



Best Practices in DNS/DHCP and IP Address Management

By Tere' Bracco
Vice President, IT Infrastructure and e-Commerce

This Special Advertising Section Produced By:

NetworkWorld
www.nwfusion.com

Sponsored Exclusively By:

Lucent Technologies
Bell Labs Innovations





Table of Contents

- 3 Finding Yourself: A Brief History of IP Addresses, DNS, and DHCP**
- 3 Where IP Addresses Come From - DHCP**
- 4 The Present: Good News and Bad News**
- 4 Losing Yourself Again: The Problems and Challenges of IP Address Management Now**
- 5 New Technologies, New Threats**
- 6 The Consequences**
- 7 Settling Risky Business**
- 7 Practice Makes Perfect, But the Trick Is in the Tools**

IP Addresses, Domain Name Services (DNS), and Dynamic Host Configuration Protocol (DHCP). Together, these three mechanisms make it possible to locate everything you need on the Internet, including your own computer. Each system presents a means to improve performance and maintain order on your network. DNS keeps track of the names and the IP addresses associated with each device on your IP network. DHCP assigns IP addresses to devices as they connect to the network, and helps you make the most of the scarce IP address space. IP address management tools and practices ensure the integrity and reliability of your IP network.

As crucial as DNS, DHCP, and IP address management are to the smooth running of your network, each represents serious threats to the security of your network and your business. Understanding, managing, and protecting them is crucial. In this article we'll discuss what these systems are, what they do, and where they came from. We'll also explore their vulnerabilities and threats, then discuss the best practices and tools to manage and protect them.

About the Author

Tere' Bracco

As Vice President of Enterprise Systems & Solutions at Current Analysis, Tere' is responsible for analyzing the professional services market for all types of enterprise networks, from telecommunications carrier networks to SME networks. In addition, she oversees coverage for enterprise network infrastructure, enterprise packet telephony, and converged networks. A renowned engineer, author and analyst, Tere' has published four books on networking and has designed global networks for organizations such as Sprint and MCI.

Current Analysis is the fastest-growing and most innovative provider of in-depth, real-time competitive intelligence. The firm serves more than 60,000 users at over 275 corporate clients representing the preeminent firms in the telecommunications and information technology industries. CurrentCOMPETE, the firm's award-winning Web-based delivery system, enables the effective use, customization, and distribution of its tactical competitive information; and integration services to support broad enterprise deployment through corporate intranets, portals, and customer relationship platforms. For more information, visit www.currentanalysis.com



In the Internet World, three guidance systems exist: IP Addresses, DNS, and DHCP. Working together, these three mechanisms make it possible to locate everything you need on the Internet, including your own computer. As the key means to finding everything on your internal IP network as well as the Internet, these systems are literally the keys to the kingdom. Therefore, managing and protecting them is crucial. In this article we'll discuss what these systems are, how they developed, why they are so important, and how to protect them.

Finding Yourself: A brief history of IP Addresses, DNS, and DHCP

DNS was born on June 23, 1983. This date marked the first use of a global database of computer names and the IP addresses associated with those computer names. This event took place at the University of Southern California School of Engineering's Information Sciences Institute (ISI).

This DNS global database solved a weighty problem. The system of using 4-byte numeric IP addresses had been well established and universally employed by the time the DNS was developed. These 32-bit addresses did more than identify network devices: Not only do they provide a unique address for a network host, but also contain a great deal of information on network architecture and host configuration. Unfortunately, while computers have no problem remembering and associating numeric IP addresses with specific systems and network domains, people have a really tough time of it. The team at ISI developed a standard system of associating names that people can remember with numeric IP addresses to make finding hosts easier for people.

The DNS resulting from the work at ISI is the system that enables people to use names instead of numeric IP addresses to identify network hosts and network domain names in an internetworking system. DNS provides unique names for network hosts and IP networks, then translates these names into IP addresses – and vice versa.

From the very beginning, implementing DNS in networks presented challenges to ensure the accuracy and security of the

DNS data. After all, the DNS is essential to finding any resource on the network. Because this is such a large and important task, extra safeguards have been put in place. For example, rather than use one server for the DNS, a DNS is distributed across network servers. Each network is required to have at least two DNS servers to keep track of the moves, additions, deletions and changes of different host names and network domain names that take place in that network.

Where IP Addresses Come From – DHCP

DNS keeps track of the associations between host names and IP addresses, but it doesn't assign host names to host IP addresses. This task is performed by another mechanism, the DHCP. This protocol is the result of the evolution of internetworking technology and PC and workstation devices.

In the early days of IP networking, IP addresses were assigned using the Bootstrap Protocol (BOOTP), a simple protocol designed to enable the exchange of addressing data between a boot server and host. In a BOOTP exchange, the host first tried to discover its own IP address, along with the location and name of its boot file. Then the server responds to the host with enough of the addressing information that the host doesn't know about itself to allow the host to boot. BOOTP was a great idea back in the days when most network hosts had limited



Lucent VitalQIP™
IP Address Management Software

Automatically configure,
integrate and
administer IP services
across your business.

Lucent Technologies
Bell Labs Innovations

[Lucent Technologies](http://www.lucintel.com)

resources because it required few resources and used a simple format to transmission data between host and server.

But IP networking soon outgrew BOOTP. By the late 1980s, most hosts on any given network had ample memory and disk storage to boot themselves. Nonetheless, managing IP addresses and host names was still a problem. Allocating IP addresses, configuring hosts properly, and keeping up with mobile users became far more challenging than conserving scarce host resources. After all, allocating and managing a scarce resource is always challenging, and IP addresses are no exception. Manually administering IP addresses for all the devices in a network quickly became a problem. Enter DHCP.

To solve the problem of managing IP addresses, DHCP was developed to assign dynamic IP addresses to devices on a network. DHCP solved a lot of problems in IP address management, because the protocol presents a wider array of boot attributes among networked devices. It also has the added benefit of being backward compatible with BOOTP. Hosts that use DHCP can fully configure themselves without operator intervention. DHCP generally employs three methods of assigning IP addresses: automatic, in which a host receives a permanent IP address; dynamic, in which a host receives a temporary IP address each time it connects to the network, and that IP address is valid only for the duration of the network session; and manual, in which operator-configured IP addresses are delivered to hosts via DHCP.

In general, DHCP addressing is either “static addressing” or “dynamic addressing.” With static addressing, a network resource has a fixed IP address; it has the same IP address every time it connects to the network. Dynamic addressing DHCP assigns a temporary IP address to a device each time it connects to the network that is valid only for the duration of the network connection. Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means a new computer can be added to a network without having to manually assign it a unique IP address. Generally, in most network implementations DHCP supports a mix of static and dynamic IP addresses.

The Present: Good news and bad news

The good news is these standard protocols provide Internet users worldwide with a means of connecting to the Internet and finding the resources they need. Today, all network users

depend on DHCP every time they turn on their computers and connect to an IP network. And all Internet users depend on DNS every time they visit a Web site or send an e-mail. As the world’s largest and busiest distributed database, the DNS handles billions of requests every day. The bad news, however, is that this ubiquitous dependence on these mechanisms means that IP address management, DHCP, and DNS are the largest, most universal security challenges in the networking world.

Losing yourself again: The problems and challenges of IP address management

Systems do fail, and an IP address management system, including DNS and DHCP services, is no exception. An IP address system can fall apart for a variety of reasons, from the accidental to the malicious.

Simple human error is one of the most common causes for problems in IP addressing and DNS functions. The causes for this are widespread and well-known: overworked IT staff, no time to follow rigorous practices manually, no money for training or advanced automated management tools.

Many companies manage their IP addresses using manual methods that are loaded with opportunities for error. Change management is done “on the fly,” and so changes to the IP addressing structure aren’t properly recorded. Outdated IP

Lucent VitalQIP™
IP Address Management Software

#1 Market Share

- 2000
- 2001
- 2002

Source: IDC

IDC
Analyze the Future

Lucent Technologies
Bell Labs Innovations

[Lucent Technologies](#)

address management tools aren't equal to the task, or they don't work with older versions of the DNS. The result is that most companies use inaccurate DNS configurations somewhere in their networks.

Mergers and acquisitions cause problems in scalability as well as merging two IP addressing schemes. Especially in a merger situation, where there is no central repository of IP information, network administrators are likely to face duplicate IP addresses in the private address space, and the methods used to extend the available address space, such as classless subnetting, will make it tricky to sort out these duplications. Add to this the often political issues of determining whose IP address management system – and whose private IP addresses – are adopted, and you have a sticky administrative problem that could take lots of time and an army of diplomats to resolve. The staff of the merging organizations also will likely have differing levels of capability, differing tools, and differing methodologies to manage the IP address space. And there is the burden of looking forward – network planning for the merged organization.

Another increasingly common problem in IP address management is unauthorized access points. This phenomenon is as old as LANs, which popped up unannounced, unapproved, and unknown in the mid-1980s as do-it-yourself projects that employees undertook to enable share printers and files. Now access points to the network are the unsanctioned technology, such as wireless LANs. These “open doors” to the network make it easy to launch attacks on a company's IP address system.

Of course, not all sources of failure are inadvertent and innocent. The IP address space is a favorite target for attack from both internal and external parties. Internal attacks are the most commonplace and the most threatening. A disgruntled employee knows the company network's vulnerabilities better than an outsider and often has the access rights, as well as the time, to plan the perfect attack. An internal employee knows the IP addressing method, the version of software and hardware, and therefore is in a position to plan an attack that is much more efficient, harder to stop, and potentially more devastating than an external hacker. For example, exploiting buffer-overflow vulnerabilities or initiating denial of service (DoS) attacks is easier to accomplish from the inside. And don't think it's just a ticked-off employee; it could even be a plant from a competitor!

External attacks get more press, but are rarer. Still, the outside threat exists. The motivations are increasing – from thrill-seeking students and industrial spies to identity thieves running illicit businesses of reselling personal information. Throw in a political activist or two, along with the so-far-unrealized threat of “Internet War,” and it's pretty clear that external parties pose a significant threat.

No really problematic flaws or insurmountable vulnerabilities have yet been found in the DHCP. Still, it's important to remember that DHCP server generally has root privileges. A DHCP server with root privileges has complete rights to the machine on which it runs, and this privilege creates an opportunity for catastrophic damage should the DHCP server be hacked. Fortunately, root privileges aren't required to run a DHCP server, but network administrators find it easier to grant root privileges than to design the involved security access that would let a DHCP server to do its job without root privileges. It's definitely worth the time and trouble to avoid granting root privileges to the DHCP server.

New technologies, new threats

New technologies also are making managing the IP address space difficult. Some new innovations require that the already scarce IP address resource be stretched even further, thus requiring more careful management. Other new technologies



Lucent VitalQIP™
IP Address Management Software

Over 75% of the Fortune 100 Companies use Vital software to run their businesses reliably and profitably.

Lucent Technologies
Bell Labs Innovations

[Lucent Technologies](#)

Settling risky business

Now that you know what a dangerous world it is for your IP address management systems, and especially your DNS and DHCP servers. Is there any way to protect this vital resource?

Relax. There's help. There's hope. It begins with some fairly straightforward changes to improve the security and reliability of your DNS and DHCP servers. Here are a few best practices:

1. Keep abreast of the latest known vulnerabilities to DNS and DHCP. Forewarned is forearmed. The bad news is that new security holes and flaws in DNS servers are uncovered constantly. The good news is DNS vendors generally fix these problems right away. By using such resources as your DNS and operating system vendors' security announcement mailing lists, for example, the CERT Advisory mailing list (cert-advisory-request@cert.org) or the Internet Software Consortium's Web site (www.isc.org), you can keep up on the latest threats and find out how to get the appropriate patches.
2. Restrict access. Keep a careful eye and a tight reign on access control lists (ACLs) for DNS servers. Keeping track of who is authorized to access the DNS server is fundamental to security, and yet is sometimes difficult to do through manually. Monitor ACLs closely and carefully.
3. Keep DNS and DHCP software applications updated. This is a corollary to Item 1. After all, the older the version of software, the better known its weaknesses. By running the latest proven version of your DNS and DHCP software, you are eliminating the risk of being attacked through the well-known vulnerabilities of older versions. You are also buying a bit of time because hackers look for vulnerabilities in the newer versions. On the other hand, you also are opening yourself to possible instabilities, which is why we suggest running the latest proven version.
4. Remove single points of failure. Think of how you can split functions among several machines. For example, run DHCP and DNS services on separate, dedicated machines that aren't being used by other applications. You also can consider using separate servers for external and internal DNS information. You might also use separate hardware for servers handling the company's internal DNS data and caching servers, which retrieve DNS data from external sources.
5. Filter traffic. If you follow the advice above and keep your DHCP and name servers on separate, dedicated machines, these machines won't have any reason to receive non-DNS traffic. So eliminate unnecessary risk, and filter out all but DNS traffic to dedicated name servers.
6. Don't forget redundancy. This is essential to any critical network element, and your DNS and DHCP servers are no exception. Be sure that critical servers are duplicated, either through duplicate servers or by using an external DNS service as a backup. Keep name servers in separate physical locations using separate power sources, Internet connections, and routers. Put these servers on different subnets, too. And think about running different operating systems on these redundant servers, so that a flaw in the operating system won't cripple your back-up plan.

Practice makes perfect, but the trick is in the tools

Best practices are crucial but not enough. Maintaining security for your IP address resource often requires automated tools to execute best practices. For example, a critical practice in IP address management is auditing IP address usage. Knowing which user has which IP address and when not only helps you make better use of your IP address space, but also helps you track down suspicious IP traffic and network activities. The problem is, this type of audit trail is extremely difficult to main-

Lucent VitalQIP™
IP Address Management Software

Boost your bottom line by streamlining IP address management. Our IDC ROI WhitePaper shows you how!

[DOWNLOAD NOW](#)

Lucent Technologies
Bell Labs Innovations

[Lucent Technologies](#)

tain with manual processes. It's best to find an automated IP management tool to perform this type of function.

Automated tools can also assist in other tasks, such as helping to maintain tighter security on ACLs to DNS servers.

Choosing the right automated IP address management tools involves much the same criteria as choosing the right DNS. Here are a few things to look for:

- 1. Ease of use.** If an IP address management system is too difficult to use, it won't be used properly or it won't be used at all. In either instance, all the security and management benefits are lost. Make sure your IP address management system has an intuitive user interface and easy-to-use wizards and templates that help administrators write and enforce appropriate policies.
- 2. Centralized IP Management.** The ability to manage multiple technologies in one holistic IP management system (Microsoft, DNS, DHCP, VoIP)
- 3. Scalability.** All systems – IP address management, DNS, and DHCP– need to be able to scale to meet the projected growth of your organization and your network, with room to grow. Spend some time thinking about the future IP address space needs of your company, including the demands placed on the IP resource by Web services, wireless communications devices, point of sale devices and IP telephony.
- 4. Redundancy and failover capabilities.** As mentioned earlier, physical and logical redundancy is fundamental to the security of your DNS and DHCP servers. Therefore, it's critical that any automated tools and systems can support the redundancy and failover configurations you have implemented.
- 5. Performance.** DNS and DHCP services can be a bottleneck for the entire network, so look for high performance in both your DNS server and your DHCP server. Also look for fast recovery and restart capabilities, especially for DHCP servers. Be aware: Some DHCP servers have to restart after every change and some can take hours to restart after a reboot or outage.
- 6. Granularity of administrator access controls.** Select systems that allow the greatest possibility granularity of administrator access controls. This enables you to give users the levels of access to resources they need without threatening network security by granting excessive rights.

It's entirely possible to manage your IP address space effectively and conserve this scarce resource while maintaining security and control. By carefully choosing your DNS and DHCP servers, fine-tuning practices and selecting a good automated IP address management tool set, you can reduce costs, avoid problems, and be set for (almost) painless network expansion.

© 2004 Network World, Inc. All rights reserved.



[Request a reprint of this report.](#)

