DNS/DHCP: Why Users Prefer Appliances

IT Professionals Discuss DNS/DHCP Appliance Advantages over BIND and Microsoft Active Directory Services

By:

Jon Oltsik
Enterprise Strategy Group

October 2005
# Table of Contents

Table of Contents .............................................................................................................. .......................................i  
List of Figures ................................................................................................................ ...........................................i  
Executive Summary .............................................................................................................. .................................. 2  
The Network Is the Business .................................................................................................... 2  
Network Identity Infrastructure, a Ticking Time Bomb ................................................................. 3  
  - Traditional BIND Is No Longer the Right Solution................................................................. 3  
  - Microsoft DNS/DHCP Does Not Fill the Void....................................................................... 5  
Alternatives for DNS/DHCP ...................................................................................................... 5  
  - Appliances Simplify DNS/DHCP Management................................................................. 5  
  - DNS/DHCP Appliances Are Networking Devices ............................................................. 6  
  - Security Concerns Favor DNS/DHCP Appliances.............................................................. 6  
  - IT Wants Advanced Management Functionality for DNS/DHCP .......................................... 9  
  - DHCP Requirements Are Also Important......................................................................... 9  
Final Analysis ......................................................................................................................... 10  

# List of Figures

Figure 1. Typical DNS-Practices Cannot Meet Business Requirements........................................... 4  
Figure 2. DNS/DHCP Appliances Support Organizational Requirements ......................................... 7  
Figure 3. The Impact of Sarbanes-Oxley on Security Investment and Resources............................. 8  
Figure 4. Users Describe Microsoft Weaknesses and Infoblox Benefits .......................................... 11  

---

The Enterprise Strategy Group, Inc.  
20 Asylum Street, Milford, MA 01757 • 508-482-0188 • www.enterprisestrategygroup.com / info@enterprisestrategygroup.com
Executive Summary

Ask any seasoned networking professional and he will tell you that while corporate DNS/DHCP services are mission-critical they tend to receive minimal attention. This negligence is no longer tolerable -- businesses depend upon the network for access to data center resources, web-based applications, and IP phones; and, network availability depends upon DNS/DHCP. Over the next few years, large and small organizations will finally give DNS/DHCP its due as:

- **Companies give ownership of DNS/DHCP to networking groups.** A big reason for DNS/DHCP neglect in the past was that these services sat somewhere between UNIX and Windows administrators and the networking group. ESG believes that companies will move the care and feeding of DNS/DHCP exclusively to networking as these services anchor network architecture, administration, and service levels.

- **Business needs demand an alternative to legacy BIND.** BIND is clearly the workhorse name server platform but the old nag has gotten a bit long in the tooth. To meet dynamic business requirements, large organizations will implement a new generation of appliance-based DNS/DHCP systems offering superior availability, security, and reporting capabilities while providing for ease-of-use administration.

- **Users see DNS/DHCP appliances as a worthy alternative to Microsoft.** While Microsoft bundles DNS/DHCP in Windows Server software as an essential component of Active Directory, users describe major shortcomings in Windows DNS/DHCP’s ability to meet business and regulatory compliance needs. As a result, many organizations are willing to pass on Microsoft’s “free” DNS and DHCP and invest in a robust appliance-based DNS/DHCP infrastructure as part of their AD rollout.

To research this report, ESG interviewed numerous IT and network managers responsible for DNS/DHCP services. These individuals came from various industry segments including federal government agencies, local/state government agencies, healthcare companies, and high-tech manufacturing companies.

The Network Is the Business

Ten years ago, the Internet was a technology and cultural phenomenon, prominently featured as a trendy topic the business press. The buzz has since subsided. The Internet is taken for granted, but it continues to have a profound impact on our daily business lives and its use and pervasiveness continues to grow exponentially.

In support of this growth, worldwide telecommunications providers and enterprise companies will spend approximately $60 billion on networking equipment in 2005 (source: ESG). Investments in networking gear will continue as companies build new Internet-based applications and business processes that drive revenue and boost productivity. In this climate, the network must be highly available, scalable and flexible to meet ever-changing business needs.

In this era of network-based business processes, downtime can have a profound financial impact. ESG estimates that downtime carries a financial loss of $50,000 or more per hour at 15% of all U.S.-based businesses. For example, a leisure travel company claimed that it drove $410 million in revenue through its 7/24 call center operations. An hour of downtime for this company would cost $46,804!

Clearly, there is a balancing act here. Of course companies will continue to implement new applications and network infrastructure that help them drive revenue and cut costs, but these investments must be supported simultaneously with processes, management tools, and network services that help minimize unplanned downtime.
Network Identity Infrastructure, a Ticking Time Bomb

The massive investment in networking and telecommunications equipment reflects the fact that business and government leaders understand the impact of IP networks on modern society. In spite of this, many organizations spend little time or money on the network identity infrastructure that provides critical network Domain Name System (DNS) or Dynamic Host Configuration Protocol (DHCP) services required to keep the network running.

What do these services do? In simple terms, DNS acts an Internet phone book of sorts that maps human readable names like www.google.com into a 32-bit IP addresses (IPV4) like 66.102.7.99 and visa versa. DHCP is a communications protocol that lets network administrators centrally manage and hand out IP addresses to users on a network. If DNS or DHCP services are unavailable, users are unable to access network services like web sites, e-mail, and business applications.

Given the strategic importance of the network, common wisdom suggests that companies would consider DNS/DHCP as 'gotta-have' services like electricity, HVAC, and telecommunications. Ironically, this is not the case. Many organizations are guilty of slacking on DNS/DHCP management. It is not unusual to see Fortune 500 companies controlling DNS/DHCP with an ad-hoc collection of systems, processes, and DNS/DHCP software revisions (see Figure 1). Typically, these include:

- **A lack of ownership and accountability.** Many firms report that DNS/DHCP lives in an organizational “no-man’s land.” Numerous companies run DNS/DHCP on UNIX or Windows hardware and divide administrative tasks between UNIX and networking administrators. This split ownership can lead to turf wars, negligence, security problems, and unanticipated downtime. When the UNIX group takes a name server off-line for monthly maintenance, they may inadvertently disconnect users or interrupt application traffic in the process. Additionally, a lack of reporting and auditing tools means that it may be difficult or impossible to meet regulatory requirements like Sarbanes Oxley.

- **Minimal resources or skills.** With DNS/DHCP management in a frequent state of organizational flux, IT professionals have little motivation to bone up on their skills. As a result, many shops have one or two “go-to” people to baby sit DNS/DHCP. This creates a risky situation where a few IT staffers are ultimately accountable for maintaining network availability to thousands of employees.

- **Manual management processes.** Organizations with complex distributed networks made up of tens of thousands of devices still keep track of IP addresses in PC-based databases and spreadsheets. This makes the process of assigning unique IP addresses, managing subnet ranges, and keeping track of devices an operational nightmare. Administrators inundated with a backlog of moves, adds and changes must sacrifice tons of man-hours to keep pace.

These fundamental problems present an unavoidable scenario - it is only a matter of time until DNS/DHCP issues or security attacks lead to a network failure. The results can be costly as an hour of network downtime can result lost revenue and productivity.

**Traditional BIND Is No Longer the Right Solution**

The most popular tool for DNS is the Berkeley Internet Name Domain (BIND) which is currently in release 9.3.1. About 75% of Internet-based name servers run BIND as of July 2005 (source: ISC). BIND is a mature, robust
name server platform but deploying it on general purpose Microsoft Windows, UNIX or Linux platforms won’t meet today’s business needs. Why? Several reasons:

- **BIND has become too complex for most shops.** BIND administration is based upon the manipulation of arcane text files for updating configurations, host names, IP addresses and zones. Because of this, BIND can be very unforgiving where even a small error can cascade throughout the network interrupting critical services. In addition, BIND servers must be updated from time to time to fix security vulnerabilities. Patching dozens of name servers is a challenge, even for organizations with large IT operations groups. In fact, only a small percentage of organizations run the most up-to-date version of BIND because of the disruption associated with patching a server.

- **Mixed BIND can lead to interoperability problems.** Since DNS infrastructures are widely distributed, many companies maintain a mix of BIND servers ranging from version 4 through 9. This can quickly turn into a management nightmare as a simple change may require DNS administrators to painstakingly update records on each server.

- **Commercial server platforms present security and operational challenges.** Typical BIND implementations run on UNIX or Linux systems. These server operating systems need continuous care and feeding like locking down configurations, patching vulnerabilities, and upgrading to new OS revisions. This adds up to a lot of maintenance - and downtime - over the life of the system.

In summary, BIND can’t meet today’s dynamic business needs because administration is costly, complex, time consuming and prone to accidents. As one user clearly stated:

“UNIX BIND is just plain cumbersome! It requires a lot of administration, changes, and work hours. It got to the point where my staff couldn’t provide the right level of support and that’s a huge problem.”
Microsoft DNS/DHCP Does Not Fill the Void

One possible solution to the DNS/DHCP quagmire may already be in place. Most companies use Microsoft Windows for network services like directory, file and print. Windows Server also ships with DNS/DHCP services as a part of Active Directory. Users could simply migrate from BIND to Windows DNS/DHCP services already present in the network.

At first glance, this decision is a “no-brainer.” Since Microsoft gives away DNS/DHCP services, why would anyone even consider an alternative solution? It turns out that there are plenty of compelling reasons. The users that ESG spoke with said that Windows-based DNS/DHCP services:

- **Didn’t meet their security and availability needs.** Users lambasted Microsoft DNS/DHCP for its lack of role-based administration, frequent vulnerabilities, and all-in-one Active Directory architecture. In addition, Windows DNS/DHCP isn’t built for high-availability on its own and users can’t afford expensive add-on clustering solutions.

- **Require frequent off-line operations.** IT managers know that they will have to take Windows servers off-line for patching and rebooting. This does not work when network availability is synonymous with business productivity.

- **Are weak on reporting and auditing.** To comply with government regulations and cope with growing networking needs, IT managers need detailed reporting and auditing. Users say that Microsoft is especially weak here.

Alternatives for DNS/DHCP

Business-enabling initiatives like Service Oriented Architectures (SOAs), Extranet applications and IP telephony demand network flexibility, rapid administration, and round-the-clock uptime. To support these needs, enterprises must treat DNS/DHCP as core network services. ESG believes that this means that CIOs must delegate DNS/DHCP ownership exclusively to the networking group and build a highly available DNS/DHCP infrastructure that is scalable, secure and easy to administer.

This poses a logical question: If generic software on servers, such as BIND on UNIX or Windows DNS/DHCP can’t get the job done, what can?

Over the past few months, ESG spoke to numerous public and private sector organizations that decided to eschew BIND and Microsoft DNS in favor of an appliance-based infrastructure from Infoblox, a venture-backed company in Sunnyvale California. The remainder of this paper will describe why these organizations made this decision and what benefits they experienced as a result.

Appliances Simplify DNS/DHCP Management

The organizations interviewed by ESG varied in terms of size, geographic distribution, and number of network nodes. Respondents consistently stated that their decision to change their DNS/DHCP infrastructure was based upon the business need for high availability, ease-of-administration, security, reporting and regulatory compliance. While almost all the organizations had a Windows environment and Active Directory deployed, they were either switching from Windows DNS/DHCP to appliances or they were simultaneously implementing both Active Directory and Infoblox appliances running the DNSone software module, which provides integrated DNS, DHCP and IPAM functionality.
Why did they decide on Infoblox? Users recognized the value of an appliance approach and appreciated the ease of this model:

“Our department has really embraced the network appliance mentality. It’s just easier to configure and support.”

“Plain and simply, it’s easier to administer DNS if it is the only service running on a dedicated appliance.”

DNS/DHCP Appliances Are Networking Devices

As previously stated, one of the problems associated with legacy DNS/DHCP was the lack of defined organizational ownership as administrative responsibility often fell between the UNIX administration and networking group causing operational problems and a lack of accountability for a mission-critical network service.

Like ESG, many IT managers believe that DNS/DHCP management should live within the networking group and saw DNS/DHCP replacement as an opportunity to define an appropriate organizational model. In addition, users believe that the networking group has the right skills and goals while Windows administrators lack network and DNS/DHCP knowledge (see Figure 2):

“Don’t get me wrong, but I don’t think the Windows administration team has the right skill set for IP address management. That’s a networking job.”

“We determined that DNS administration is a networking function so Infoblox was a good fit.”

“We really wanted to separate Church and State if you know what I mean. DNS/DHCP administration goes to the networking group and Active Directory management goes to system administrators.”

IT managers whose organizations migrated from Windows/Active Directory DNS/DHCP to Infoblox also said that separating these two technology functions provided more flexible network configuration options while removing Windows problems from the DNS/DHCP equation. All claimed that this separation of duties helped them improve network availability and service levels:

“With Active Directory, remote users were accessing centralized DNS/DHCP services over a WAN link. This method was slow and the WAN link was a single-point of-failure but we certainly didn’t want to put an Active Directory domain server out in the open at every remote office. Infoblox appliances gave us much more flexibility. I can lock the box in a rack, localize DNS/DHCP, and solve my performance and availability problems.”

“We had one major problem with Active Directory corruption. Unfortunately, this meant taking all the domain servers off-line which killed DNS/DHCP and the entire non-Microsoft part of the network. This was reason enough to pull DNS/DHCP out of Microsoft servers.”

Security Concerns Favor DNS/DHCP Appliances

Over the past few years, information security has become a fundamental corporate governance issue. Why? Think ChoicePoint, CardSystems, Seisant/Lexis Nexus - all examples of companies that experienced embarrassing and damaging security breaches involving customer identity theft. CEOs
are rightfully paranoid that their company may experience the next major security breach and become a front-page news story. In addition, organizations large and small are under the gun to define IT controls, address vulnerabilities, and satisfy auditors to comply with government regulations. A recent ESG Research Report illustrates this relationship between compliance and security as 73% of respondents said that their company’s obligation to comply with the Sarbanes-Oxley Act of 2002 had led to an increase in network security investment and resources (see Figure 3).
This emphasis on security was clearly an important criterion in users’ decision to deploy DNS/DHCP appliances. Securing generic Windows servers and Windows administration were often identified as an operational problem area:

“DNS and DHCP need to be available all the time so I was uncomfortable with a Windows-based solution. The IT operations team needs access to the boxes to apply patches and configuration changes but this requires maintenance windows and downtime. And what if they accidentally blow away my DNS files? This wasn’t a risk worth taking.”

“I know Microsoft says you get DNS for free, but let me tell you, free doesn’t always mean free! Take security. With Microsoft, I have to lock down the platform and patch vulnerabilities but I still have to live with multiple services and administrators on a single box. We would end up spending a ton on IT operations and still have to live with security risks!”

“Unfortunately with Microsoft, you need administrator privileges to manage DNS and there is no role-based access control. Because of our security policies, I was the only one in my group who could update the DNS records; I couldn’t delegate these tasks to my group because we wanted to limit the number of administrator accounts in the company.”

In addition to concerns about security configuration and administration, many users stated that Microsoft’s DNS/DHCP solution was insufficient as it did not provide the type of security, reliability, reporting and auditing functions they needed for regulatory compliance.

“We are required to do DHCP auditing for users and locations and retain these records for seven years. Microsoft doesn’t support standard logging and the information is generally unacceptable. Infoblox really shines here.”
"We had a real problem with audits. We need to know who has access to the systems and what changes were made. Microsoft DNS logging couldn’t support this. Infoblox let’s us use standard Syslog."

“To comply with FISMA we need TSIG support for zone updates in an encrypted format. Infoblox supports this but Microsoft does not.”

**IT Wants Advanced Management Functionality for DNS/DHCP**

Although BIND is extremely complex, it is also a powerful tool offering rich feature/function. Users migrating from BIND found Microsoft DNS/DHCP administration lacking in areas such as updating DNS records, troubleshooting problems and transferring zone information:

“In our environment, I’d say that 20% of our sites are in a constant state of flux. We need to be able to make changes and propagate them quickly. This is way harder to do with Microsoft!”

“Troubleshooting was a big concern. With Microsoft, I’d have to do a box-by-box investigation. Infoblox centralizes logging making troubleshooting a lot easier.”

“We are consolidating the network so I anticipate a lot of moves, adds, and changes. I needed DNS to more flexible and Microsoft just didn’t have the features.”

“We ran into a lot of problems propagating DNS changes. Microsoft uses Active Directory replication for this rather than DNS zone transfers. I feel like replication is fine for directory changes but it can’t support real-time networking requirements.”

“It takes too long to replicate with Active Directory. It’s not nearly as efficient as our old BIND DNS.”

Microsoft also does not integrate DNS/DHCP administration; rather each service must be managed on its own. Users were not pleased with this design:

“To me Microsoft offers a bunch of service silos in Windows. DNS and DHCP are bolt-ons to Active Directory. This adds time and complexity to managing our IP addresses.”

While IT professionals were less than pleased about Windows DNS/DHCP administration and operations, they were far more upbeat about an appliance-based solution and had some specific positive feedback about Infoblox solution. Users raved about the appliance ease-of-use and built in high-availability:

“Infoblox is easy to update. The static stuff can all be done through a web browser.”

“With Infoblox Keystone service, I can upgrade 30 boxes in the time it would take to re-boot one Windows server. That buys me a lot!”

“I’d say you have to go through ‘unnatural acts’ to make Active Directory highly available. This is an out-of-the-box feature of Infoblox.”

**DHCP Requirements Are Also Important**

DNS tends to receive much of the IP address management spotlight but IT professionals were quick to describe their DHCP needs as well and point to inadequacies in the Microsoft implementation. Interestingly, many users said that Infoblox DHCP strengths such as high availability and IP address utilization reporting were very important decision criteria.
“One of our most important requirements was the need for 100% failover of DHCP. We looked at Infoblox and Active Directory and determined that the Infoblox solution could offer this in a simpler and cost-effective way versus Microsoft.”

“To support Microsoft’s DHCP we had to over supply IP addresses which is a waste of resources. Infoblox offers DHCP failover and fixes this problem.”

“We wanted to manage our IP address utilization but you can’t do capacity planning with Microsoft’s DHCP. This was another reason why we chose Infoblox.”

Final Analysis

As networks continue to anchor more and more business processes, DNS/DHCP services are simply too important to undervalue or dismiss. This DNS/DHCP significance leaves CIOs with a critical yet confusing decision. Should BIND remain the primary solution? Are Microsoft’s bundled DNS/DHCP services “good enough?” Is it worth considering other options like dedicated DNS/DHCP appliances?

After speaking with IT professionals from large and small organizations, it is apparent that relying on BIND or Microsoft for critical network services is not considered the most attractive or prudent option. Many users are willing to pass on free DNS and/or DHCP from BIND and Microsoft and invest in appliances from Infoblox for several reasons (see Figure 4):

- **BIND is too difficult to manage.** Too many administrators have stories about mis-configuring a BIND file and causing a network outage. Given the criticality of DNS, it simply isn't acceptable to use the software-on-server approach when simple, powerful appliance alternatives are available. Additionally, BIND must be kept up to date to eliminate security vulnerabilities, and the pain of bringing down servers, patching, and hardening causes many administrators to delay upgrades and dangerously increase their exposure to attacks. Easily updated appliances address this problem.

- **Microsoft DNS feature/function is too lightweight.** Users need more in terms of administration, high availability, and reporting than Windows DNS offers. Obviously, these are not minor issues as they translate into network availability, operating cost, and regulatory compliance. Infoblox is an attractive option because it has taken advanced BIND functionality and added ease-of-use and reliability in a DNS/DHCP-specific appliance form factor. In addition, the ability to manage a collection of appliances as a single system for upgrades, backup & restore, reporting, and resiliency makes it possible to deliver more robust DNS and DHCP infrastructure.

- **DNS security requirements don't fit the software-on-server model.** Windows DNS/DHCP depends upon hardening and patching Windows, a time consuming and potentially service-disrupting process. Administering DNS/DHCP also requires an administrator password creating a risky situation where multiple IT groups and staffs have access to a critical network service. Finally, Microsoft reporting and logging does not provide the necessary level of detail needed for compliance audits. Infoblox appliances are single-function secure appliances that alleviate the need for patching, support role based access control, and provide detailed reporting and logging for auditors.

- **DHCP must go beyond handing out IP addresses.** Microsoft’s DHCP is not designed for today’s IP address management needs. High availability is a kludge at best and the system does not provide the type of information needed for managing leases, planning for future capacity needs, and auditing scarce IP address resources. Infoblox provides DHCP failover capabilities as a core feature which allows firms to share and centralize IP address pools. Infoblox also provides rich management information so administrators can assess IP address utilization for capacity planning.
Some of the IT professionals that ESG spoke with mentioned that Microsoft wasn’t happy about their decision to implement appliance-based DNS and DHCP services and pressured them to rethink this plan. ESG also heard stories where Microsoft field personnel told customers that non-Microsoft DNS and DHCP would not work with Active Directory or that it couldn’t offer support if 3rd party DNS and DHCP services were introduced into a Windows environment. Sounds like the IBM mainframe battles all over again! It should be noted that once these organizations implemented Infoblox appliances and had no problem integrating with Active Directory, Microsoft field personnel abandoned their strong-arm tactics.

Microsoft DNS/DHCP may work for small shops with a limited number of IP nodes and name server domains but security, administration, and operations problems quickly become an issue as a function of network complexity.

As for larger organizations, network availability is just too important to gamble on. Yes, Microsoft DNS/DHCP is technically “free” but this is offset by high operating costs, security risks, and unplanned downtime. ESG believes this is a simple example of choosing “the right tool for the right job.” According to users, Infoblox availability, administration, and security benefits are well worth the investment.