THE COST OF FREE:

How much are you REALLY paying for Microsoft DNS?

BLUECAT™

bluecatnetworks.com

If you've played Jenga before, then you know how Microsoft's Domain Name System (DNS) plays out as networks evolve.

Everything starts out in perfect alignment. The structure is simple, but it holds together well.

Over time, the foundation starts to erode. Pieces of critical infrastructure are moved around. A new network region here, a hundred new employees there – each layer of complexity puts new strains on the system. Mergers and acquisitions create an awkward tangle of network pathways. New security layers lead to additional complications.

You know what's coming, and try to avoid it. You patch. You reallocate resources. You hire more system administrators to manage an increasingly unstable architecture. You build an entire organization to manually respond to network demands.

Then it happens – the moment of reckoning.

Administrators spend so much time fixing zones and domains that they have little time for their "real jobs". Downtime slows ordinary business functions to a crawl. Domains get stuck in a circular resolution process through overlapping regions and zones. An inflexible network architecture makes new initiatives either too costly or impossible. Poor visibility leads to compromises on security.

The costs of Microsoft DNS may start as a slow drip, but at a certain point they become a torrent that threatens network stability and constrains strategic initiatives.

The costs of Microsoft DNS may start as a slow drip, but at a certain point they become a torrent...

How can network administrators and CIOs keep their networks from reaching this problematic state?

In this eBook, we'll examine the true cost of Microsoft's "free" DNS by looking at the business implications and hard numbers associated with a dysfunctional network architecture.

The Domain Name System (DNS) lies at the core of every network. DNS acts as the "phone book" for every query, channeling traffic to its proper destination.

Most networks start with a simple, easy to administer architecture. Administrators just want to get the system running with as little expense as possible. It's not surprising, then, that so many network administrators go with Microsoft as the default service for DNS. Microsoft's DNS tools are free, and at a basic level they work.

This early in the game, few IT administrators have a long-term perspective on how Microsoft DNS will constrain business initiatives or ultimately weaken their system architecture. Enabling strategic business initiatives and managing network complexity don't even appear on the radar.

Over time, the business logic of sticking with Microsoft DNS will gradually erode for any organization. Microsoft DNS is included in the standard toolkit, but that means that it only handles standard tasks. As organizations evolve, they need a DNS management system that can handle changing requirements and increasing complexity. If administrators don't pay close enough attention to the infrastructure needs that underpin these changes, the network can quickly slide into dysfunction. In this context, the cost of remaining with Microsoft can be quite high.

DOWNTIME BY THE NUMBERS

In a 2016 study, companies surveyed reported an average of five downtime events each month, with the cost of each downtime event ranging from $1 million a year for a typical midsize company to more than $60 million for a large enterprise.[1]

Tactical Constraints

SLOW ZONE TRANSFERS

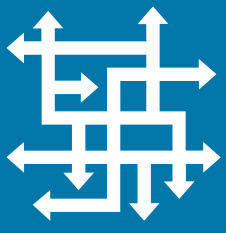
Complex, overlapping zones in Microsoft DNS often lead to latency and dropped connections. It can sometimes take several hours for IP address changes to filter through a Microsoft-based DNS schema spread across multiple regions.

STALE RECORDS

When network complexity reaches a critical point, Microsoft tools can produce a DNS database that is never fully up to date. Changes are quickly overcome by events in other zones, resulting in a continuous circle of updates that never fully resolves.

NO ERROR PREVENTION

As DNS complexity mounts, the slip of a finger can result in misdirected traffic that snowballs through chains of connected servers. Microsoft's DNS tools have no mechanism to identify or correct the source of a "fat finger" issue. Tracing the origin of a problem can result in hours or days of downtime.



COMPLEXITY

Many standard tasks in Microsoft DNS environments are onerous, increasing the probability of human error, poor service, and outages. Without centralized and automated management capabilities, updates require hands-on support from IT support personnel.

Strategic Constraints

DEV OPS

Agile operating environments require a flexible, easily adaptable network architecture. Testing new iterations of software, creating temporary zones for a development push, and de-provisioning unneeded parts of the network, are all difficult to accomplish on the fly in an admin suite reliant on Microsoft DNS.

AUTOMATION

Automation eliminates manual processes that used to consume IT departments. Unfortunately, Microsoft DNS tools do not support automation in any form, hindering the automation of business processes like the ability to stand up and tear down domain names quickly or leverage APIs.

SECURITY

Microsoft's DNS tools were not built with security in mind, even though an estimated 91% of malware uses DNS to maneuver through target networks. When a breach or incident occurs, the patchwork nature of Microsoft DNS makes it difficult for network administrators to identify, isolate, and mitigate harmful activity.

Microsoft DNS Horror Stories:

The Nuclear Football

"We're one of the world's largest brands. We operate in 150 countries with 150,000 employees. Yet, just three network admins manage Microsoft changes using specially assigned laptops. They refer to these laptops as their 'nuclear football'. Once someone mistakenly deleted a zone that took out the intranet and Exchange for half a day. As most don't know, there is no 'Delete Undo' function in Microsoft DNS so it was lost altogether. Had they not had an off-line copy in the lab, they would not have been able to restore those critical applications."

Information Technology Director,
Multinational Manufacturer

The MacGyver Delusion

MacGyver was famous for working his way out of any jam. He could escape from a maximum security facility with little more than duct tape, a Swiss army knife, and dental floss.

Some savvy network administrators think they can MacGyver their way around the shortcomings of Microsoft DNS. They devise tools and work-arounds. They conjure up hybrid solutions that integrate BIND and other "flavors" of DNS on top of a Microsoft foundation.

Yet these tend to be short-term patches rather than long-term solutions. Custom software layered on top of Microsoft DNS may have the appearance of a well-oiled machine, but there are significant risks in pursuing this strategy.

RISK #1: PASSING THE STRESS TEST

Adapted Microsoft DNS solutions may work reasonably well during a time of normal operations, but they quickly fail during times of stress on the network. A surge in network traffic, DNS routing errors caused by human error, or integration with a new network tool – all of these can bring a patchwork solution to its knees.

RISK #2: THE COST OF ADAPTATION

Like the Microsoft DNS tools they are built on, work-around solutions lack the flexibility to adapt to an increasingly complex network. When DNS practices start to diverge on different parts of the network, or if a different variety of DNS management comes into the picture (through an acquisition, for example), custom solutions based on Microsoft DNS will consume resources and time to adapt to the new situation.

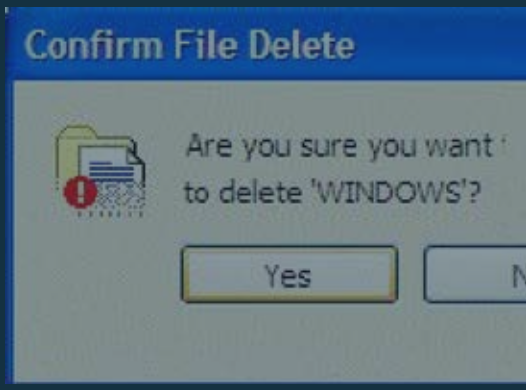
RISK #3: TURNOVER

Microsoft DNS work-arounds also have a single point of failure – the person or team responsible for creating them. If the one knowledgeable person in Microsoft DNS leaves the organization, the work-around they created suddenly becomes endangered. Any change in network architecture might require the creation of a new tool, or a costly adaptation of the existing one.

RISK #4: THE COST OF INTEGRATION

Patchwork solutions are never seamless. Building new layers on top of Microsoft DNS inevitably creates more complexity and a greater chance of something slipping through the cracks. The cost of developing, managing, and deploying these integrations over time can add up quickly.

In the end, work-arounds, patchwork solutions, and hybrids end up demonstrating the need for a comprehensive resolution to the fundamental problems of Microsoft DNS. They are not a long term solution. They merely delay the inevitable move to a more systematic, unified approach.



Microsoft DNS Horror Stories:

I deleted EVERYTHING

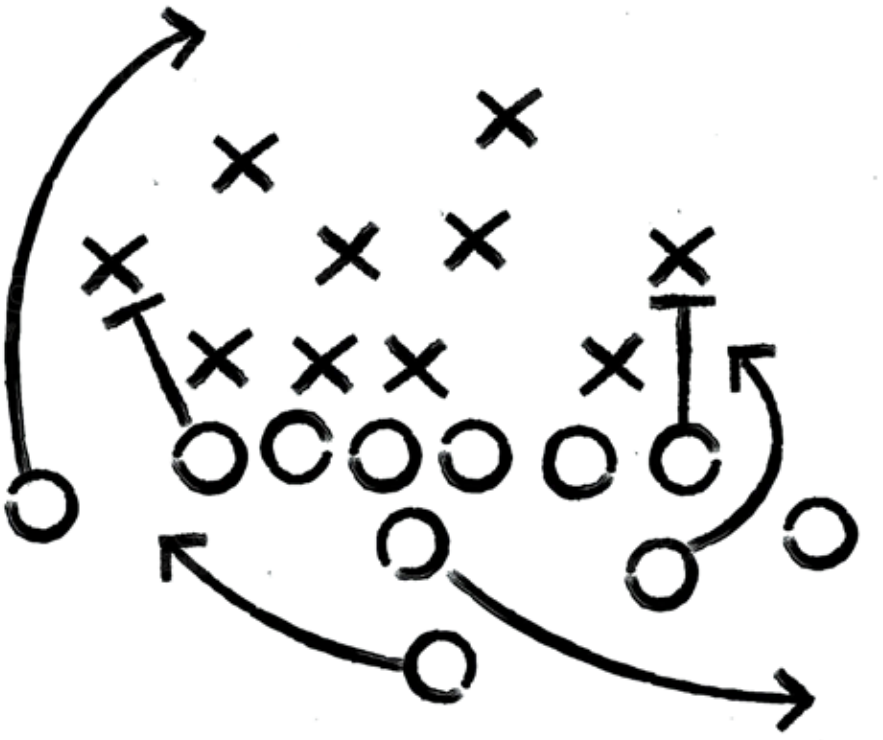
"I did a deployment and it deleted EVERYTHING... Then I had no choice but to sit there while it rebuilt everything. In the meantime, Active Directory (AD) replicated all the delete operations to the other Domain Controllers (DC) and all the DNS data magically disappeared from AD. I ended up with an outage of nearly an hour!"

Sr. Network Engineer, University

Migration Challenges and Opportunities

Despite the well-documented shortcomings of Microsoft DNS, risk-averse network administrators are often reluctant to move away from it. Migrating to any new network system comes with risks and potential costs; DNS management platforms are no different. Many Microsoft DNS customers rightly fear the ripple effects from a disruption of this core service.

At a certain point, the risks of continuing with Microsoft DNS start to outweigh any concerns with migration, but there are also ways to minimize risk. With a measured, clearly mapped out strategy to move DNS into a centralized management system, migration from Microsoft DNS can be accomplished with few hiccups.



Changing from one DNS management system to another can be stressful, but it can also yield concrete dividends. Here are just a few things a network administrator can expect to have visibility into when switching from a Microsoft DNS system to a unified management platform:

ORPHANED DATA

As Microsoft DNS architectures evolve, information inevitably gets lost in the shuffle. A unified DNS system will show network administrators these "bridges to nowhere", allowing the network to once again encompass the entire universe of available data.

INACCURATE DATA

When DNS records are misconfigured, stale, or incorrectly deleted, network traffic comes to a halt. A single point of truth for DNS data can identify these broken resolves, correcting (or at least identifying) inaccurate information to keep queries humming.

OVERLAPPING DATA

Redundancy has its merits in network administration, but there is a limit to its usefulness. Active management of a DNS system allows system administrators to reduce the inefficiency of overlapping information.

NON-STANDARD DATA

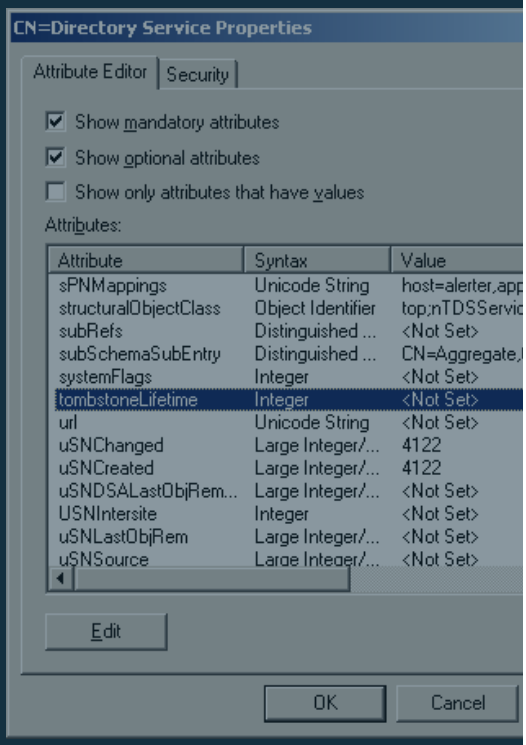
To achieve maximum performance, DNS architectures need standardized rules and procedures throughout the network. Active management of DNS allows administrators to eliminate non-standard data which can derail normal operations.

INEFFICIENT DEFINITIONS

As the complexity of DNS architecture grows, queries can be routed in odd ways that negatively impact network performance. A DNS management platform provides administrators with the strategic view they need to streamline operations.

DOWNTIME BY THE NUMBERS

Service provider problems and internal human errors each make up nearly 25% of downtime.[2]



Microsoft DNS Horror Stories:

Data still lurks

"Delete operations don't actually delete the data, as you would expect. Data still lurks there until Active Directory (AD) purges the data as part of the tombstoning process. In the meantime, it adds all the records again as new AD objects, so your AD object database grows massively with every deployment."

IT Systems Administrator,
Major Retailer

Quantifying the Cost of "Free"

Microsoft DNS tools are included with the standard network package, but that doesn't make them free. As networks scale and evolve, the constraints of Microsoft DNS become significant. They also become quantifiable – measurable in terms of administrator hours, downtime, and likelihood of a security breach.

At BlueCat, we've helped hundreds of organizations move from Microsoft DNS to a flexible, automated, intuitive DNS management system that meets their needs. In the process, we've learned a lot about the true cost of Microsoft DNS, both at the tactical level and the strategic level.

What is your organization actually paying for Microsoft DNS?

We've developed a calculator that provides IT administrators and CIOs with hard numbers about the business cost of the status quo. With baseline knowledge about your IT operations, we can provide you with instant feedback. You even have the option of sharing the information with BlueCat to start a conversation about how an Enterprise DNS solution can add value to your organization.

Let's Get Started!

[1,2] https://www.networkcomputing.com/networking/high-price-it-downtime/856595126