Debugging DHCP Performance

Vladimir Brik, Jesse Stroik, Suman Banerjee
Department of Computer Sciences, University of Wisconsin-Madison, WI 53706, USA
Email: {vladimir,jstroik,suman}@cs.wisc.edu

ABSTRACT

Dynamic Host Configuration Protocol (DHCP) was defined to facilitate automatic configuration of IP addresses and other network parameters to hosts in a network. Efficiency of DHCP's address management is especially important today in part due to proliferation of mobile devices with transient network access patterns and the consequent increased demand on transient IP addresses in open-access networks. Unfortunately, DHCP's flexible design makes it susceptible to a variety of misconfigurations. The focus of this work is, therefore, to evaluate the performance and vulnerabilities of DHCP in operational networks today. To this end, we developed a tool called DHCP-Watch that facilitates DHCP-related network debugging and enables better capacity planning. We used this tool to perform a first-of-its-kind detailed measurement study of DHCP performance in operational university campus networks. Our measurements revealed various trends of IP address usage. Additionally, we discovered frequent anomalous operations due to network misconfigurations and presence of misbehaving hosts.

Categories and Subject Descriptors

C.2.3 [**Computer-Communication Networks**]: Network Operations—*Network monitoring*

General Terms

Experimentation, Measurement, Performance

Keywords

DHCP, Experimentation, Measurement, Performance, Tools

1. INTRODUCTION

When a host is connected to a network, traditionally, the network administrator needs to configure it with a whole gamut of network settings, such as IP address, subnet mask, and the default gateway. However, a manual configuration of each host is labor-intensive, error-prone, and hence inefficient. The Dynamic Host Configuration Protocol (DHCP) [2] was created to automate the configuration of hosts on a network. Over the last decade two developments have led to increased demands on the performance of DHCP in networks today. First, the potential threat of IPv4 address exhaustion has led to careful allocation of IP address blocks. As a consequence, increasing number of networks have a limited number of available addresses to serve their user bases. Second, the continued proliferation of numerous mobile and wireless devices with transient network access behaviors has made optimal usage of IP addresses quite challenging. In order to devise effective IP address allocation strategies, there is a significant need to perform a systematic study of DHCP performance in operational networks.

The goal of this work is, therefore, to define mechanisms for "debugging" DHCP performance in operational networks. The following are the key contributions of this work:

DHCP Measurement Study: We present a detailed measurement study of DHCP performance in multiple operational networks. Our study, performed over several weeks in networks on University of Wisconsin-Madison campus, provides a first benchmark of its kind for DHCP-enabled networks. In particular, we present results of this performance study for two networks with contrasting administrative styles — a small, tightly controlled network where each host is authenticated before being admitted into the network, and a larger loosely administered network where such tight central administration is difficult for a variety of technical and non-technical reasons. Our study demonstrates that in both cases IP address leases follow a definite daily and weekly pattern, analogous to what has been observed for network traffic [6, 3]. Additionally, some "open access" networks regularly experience IP address allocation problems that are primarily due to sub-optimal DHCP configurations. Through our measurements we were able to map many such problems to misconfigured or misbehaved clients in the networks.

A tool for DHCP Debugging: For the purpose of this study, we have developed a tool called *DHCP-Watch* that performs real-time monitoring of DHCP-related activities in networks. [1] This tool tracks DHCP lease usage, reports incorrect behaviors, such as misconfigured or malfunctioning hosts, presence of unauthorized DHCP servers, along with performing a variety of other functions that are particularly useful to network administrators. DHCP-Watch is primarily

[1]Available at http://www.cs.wisc.edu/~suman/projects/dhcpw

IMC'04, October 25–27, 2004, Taormina, Sicily, Italy.

passive; it monitors a subset of the traffic "on the wire" at the DHCP server. Optionally, DHCP-Watch performs active subnet scans in an effort to construct more information about the network.

2. DHCP AND POTENTIAL PROBLEMS

DHCP automatically supplies network configuration parameters, such as IP address, subnet mask and network gateway address to network hosts. DHCP is attractive to network administrators for two primary reasons: (1) any host on the network can be automatically configured through a centralized point of IP address management; (2) networks with a limited number of IP addresses can be configured with DHCP to reclaim IP addresses of transient hosts for reassignment.

The most basic DHCP server configuration involves definition of two sets of IP addresses, the *static pool* and the *dynamic pool*. An IP address from the static pool is assigned to a specific interface identified by its MAC address. An IP address in the dynamic pool can be assigned to any interface not specified in the static pool.

The set of configuration parameters supplied by a DHCP server to a client is commonly referred to as a *lease*; a lease is identified by its IP address. Leases that correspond to addresses in the static range are called *reserved* leases.

In order to self-configure, a host first discovers available DHCP servers by broadcasting a *Discover* message. DHCP servers respond with *Offer* messages, which include an offer for an address lease. If multiple offers are received, the client chooses one of them and requests a commitment from the corresponding server. The chosen server responds with a positive acknowledgment, thereby committing the lease to the client. At this point the lease for the assigned IP address becomes *active* and the client starts to use it.

A lease assigned by a DHCP server is valid only for a finite period of time, called a *lease period*, which is agreed upon during lease acquisition. In order for a client to continue using the same network configuration for longer, the client is supposed to periodically re-negotiate a *lease renewal* with the DHCP server. If the lease is not renewed, the server considers the lease to be *expired* and may choose to assign it to a different client.

The duty of the DHCP server in the lease negotiation process is to ensure absence of conflicting client configurations in the network. However, since clients configure themselves, a DHCP server cannot guarantee that all clients will be, in fact, properly configured.

A DHCP server's view of the available IP addresses may be inaccurate. In order to reduce conflicting address assignments, a server may employ a *ping-before-offer* technique — where the server "pings" to verify address availability before offering it to a client. Additionally, clients upon receiving an address offer independently verify that the address is not already in use by sending a gratuitous ARP. If the client detects that the offered address is already in use, a *Decline* message is sent to the server. When the *ping-before-offer* test or a *Decline* message reveals that an address is already in use, the server assumes that the IP address in question is no longer under its control and marks the corresponding lease as *abandoned*. Abandoned leases typically are not offered to clients for assignment.

Need for DHCP Debugging

DHCP is a protocol designed to automate address management in networks. To operate properly, a DHCP server relies on the clients to follow the protocol specifications. Clients that break the protocol can greatly reduce efficiency of address usage in the network. The detection of misconfigured clients is often non-trivial in a reasonably-sized network.

In addition, the recent proliferation of mobile devices has made networks more dynamic and has put more strain on the performance of DHCP. Mobile hosts have transient network access patterns and DHCP must be properly configured to efficiently recycle unused addresses of these transient hosts back to the pool of available addresses.

Hence, it is important to study the performance of DHCP, identify the common causes of address related problems, and define techniques that will allow administrators to quickly and efficiently remedy such situations in networks today.

Problems with DHCP

In the course of this DHCP measurement study, we encountered a number of problems that are reported in this paper. In this section we categorize some of the common problems, based on their causes:

Client Misconfigurations: Misconfigured (or misbehaving) clients can lead to many inefficiencies in address usage. The following commonly arise due to client misconfigurations.

Address theft: A host assigns an IP address to its interface without acquiring a lease from the DHCP server. This can lead to an address conflict between two hosts. Address thefts may result in two phenomena.

- *Lease abandonment:* When an address is detected by the server to be stolen from the dynamic pool, the corresponding lease is marked abandoned and is not considered for future assignment, causing the effective size of the dynamic pool to shrink. This can be detected by observing the response to a DHCP server's *ping-before-offer* verification or a *Decline* message from a client.

- *Interface Roaming:* This occurs when a host with a reserved lease uses an address other than the one configured for it in the server's static address pool. Since the reserved address cannot be re-assigned, the interface in question is effectively consuming two addresses. This violation can can be detected by comparing the IP to MAC address mapping according to the DHCP server and the mapping observed in network traffic.

Usage of BOOTP: Hosts are sometimes configured to use BOOTP [1] instead of DHCP for automated network configuration. BOOTP leases are assigned permanently and are never released. Because of this, BOOTP is undesirable on most networks. BOOTP can be detected by observing its broadcast traffic.

Sub-optimal Server Configurations: Two important parameters for configuring a DHCP-enabled network are the size of the dynamic address range and an appropriate time period for the default lease duration. The optimal choice of these parameters depends on various network access characteristics. For example, some university networks expect to have many transient network hosts that require connectivity for a short duration (students may connect their laptops

only for the duration of a class). In such a network the duration of address leases should be short enough to allow the DHCP servers to quickly reclaim address leases. However, short lease time may imply greater address turnover, which means increased probability that a machine that has been turned off for some time will change its IP address (even for hosts using DHCP, persistent IP addresses are often desirable for convenience reasons). Moreover, network behaviors change over time. DHCP configurations in many networks are detected to be sub-optimal only when the servers run of out available leases and clients are unable to access the network. Therefore, it is important for network administrators to monitor evolution of lease usage in their networks and use this information be periodically re-configure the various DHCP parameters.

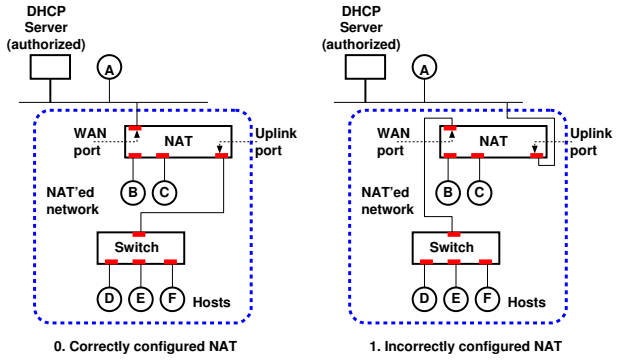

Figure 1: Example of unauthorized DHCP servers due to misconfigurations.

Lack of Access Control: Before a client can configure itself, it needs to discover the available DHCP servers using broadcast. The client has no means of distinguishing between responses from authorized and unauthorized servers and therefore may choose to accept wrong network parameters that could prevent the client from normally accessing the network. A single unauthorized DHCP server can very quickly spread misconfiguration across the entire network.

Unauthorized servers are a growing problem that often arises due to incorrectly configured NAT devices in the network. Consider the scenario shown in Figure 1, where a network user wants to move a set of hosts (B to F) behind a NAT. Most NAT devices today include embedded DHCP servers which are enabled by default. If connected correctly (Panel 0) the NAT provides address leases to the right hosts and in turn gets an externally visible address from the authorized DHCP server of the network through its WAN port. However, if the connections of the WAN port and the uplink port are interchanged in a simple misconfiguration (Panel 1) the DHCP server embedded in the NAT starts responding to DHCP *Discover* messages from clients in the public part of the network, such as client A. The NAT becomes an unauthorized DHCP server for the public part of the network. The DHCP server which is responsible for addresses in the public part of the network also incorrectly starts serving addresses to clients B to F. While a careful network administrator will guard against such potential misconfigurations, less discerning users can be susceptible to such mistakes leading to address assignment problems in the whole network.

3. DHCP-WATCH

We developed a tool called *DHCP-Watch* that monitors the performance of DHCP in networks, automates the process of detecting addressing related problems, appropriately alerts the network administrators, and suggests possible remedies. DHCP-Watch uses a mix of passive monitoring and (optionally) active network scanning. The tool monitors ICMP packets, ARP frames, and DHCP/BOOTP UDP messages on a DHCP server by capturing packets, and generates real-time reports about the state of a network's address space, such as number and state of various DHCP leases, and how various types of DHCP leases fluctuate over time. Administrators can query DHCP-Watch for various traces of interest, e.g., all IP addresses used by a specific interface, or interfaces that used a specific IP address during a given time period. Additionally, DHCP-Watch infers the internal state of the DHCP servers and clients through traffic analysis and alerts network administrators as violations are discovered. DHCP-Watch optionally uses ARP scanning to get accurate information about IP to MAC address mappings as well as times when hosts go up and down. This information will allow the tool to present more accurate statistics about the state of the network and allow network administrators to use DHCP-Watch to simulate effects of changing DHCP server parameters on the network. For example, it would be possible to simulate the effects of changing lease time on the number of available leases, MAC-IP associations, etc.

Sometimes, multiple DHCP servers are used for the purpose of graceful failovers and DHCP relay agents may be used to extend DHCP services of a single server to multiple subnets. In these network configurations an instance of DHCP-Watch needs to run near each server and relay. The partial views of each DHCP-Watch instance are merged together to create a consistent global view across all servers and subnets.

Apart from using DHCP-Watch for monitoring address usage and violations in the network, its functionality can also be extended to provide temporary remedial solutions when a critical problem emerges. Consider the scenario where the entire dynamic address pool gets exhausted and the administrator knows through DHCP-Watch that some active leases are unused and will remain unused until they expire. In such a scenario, DHCP-Watch can be instructed to release the unused leases by sending the appropriate *Release* messages. Clearly, such a feature breaks DHCP and requires proper judgment of the network administrator prior to its use.

Finally, DHCP-Watch can be used by network administrators to perform capacity planning of their address space. Statistics generated by DHCP-Watch would allow network administrators choose optimal lease times, anticipate depletion of the dynamic pool before it occurs, and analyze long term network usage patterns.

4. MEASUREMENT STUDY

An early version of DHCP-Watch was used to study the performance of DHCP in two operational networks of the University of Wisconsin-Madison. Network traffic was captured using tcpdump on the DHCP servers of the studied networks and then processed off-line with DHCP-Watch. Obviously, no active scanning was done. The study was performed from April 14 to May 7, 2004.

Environment Description

The measurement study was performed on two contrasting campus networks — a small, tightly controlled "closed" network (requires authentication for each user and host), and a larger, loosely administered, "open-access" network (requires no authentication for general use). While tightly controlled, closed networks are generally more desirable and predictable than open networks, they may not always be an option. For example, some academic networks may be open and loosely-administered for reasons of convenience, such as having to accommodate frequent guest lecturers, and for reasons of necessity, such as not having the resources necessary to efficiently authenticate all users, transient or otherwise. Sometimes the open structure persists in a network for various historical and psychological reasons. The results in this section will compare and contrast DHCP performance that arises in both types of networks. The networks we examine are as follows:

Network-A: is an open-access network with 1024 addresses available. The static pool has 120 address, the dynamic pool has 420 addresses and the rest are not controlled by the DHCP server. Under typical conditions the network consists of well over 700 active hosts. The network is extremely dynamic with many hosts entering and leaving on a daily basis. The hosts on the Network-A include a large number of desktops in faculty and student offices as well student laptops used in instructional classrooms during classes. In addition, Network-A serves a large transient user base that includes, for example, frequent guest speakers in the department. To handle such dynamic scenarios, the network administrators configured the DHCP server to assign 6 hour long leases by default, while the maximum permissible lease duration is 48 hours. The distribution of hosts on Network-A is roughly as follows: 65% Windows-based OS, 30% MAC OS, and the remaining 5% consist of Linux and various flavors of Unix.

Network-B: is a tightly controlled network that provides access for VPN users and requires authentication to attain a routable address. It has a total of 256 IP addresses, of which 203 addresses belong to the dynamic pool. 15 of these dynamic pool addresses are not routable and are assigned to users who have not yet authenticated. The entire address space is used to support a total of 110 registered hosts. There is approximately an equal number of Windows (2000 or XP) and Mac OS X hosts. The default as well as the maximum lease periods for authenticated users is eight hours.

4.1 DHCP Usage Trends

We first present various properties of DHCP client behaviors of Network-A. Subsequently, we briefly present similar trends as observed in the tightly controlled environment of Network-B.

Active, Released, and Expired Leases: In Figure 2 we plot the variation of the number of active leases from the dynamic pool of Network-A for two consecutive weeks of this measurement study (for the sake of clarity). The peaks in the plot represent late mornings to early afternoons (11am to 2pm) while the troughs correspond to nights. The plot also indicates decreased activity on weekends (e.g. April 24-25). There are never fewer than about two hundred forty active leases, which was primarily because a large number of clients never relinquish their leases.

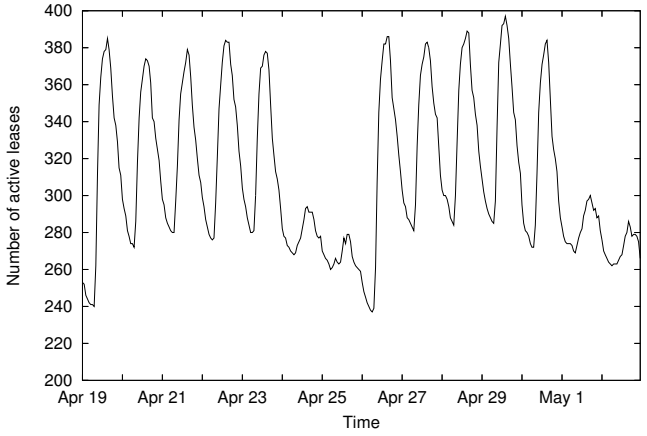

Figure 2: Variation in active Leases in Network-A

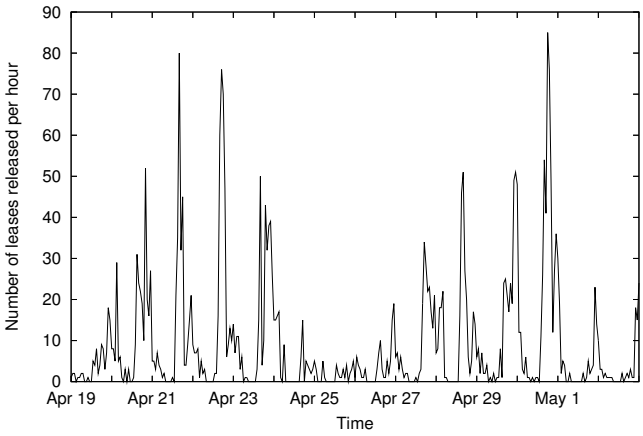

Figure 3: Lease releases in Network-A

Since the maximum size of the dynamic pool is 420, the data indicates that the dynamic pool routinely approaches to within 37 addresses of complete exhaustion. In fact, the situation is somewhat worse than that, since some of these 37 addresses are not available for assignment due to various DHCP violations (discussed in Section 4.2).

In Figure 3 we plot the number of leases that are explicitly released by the clients hourly. Such leases can be immediately re-assigned to other hosts. In most cases, leases that are allowed to expire by their owners are not used just prior to the expiration, which is wasteful. In order to reduce such wastage, the DHCP server of the Network-A instructs clients to release their leases on shutdown.

There is an inverse relationship between graphs in the Figure 2 (number of active leases) and Figure 3 (number of lease releases). For example, at the end of each day, as a number of users turn off their computers, leases are released and correspondingly the number of active leases goes down. In fact, lease release peaks occur between 4pm and 5pm on most weekdays. On Fridays the peak occurs somewhat earlier, around 2pm, due to users leaving work early for the weekend.

Lease Durations: Not all clients adhere to the release-on-shutdown directive from the server. Data collected by *DHCP-Watch* indicates that about 30% of the clients let their leases expire rather than explicitly release them. This is a common default behavior of Windows 9x/ME, and most MAC OS clients. In fact, many of the six hour leases assigned at 9 am on weekdays do not expire around the peak lease usage period (between 11am and 2pm) even though they fall idle. Hence, the current default lease duration of six hours is too long to recycle leases of transient hosts in time for the period of peak usage.

We next examined the distribution of lease durations that were negotiated by hosts in Network-A. We found that 75% of the hosts are assigned the default lease duration of six hours, and the remaining hosts negotiated the longest allowed lease time of 48 hours. Using DHCP-Watch, we determined that most of the hosts that negotiated long lease periods were network printers and OS X hosts. Such information is valuable to the network administrators in order to improve DHCP performance. For example, printers using DHCP are in violation of Network-A administrator's policy, according to which, network printers should either have reserved mappings or should not use DHCP at all. Additionally, OS X laptops, which are common in Network-A, do not always release their leases on shutdown. Such behavior significantly affects DHCP performance as the dynamic pool gets close to exhaustion. This is exemplified by the discovery of unexpectedly high number of lease expirations occurring on weekends, almost all of which were 48 hour leases acquired on Thursday and Friday by MAC OS X hosts that did not release on shutdown. The prevalence of 48 hour leases is further illustrated below.

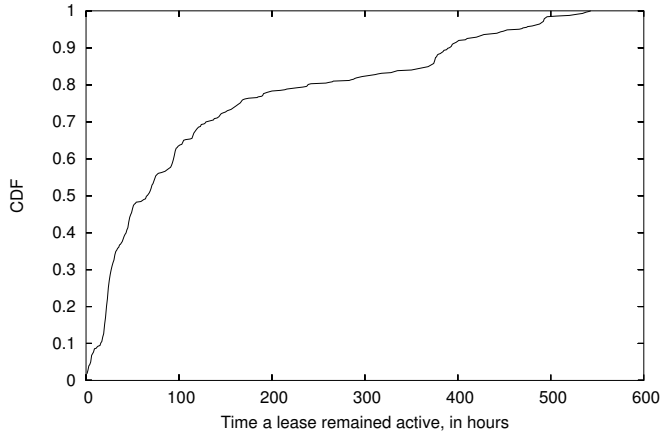

Figure 4: Lease lifetime distribution in Network-A

Figure 4 plots the cumulative distribution of the time durations for which leases were active. Such data can provide network administrators with valuable insight into network access patterns. In particular, it can be observed that about 45% of issued leases remained active for up to 48 hours. In many of those cases hosts negotiated 48 hour lease and then neither renewed nor released, even though the hosts remained on-line only for a brief period of time. The figure also indicates that a few leases remained continuously active throughout the measurement study.

Number of "persistent" hosts	IP addresses used
234	1
68	2
44	3
32	4
29	5
5	6
2	7

Table 1: Number of IP addresses used by interfaces of "persistent" hosts in Network-A.

IP Address-Interface Associations: Table 1 shows how many distinct IP addresses "persistent" hosts used over the duration of the measurement study. We define a host to be persistent if it uses DHCP's dynamic pool and accesses the network at least once every 48 hours. As it is unreasonable to expect hosts that use the network infrequently to maintain the same IP address, they are not included in the table.

For convenience reasons, it is typically desirable for hosts that frequently use the network to maintain the same IP address. Table 1 indicates Network-A's 6 hour lease achieves this goal fairly well. 234 interfaces were continually assigned the same address by the DHCP server throughout the measurement study period. The remaining 180 interfaces were bound to multiple distinct IP addresses, number of which varied between 2 and 7. DHCP-Watch will report which interfaces changed IP addresses and how often. This information can be used to justify an increase in the default lease period.

Unused Addresses: Over the duration of our experiment, DHCP-Watch reported nearly 300 addresses that were never assigned to any interface. 93 of these addresses were explicitly mapped in the static pool, the rest were outside the control of the DHCP server. The addresses from the static pool were assigned to specific hosts that had since been replaced or re-assigned and represent wasted address space. These 93 addresses can be used to increase the size of the current dynamic pool, thus significantly increasing the number of addresses available in the dynamic pool during peak periods. Normally, it is non-trivial for network administrators to realize that such an optimization is possible, but DHCP-Watch makes it obvious.

Network-B: Measurements were performed over a one-week duration. In Network-B, the number of registered users, 110, is far less than the 188 available routable dynamic IP addresses. Hence, addresses are not highly contended. Network-B DCHP server does not require clients to release on shutdown.

In Figure 5 we plot the number of active leases and the number of leases that have expired. Since Network-B clients never release, the plots mostly shows leases flipping state between *active* and *expired*. Occasionally, one of about 130 never-assigned leases would become active. We can observe the familiar daily trends in this figure — the peaks in the active leases plot correspond to day times and troughs correspond to night times. As expected, the number of active leases stays low during the weekend (May 8 and 9).

Network-B's other usage trends such as those discussed for the Network-A, do not offer insights beyond what has already been presented, and hence are omitted.

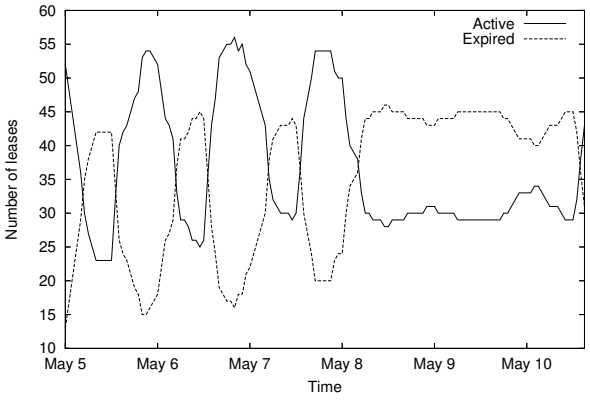

Figure 5: Active and expired leases in Network-B

4.2 Non-conforming DHCP Behavior

We now examine the non-conformant DHCP behavior in the two networks, which is summarized in Table 2.

As expected, almost all non-conforming behaviors are observed in Network-A. There were two instances when unauthorized servers were discovered in the network, due to the presence of misconfigured NATs. There were four instances of clients attempting to use BOOTP for configuration instead of DHCP. There were no address thefts from the static pool, but 11 instances of such thefts from the dynamic pool. 5 out of these 11 thefts led to lease abandonment by the DHCP server. Subsequently 3 of these abandoned addresses were reclaimed by hosts that explicitly requested them. Additionally, we detected 5 instances of IP address conflicts on addresses that are outside of the control of the DHCP server.

In both networks we observed frequent occurrences of DHCPNAKs. These are not necessarily errors. For example, a laptop that migrated into a new network would initially try to acquire its last IP address from the DHCP server. However, the last IP address may not be part of the new network, in which case the server responds with a DHCPNAK. In other cases DHCPNAKs could indicate a misconfiguration in the network, such as hosts trying to renew somebody else's lease.

Network-B provides a point of reference of how well DHCP can function. In stark contrast with the Network-A, Table 2 reveals perfect performance by DHCP in a tightly controlled closed-access network. However, for many practical, historical and psychological reasons, open-access networks are unavoidable. A tool such as DHCP-Watch can be used to better manage address resources by giving an insight into address space dynamics and thus helping to optimize DHCP configuration in open networks.

5. RELATED WORK

We are unaware of any systematic study of DHCP performance in operational networks in prior literature. However there are some related efforts that we briefly outline in this section. Perkins and Luo [7] have studied how DHCP needs to be adapted to better support host IP mobility. This work called for some specific additions and refinements to DHCP for such scenarios, which led to some of the updates to DHCP in RFC 2131 [2]. Battiti et. al. [4] explored the evolution of networks in general and increasing prevalence of open networks in particular, as well as examined the technical challenges created by open networks. In another related work, Huston [5] presents an insightful study on the current allotment and depletion trends of the IPv4 address space.

Violation Type	Network-A	Network-B
Unauthorized servers	2	0
BOOTP usage	4	0
Address theft (static pool)	0	0
Address theft (dynamic pool)	11	0
Abandoned leases created	5	0
Abandoned leases reclaimed	3	0
Address conflicts	5	0
DHCPNAKs	83	49

Table 2: Non-conforming DHCP behavior for the two networks for a seven day period.

6. CONCLUSIONS

Our measurement study indicates that DHCP performs flawlessly in tightly controlled environments (like Network-B), but address assignment violations and inefficiencies become prevalent in relatively open environments (like Network-A). As networks get larger and more complex, achieving optimal configuration of DHCP servers becomes difficult, and often involves trial-and-error. Furthermore, in large networks many violations related to address assignment are not noticed by the administrators. A tool like DHCP-Watch can go a long way to improve the administrator's understanding of address-related activities and violations, usage trends of network hosts, and utilization patterns of available addresses, which is particularly important when address space is scarce.

7. ACKNOWLEDGEMENTS

Above all, we are indebted to Steve Barnet, without whom this work would not have been possible. We would also like to thank Matthew Mueller and Ryan Schwartz for providing us with traffic captures.

8. REFERENCES

[1] B. Croft and J. Gilmore. Bootstrap protocol. RFC 951, IETF, September 1985.

[2] R. Droms. Dynamic host configuration protocol. RFC 2131, IETF, March 1997.

[3] A. Lakhina et. al. Structural analysis of network traffic flows. In *ACM Sigmetrics*, June 2004.

[4] R. Battiti et.al. Global growth of open access networks from warchalking and connection sharing to sustainable business. In *Workshop on Wireless mobile applications and services on WLAN hotspots (WMASH)*, 2003.

[5] G. Huston. Ipv4 address space: how long have we got? ARIN Today, 3rd Quarter, 2003.

[6] V. Paxson. Measurements and analysis of end-to-end Internet dynamics. Ph.D. Thesis, University of California, Berkeley, 1997.

[7] C. Perkins and K. Luo. Using DHCP with computers that move. *Wireless Networks*, 1(3), 1995.