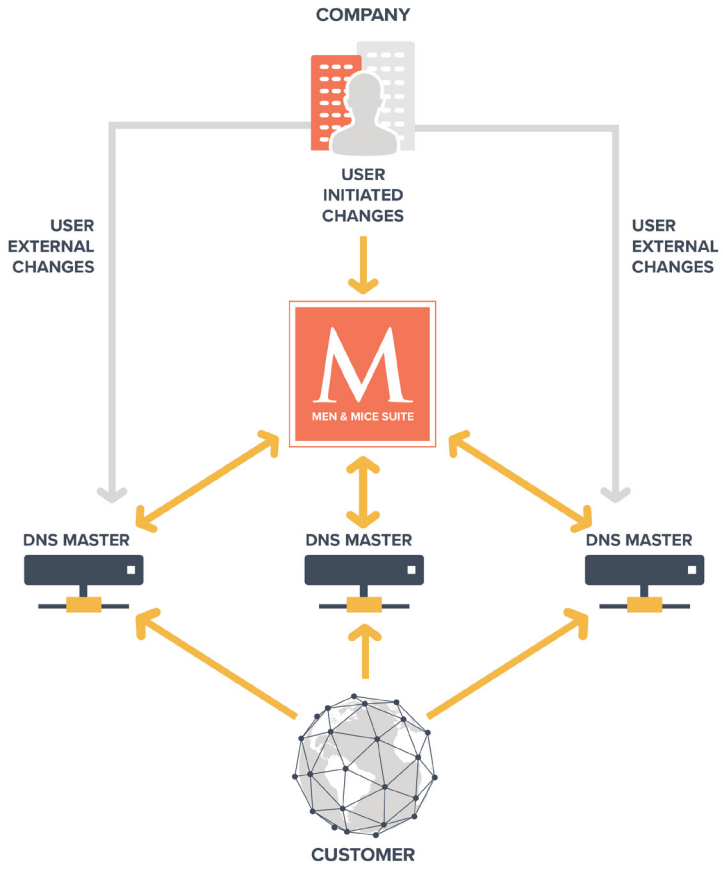

Diagram 2: xDNS redundancy

CONCLUSION

With the Internet of Things spurring on the pace of what has become known as the Fourth Industrial Revolution, the need for maintaining uninterrupted network uptime is becoming critical to business success. Leveraging multiple managed DNS services to ensure optimal DNS redundancy is quickly becoming the clear best practice for enterprises of all sizes.

Yet DNS redundancy, a great concept on paper, is proving a daunting challenge in practice. Men & Mice xDNS provides a simple way for companies to manage their DNS on multiple external platforms, with the Men & Mice Suite software automatically taking care of the replication and synchronization of data in a reliable and consistent manner.

Men & Mice xDNS takes the 'daunt' out of maintaining external DNS redundancy, providing the centralized views and control necessary to reduce the risk of network exposure to a single point of failure, improve network reliability and performance and bolster the successful mitigation of DDoS attacks and other potentially harmful DNS incidents.

Men & Mice
Hlidasmari 15
IS-201 Kopavogur
ICELAND

Tel: (Iceland) +354 412 1500
Tel: (USA) 1 (800) 616 3840
menandmice.com
sales@menandmice.com