

IP address management challenges



This white paper discusses the challenges involved in managing an IP address space, with special focus on the management of multiple DNS and DHCP servers.

The **Men & Mice Suite** is introduced as the natural solution for dealing with the challenges involved in IP management. The Men & Mice Suite provides a unified, scalable management layer on top of the existing DNS and DHCP servers. The purpose of this document is to provide an understanding of the Men & Mice Suite, its architecture, and how it enables reliable and professional network services.



© October 2008 Men & Mice. All rights reserved.
This white paper is for informational purposes only.
Men & Mice does not make any warranty of any kind, either express or implied, in this document.

All Men & Mice product names and service names are trademarks of Men & Mice.
All other company and product names are trademarks or registered trademarks of their respective owners.

Men & Mice

E-mail: info@menandmice.com

Please visit the Men & Mice web site at: <http://www.menandmice.com>



Table of Contents

1. Introduction	1
2. IP address management and its challenges	1
3. Managing multiple DNS and DHCP servers	2
Inadequate integration/control for managing multiple servers	2
Data validity concern	2
Security concern	2
Scalability is the issue	2
4. The dynamics of IP address management	3
DNS + DHCP < IP address management	3
“Home brewed” solutions fall short	3
Central administrators and their internal clients	3
Time consuming & limited scale vs. security & configuration hazards	4
Legacy solutions result in juggling act	4
5. The Men & Mice Suite: The non-intrusive network management layer	5
DNS & DHCP servers are not the problem	5
Retain server investments by introducing non-intrusive management layer	5
Men & Mice Suite	5
Deploying the Men & Mice Suite	6

1. Introduction

Since the dawn of the Internet, IP address management has been one of the fundamental tasks carried out by network administrators. DNS (Domain Name System) and DHCP (Dynamic Host Configuration Protocol) are both indispensable parts of IP address management. As networks grow in their scope and services, DNS and DHCP servers often become management problems of their own. The number of DNS and DHCP servers tends to increase as networks grow. Standard implementations of these protocols, although perfect for carrying out their core tasks, lack adequate, scalable management interfaces and functions. Managing multiple DNS name servers and zones, hundreds or thousands of DHCP scopes, and thousands and thousands of IP devices, makes IP address management using only legacy solutions an inefficient and risky endeavor.

The purpose of this paper is to provide a general overview of the dynamics of IP address management and to discuss some common issues and problems network administrators face when managing the IP address and how certain processes lead to inefficient use of time and resources.

The Men & Mice approach to the problems of IP address management is not to throw away an organization's investment in existing infrastructure. Rather, the Men & Mice Suite complements the existing server investment by providing a non-intrusive and sophisticated management layer on top of them. The Men & Mice Suite allows centralized management of DNS and DHCP, plus a central database of IP address allocation, by integrating all IP address management functionality into a single unified management interface in a Microsoft or Unix environment or mixture thereof.

2. IP address management and its challenges

IP address management includes controlling and tracking the allocations of IP addresses required by computers and other devices to connect to a given computer network. Key questions that IP address management must answer are how much free address space is available, how is the address space partitioned (i.e., subnetting), and who is using the allocated addresses. At a lower level, and for a given device, IP address management must also provide answers to the following questions:

- Is the IP address permanent or temporary?
- What host name is associated with its IP address?
- What MAC (Media Access Control) address is associated with the IP address?
- What IP-specific configuration parameters does the device have?
- What is the physical location of the device?
- What is the device's serial number, its type, asset number etc.?
- Who authorized the connection?

The ability to answer these questions in a reliable and timely fashion is absolutely a key element in providing a professional IP network service. Failure to catch a saturating subnet or a misconfigured device can, and often does, have unacceptable consequences, such as loss of connectivity or even enterprise wide loss of critical services such as e-mail or web related services.

In reality, it becomes increasingly difficult to answer these questions as networks grow. There are several reasons for this. One reason is the dynamic nature of



modern networks; roaming devices requiring temporary connections make it difficult to get an up-to-date view of the IP address space.

3. Managing multiple DNS and DHCP servers

As networks grow in size and services, the number of connected DNS and DHCP servers also tends to increase. While differing in the details between organizations, the reasons for this trend are usually the physical topology of the network (e.g., geographical dispersion) and typical IT related considerations, like performance and security. This leads to the decentralization of IP address information, which again translates into new problems for the IP address management team.

Inadequate integration/control for managing multiple servers

One of the biggest problems in managing connected DNS and DHCP servers is their limited integration. Although lower level functionality may be integrated, like in DDNS, there is little or no integration for easing the management of these services. For example, an administrator may have a difficult time telling if the host in question has any associations in DHCP when looking at host information in DNS. The problem is not only how little is integrated between the two different services, but also the lack of integration even when managing servers of the same type. The standard DNS and DHCP implementations have inadequate interfaces for managing and controlling more than one server at a time. This means that tasks such as searching or mass editing, i.e. tasks that involve more than one server, can be very time consuming and error prone. Replicating changes to multiple DNS and DHCP servers can get uncomfortably complex, leaving room for human errors to creep in.

Data validity concern

Another problem is that the standard servers perform only the most basic input and configuration validity checks, and provide no means of extending or adding new rules. This means it is difficult for organizations to define and impose their own validity checks and workflow processes. The validity of the data entered is at the mercy of the precision and care of the user.

Security concern

Standard DNS and DHCP servers do not implement any role-based access rules. This has obvious security concerns. A user that only needs to work with a limited set of IP addresses might be granted access to a given DNS or DHCP server in order to make some simple adjustments, but this would expose all of the server's data to the user.

Scalability is the issue

Dealing with multiple DNS and DHCP servers gives rise to all sorts of other management issues, but the three problems mentioned above capture the essence of the challenges involved. It is, however, important to note that the problems mentioned above have nothing to do with DNS and DHCP as such. Standard implementation of DNS and DHCP, most notably Microsoft's and ISC's, are perfectly adequate for handling their core job. Rather, the problems arise because their default management tools were not designed to (and, thus, are not able to) provide the scalability necessary for larger environments.

4. The dynamics of IP address management

DNS + DHCP < IP address management

An increasing number of DNS and DHCP servers mean more tasks for network administrators, while their available resources usually remain constant. Of course, IP address management involves more than just the management of DNS and DHCP data. Indeed, the essence of IP address management can be stated without mentioning DNS and DHCP at all. While these technologies provide answers to some of the more basic questions, other key questions of IP address management are simply left unanswered. For example, DNS and DHCP provide no means of answering how the total address space is structured or how much address space is free in a given subnet. Obviously, something more is required to bridge the gap.

“Home brewed” solutions fall short

Network administrators have traditionally fallen back on home brewed solutions, managing the IP address space and the allocation of IP-blocks, often with a special application. In the past this has often been done using measures like spreadsheets or flat text files. While such approaches may work for small networks, they only add to the confusion when networks grow. This just adds one more interface to the IP address management process and raises obvious concerns for synchronization, security and scalability. A good IP address management system must provide a means of integrating DNS, DHCP, and other IP address management functions into one unified whole.

Central administrators and their internal clients

IP address management has one other aspect. This is the obvious fact that running a large enterprise network entails certain social interactions, i.e. the interaction of groups of people with different knowledge sets, skill levels and access privileges. In particular, it is helpful to make a distinction between two groups of users: the group, or team, of central administrators and the group of their internal clients. Let's look at each in turn.

Central administrator team – The central administrator team is the group of professionals responsible for managing the IP address space and manipulating the DNS and DHCP servers. Their list of duties is typically divided into the following tasks:

1. IP address space structuring and monitoring

The core tasks here focus on the structuring of the IP address space, i.e., its division into subnets, and the allocation of IP-blocks. This also involves tracking what devices and users are on each subnet and the registration of all other additional data the organization wants to monitor, e.g., device type, serial numbers and etc.

2. DNS management

This involves the management of the organization's zones, as well as individual DNS servers. It is not uncommon that organizations use two different DNS servers:

- The *Microsoft DNS* server comes with a good management interface, although it is not designed to provide the kind of scalable and secure management capabilities necessary for larger environments.

- BIND DNS is the DNS server of choice for various Unix/Linux based operating systems. BIND is managed via command-line tools and is configured through flat text files using one's favorite Unix text editor. It requires a high level of expertise and is always an error-prone process.

3. DHCP management

Tasks for DHCP management include the configuration of individual servers, compiling statistics and reports on scope utilizations, and the synchronization of DHCP with IP address management in general.

Internal clients – The internal clients are people who are seeking services from the central administrator team. Their knowledge of DNS and DHCP is usually limited. An example of an internal client might be a person managing a Local Area Network of thousands of devices within the organization, who is responsible for such activities as connecting a new printer to the network.

Time consuming & limited scale vs. security & configuration hazards

In the absence of a good management solution, the interaction between these two groups gives rise to all sorts of problems. For example, in an attempt to keep things centralized and secure, the central administrator team might decide to service each request directly and deny internal clients any form of "self-service". In an another scenario, the administrator team might decide to give internal clients access to the relevant DHCP and DNS servers, allowing them some form of self-service.

Both approaches are unacceptable. The first approach really only works for smaller networks and can easily make serving internal clients one of the most time consuming tasks of the central administrator team. It does not scale well, as it results in long lead times as the network grows. Although the second approach might at first sight seem better in this regard, it really is not. Allowing internal clients access to DNS and DHCP servers easily results in all sorts of security and configuration hazards. So instead of serving requests from their internal clients, the administrator team will instead spend their valuable time hunting down configuration and input errors.

Legacy solutions result in juggling act

The central administration team requires qualified people. But no matter how qualified they may be, managing the IP address space on larger networks using only legacy solutions means that the central team will be preoccupied with manually running processes that should be automated. They will be juggling too many flaming torches for comfort.

5. The Men & Mice Suite: The non-intrusive network management layer

DNS & DHCP servers are not the problem

In light of the forgoing discussion, one might be tempted to think that the DNS and DHCP servers themselves are a big part of the problem and that it would be advantageous to replace the existing servers with new server boxes that provide better integration and simpler management interfaces. That is not the case.

The standard implementations of DHCP and DNS are industry hardened and when it comes to their core low-level functionality they are robust and efficient. It is their default mode of management that is the problem. In particular, it is the lack of an integrated management interface for DNS, DHCP, and IP address management functions that gives rise to the management issues we have been discussing.

Retain server investments by introducing non-intrusive management layer

Instead of replacing the existing DNS and DHCP servers, the problem should be dealt with head-on by introducing a new management layer on top of the existing servers. This is the fundamental idea behind the **Men & Mice Suite** and its concept of non-intrusiveness. Taking this natural step brings substantial benefits:

- It allows organizations to leverage existing investments by preserving the infrastructure.
- It enables an integrated and up-to-date view of the data in DNS and DHCP, effectively merging the two together, and opens up new possibilities in monitoring user input and enforcing the practices of the organization.
- Having a separate management layer allows greater flexibility in defining user access rights, making it possible to define a fine grained access control for the IP address space.

Men & Mice Suite

The Men & Mice Suite contains the following application modules:

- DNS Management Module
- DHCP Management Module
- IP Address Management Module
- DNS Analyzing and Monitoring

It is possible to implement one or more of the individual Men & Mice modules, but the real value of the Men & Mice Suite is realized as a powerful, integrated solution for DNS, DHCP, and IP Address Management. Working together, the modules provide a unique management solution that enables organizations to keep track of their IP address space, individual hosts on the network, and their associations in DNS and DHCP.

The Men & Mice Suite is carefully designed to address IP administration challenges such as:

- **A clear, integrated view and centralized management**
A centralized management layer is provided on top of a decentralized and dynamic infrastructure, integrating DNS, DHCP and other IP address management functions.
- **Secure and easy task delegation**
Senior administrators can define arbitrary subdivisions of authority over the network directory services and can delegate authority for routine everyday tasks, so that such tasks can be handled professionally by helpdesk or local operators.
- **No Errors**
User input is checked for errors and consistency.
- **No proprietary mission-critical server technology**
The Men & Mice Suite works with an organization's existing DNS and DHCP servers. Existing servers are treated as the authoritative source of information. This means that if any component of the Men & Mice Suite were to break down, all DNS and DHCP services would still continue to operate without interruption.
- **Easy, step-wise deployment; no migration**
Deploying the Men & Mice Suite requires no migration or redesign. Its modular design allows administrators to deploy the individual modules in any order, and when it best suits the organization.
- **Directory enabled**
The Men & Mice Suite builds on the existing directories, such as the existing DNS infrastructure and the user database in Active Directory.

With the Men & Mice Suite, organizations can deploy a professional and scalable IP address management system, leverage existing IT investments, and keep core network services intact, all using standard and proven technology. It means that the deployment phase will not disrupt daily network services and will not keep administrators tied up in grand scale redesign efforts.

Deploying the Men & Mice Suite

The Men & Mice Suite contains four application modules which can operate independently of each other. Each module utilizes the same application infrastructure, the core of the Men & Mice Suite.

With the non-intrusive nature of the Men & Mice Suite, no replacement of the underlying DNS and DHCP infrastructure is needed. This significantly simplifies implementation of the solution. This approach therefore requires limited efforts and includes low risk.

The core solution consists of a Central server component and a Management Console component. The deployment process will always start with the installation of these two components. With the core components in place, the individual application modules can be enabled in any order.

Depending on the network complexity, the solution can be deployed within a few hours.