White Paper

The Importance of a Resilient DNS and DHCP Infrastructure

DNS and DHCP availability and integrity increase in importance with the business dependence on IT systems
The Importance of DNS and DHCP

Most organizations view the Domain Name System (DNS) simply as a service that maps fully-qualified domain names to Internet Protocol (IP) addresses. DNS does allow for easier human-readable names (e.g. www.example.org) to be typed into a web browser, and allows a web connection to be made to the IP address (e.g. 192.168.234.123). However, DNS provides more functionality than just mapping names to numbers. DNS is the crucial underlying system that we all rely on for all digital communications.

Dynamic Host Configuration Protocol (DHCP) is the protocol used by most organizations to assign IP addresses to end-user devices so they can access network infrastructure. DHCP is used on wired and wireless networks to assign IP addresses to everything from desktops to laptops and mobile devices. A device is not functional if it does not have an IP address that it can use to access resources over the network. A mobile device without any network connectivity has very limited functionality.

Virtually all Information Technology (IT) systems rely on DNS to handle the abstraction layer of mapping names to numbers. All IT environments rely on DHCP to allow for computers and mobile devices to be able to join the network. All organizations must maintain the DNS database with this mapping and maintain DHCP systems to assign addresses. This DNS database of information is used internally within an organization and externally on the Internet. For enterprises, the DHCP system is used internally to maintain the IP address assignment process. If the DNS or the DHCP system fails, then many applications will not function properly, thus bringing the organization’s IT operations to a standstill.

The following diagram illustrates the fact that applications rely on computer operating systems’ ability to access the network. If operating systems are unable to obtain an IP address or perform DNS resolution then the computer is essentially disconnected from the network infrastructure. This layer of abstraction that DNS and DHCP provide is often overlooked as an important requirement for application functionality. The layers are similar to the foundation of a house. If the underlying layers are weak, then the entire structure is compromised.
Following is a high-level diagram of a typical enterprise environment. It shows how DNS is used both externally and internally within an organization’s network topology. The internal DNS servers often rely on the availability of the DNS servers located in the DMZ. External DNS facilitates your ability to communicate with your customers and allows your customers to communicate with your company. DHCP is used predominantly internally to assign IP addresses to internal hosts.

There are several questions to ask to determine if your organization’s operations are susceptible to risks if DNS or DHCP are unavailable.

Does your company:

- Use redundant external and internal DNS servers?
- Have a robust process to repair a failed DNS server?
- Use the DNS Security Extensions (DNSSEC) to digitally sign your external DNS information?
- Apply security patches to your DNS and DHCP servers regularly?
- Have a redundant DHCP infrastructure?

If you answered “no” to any of these questions, then this article will help your organization develop a strategy to improve in each of these areas. The results of these improvements will increase the resiliency and availability of your IT systems, and improve the security of your environment.
Reliance on DNS and DHCP Services

Most organizations do not realize the importance they have placed on their DNS systems or do not consider the criticality of this service. Our experience of assisting organizations with their IT environments has shown us that many organizations do not consider their DNS or DHCP systems as foundational elements. DNS and DHCP are often ignored until the time they fail and cause negative impact to the financial bottom line.

Many organizations have not invested in DNS/DHCP technology to the level that meets their IT infrastructure requirements. Organizations often expect five nines of availability, but they have failed to invest in the technology to achieve that goal. If your organization is striving to reach 99.999% uptime (approximately five minutes of downtime each year) then all the foundational layers must be able to exceed that requirement. If your organization were to experience a DNS server failure, it might take a full day to completely restore from such a failure. After a single DNS failure your organization may be reduced to 99.9% availability (about nine hours of downtime per year).

Additionally, many organizations have their own home-grown systems that are not redundant, are not secure, and are not kept up to date with the latest patches of configuration best practices. Organizations also use DNS/DHCP systems from Microsoft or ISC (BIND/DHCP) that did not have an initial capital expenditure, but may not have all the resiliency the organization requires. A failure of your DNS systems can have a large impact on your organization’s mission. Because DNS is often taken for granted, we wanted to raise awareness of its importance and show you ways to improve this part of your critical IT infrastructure.

DNS and DHCP Availability

The importance of DNS and DHCP availability should not be overlooked. All organizations should consider the impact of an organization-wide DNS or DHCP failure. What would happen if your DNS server went offline? Following are the various failure scenarios and the resulting impacts to the organization.

- **External authoritative DNS failure** - If your external DNS server is offline, then people on the Internet will not be able to resolve the address of your websites and they will use cached information for the standard timers. Some people who are newly connecting to your Internet-facing applications will not be able to reach them. In some cases it may take you longer than a day to repair or rebuild the server and you will be down for that length of time. Remote users will also be affected reaching the company’s public applications.

- **Internal authoritative DNS failure** - If your internal DNS server fails, then internal users will experience difficulty accessing internal applications. The impact could be as minor as application timeouts and delays that inconvenience users to as severe as complete failure to reach applications. Employee productivity will be negatively impacted the longer the failure persists and the longer it takes to repair. If the failure lasts longer than four hours your employees are likely to go home because they cannot get any work done.
• **Internal caching resolver DNS failure** - If your internal caching DNS servers fail, then end users will have difficulties reaching Internet applications. This could result in application timeouts or connection failures or complete Internet reachability failures.

• **Internal DHCP failure** - If your DHCP infrastructure fails, then devices will not be able to obtain an IP address and will be unable to join the network. Nodes that have already obtained an address will continue to function, but at some time their addresses will expire and they will be unable to re-attach to the network.

**Applications Rely on DNS**

Virtually all IT applications in an enterprise environment rely on DNS availability.

All web-based applications rely on DNS for communications to and from the application end user. Each element on the web page is a separate HTTP/TCP/IP connection and the browser renders these various text/graphical elements onto the viewable page. DNS is required for each of these elements being collected by the browser. If DNS is down, then all or part of the web application will be affected. The effect could be delays to log in to the secured web page, delays in accessing web content, or complete failure to reach the application.

Email relies heavily on DNS to be able to send and receive messages. If your DNS system is down then email will cease to flow. This will impact most of your internal and external digital communications.

Voice over IP (VoIP) systems also rely on DNS information. The Session Initiation Protocol (SIP) has a dependency on DNS, and voice and video collaboration architectures depend on DNS operating properly.

If the DHCP systems are not operational, then IP-enabled phones or video collaboration systems cannot join the network and will cease to function. If end users cannot join the network because DHCP systems are down, then their productivity will be severely affected.

**Making DNS More Redundant**

DNS servers are so heavily relied upon for all end-to-end communications and they work typically so well that we forget they are as important as electricity to a data center. There are several common methods used to make DNS more available and reliable. One method is to have multiple DNS servers. One DNS server can be the primary, and there can be multiple secondary servers that contain identical DNS databases. The DNS information is replicated from the primary to the secondary servers. Hopefully your organization is not using a single DNS server on your Internet perimeter. Best practices also dictate that you have more than one external authoritative name server.

It is also possible to set up a load balancing system to front-end several redundant DNS servers. This helps distribute the load among several DNS servers; however, if the load balancing system fails, it has the same impact as a DNS failure. DNS servers can also be geographically diverse so long as their data is synchronized.
As far as DHCP goes, many organizations implement DHCP redundancy with what is known as “split scopes.” The majority (80%) of the IP address pool could be handled by the first DHCP server and the remainder (20%) of the IP address pool is handled by the other DHCP server. If the first DHCP server fails, the systems must renew their IP address from the operational DHCP server. However, during this process, network communications is effected on the end user's computer or mobile device.

**Security: Integrity and Confidentiality**

Unfortunately, by default, DNS is not a secure protocol and DNS systems are a target for attackers. The integrity of the DNS records in the distributed database is of critical importance. Due to security weaknesses in DNS and vendor implementations, organizations can become the victim of a cache poisoning attacks. There is little confidentiality when it comes to external authoritative DNS servers as this information is publicly available. Internal authoritative DNS systems could provide confidentiality and should be protected similarly to insider threats as external DNS services would be secured against external threats.

There are options to help make DNS more secure and help prevent these types of attacks. There is a set of extensions to the DNS protocol called the DNS Security Extensions (DNSSEC), which allow for authentication of DNS information and provide for data integrity. DNSSEC uses a system of digital signatures to sign and to validate the authenticity of DNS information. While some organizations have implemented DNSSEC, the vast majority of enterprise organizations have not yet enabled this feature on their DNS servers. DNSSEC is simple to implement if you have the right DNS software and utilities, but most organizations have not invested the time to learn about it. Many organizations are using a DNS server version that makes using DNSSEC more difficult to implement and maintain.

**Operations and Maintenance of DNS/DHCP Systems**

If you have not updated the software on your DNS servers then you may be vulnerable to attacks. Organizations should update those systems just like they would any other critical server in their environment. Many organizations fail to prioritize DNS server updates with their other patch-management activities. Patching your DNS servers is important to protect against exploits against the DNS servers themselves as well as protect against data corruption.

The same holds true for DHCP servers. Many organizations are not adequately maintaining their DHCP servers and this is a risk to the IT operations. The internal DHCP servers may not be regularly patched. Also, it might be years since the DHCP server was last checked to determine if the IP address lease duration is satisfactory. Given the increased number of devices in the enterprise due to the Bring Your Own Device (BYOD) trend DHCP scopes often fill up. If the DHCP server is not cared for, then this could lead hosts to be unable to attach to the network.
Infoblox Solution

Infoblox is a global company that manufactures a set of products that allow organizations to effectively maintain their DNS, DHCP and IP addressing environments. Infoblox’s products automate the maintenance of DNS (including DNSSEC), DHCP, and IP address management functions. Infoblox offers highly resilient and high performance DNS and DHCP services that fully support all the computers and applications that rely on the availability of the network infrastructure.

At the core of the Infoblox product line are high availability (HA) pairs of DNS and DHCP servers. If a single server were to fail, its backup system would pick up where it left off without any service interruption. These systems can be physical appliances or virtualized services.

The other component of the Infoblox architecture is the Infoblox Grid. The Grid allows for multiple systems to have distributed management and control. Therefore, if one Grid member fails, then the database of DNS and DHCP information is fully retained within the other Grid members. Changes can continue to be made and the system can be managed and the failed systems can be restored and joined back to the Grid to resynchronize its database.

The combination of the HA pairs and the Infoblox Grid allow organizations to reach 99.999% availability for DNS and DHCP services. Following is a picture that shows how HA pairs of servers and the Grid create a highly resilient architecture.

Summary

Organizations should consider the importance of DNS and DHCP to their business operations. Companies should strive for operational excellence when maintaining their current DNS infrastructure and treat it like any other mission critical application. Failure to consider DNS resiliency will lead organizations to under-invest in DNS exposing their business to an unforeseen risk. If DNS or DHCP services fail, then the organization is essentially out of business until it is restored. Furthermore, you should consider the integrity and validation of the data in the database and use DNSSEC. Infoblox has products that streamline the operation of DNS and DHCP servers making them strong enough that you can depend your entire business on its robustness.

About GTRI

GTRI is an award-winning national solutions integrator enabling both private and public sector organizations to exceed their complex business objectives through technology innovation and adoption. Solution areas include private and public cloud architectures, datacenter infrastructure, network design, mobile workforce solutions, network security, information security, managed IT, professional services and consulting. GTRI delivers innovative, enterprise-grade technology solutions built to solve business challenges.

About Infoblox

Infoblox delivers essential technology to help customers control their networks. Our patented Grid™ technology helps businesses automate complex network control functions to reduce costs and increase security and uptime. Infoblox is a global company, with operations in 25 countries. Our solutions help over 6,900 enterprises and service providers make their networks more available, secure and automated.