Enhanced Intranet Management in a DHCP-enabled Environment

Jenq-Haur Wang and Tzao-Lin Lee
Department of Computer Science and Information Engineering,
National Taiwan University,
Taipei, Taiwan.
E-mail: {jhwang, tl_lee}@csie.ntu.edu.tw

Abstract

DHCP (Dynamic Host Configuration Protocol) is widely deployed in resource allocation and intranet management. However, DHCP mechanism is not mandatory, and DHCP server can neither force DHCP clients to release their leases, nor enforce cooperation from externally configured hosts that are DHCP-unaware. Although new DHCP options such as DHCP reconfigure extension have been proposed, the basic problems inherent in DHCP mechanism cannot be solved without first strengthening its operations.

In this paper, a DHCP-based infrastructure for intranet management was proposed by combining the resource allocation functions of DHCP server with the packet filtering features of MAC (Medium Access Control) bridges such as Ethernet switches and wireless access points. DHCP clients and DHCP-unaware hosts that do not abide by DHCP mechanism or our management policy will be denied network accesses by MAC bridges. Resource allocation and access control can be integrated and local configuration conflicts can be reduced to the minimum.

Keywords: intranet management, network security, wireless LAN, DHCP, MAC bridge

1. Introduction

Network security has continued to be a major issue in all kinds of applications as Internet becomes a necessity. Various types of intrusions and attacks such as DDoS (Distributed Denial of Service) are threatening the enterprises and individuals as well. Unlike attacks from the outside, local conflicts in network configurations have direct impact on the daily operations of the intranet.

The primary concern of intranet management includes allocation of resources such as IP addresses, network configuration of hosts and servers, among others. Manual configuration of hosts is prone to errors and any modification would require human interventions that are time-consuming. Therefore, DHCP (Dynamic Host Configuration Protocol) [1, 2], an extension to BOOTP protocol [3], has become more widely adopted as a mechanism for automatic and dynamic resource allocation and configuration in intranet management. Although it is commonly deployed, some drawbacks inherent in DHCP mechanism may cause more trouble than the benefits it can bring.

First of all, DHCP server cannot force DHCP clients to release their leases. DHCP server only acts as a resource dispatcher, and normally DHCP clients will not release their leases at shutdown. Although the new *DHCP reconfigure extension* option [4] can be used for DHCP server to force a "cooperative" DHCP client to renew its lease, malicious hosts may still be able to allocate new addresses without releasing them at all which would easily exhaust available IP addresses.

Secondly, since DHCP is not mandatory, externally configured hosts may deliberately or accidentally use the same network addresses as DHCP clients. For such hosts, their IP addresses are manually configured and other local network parameters can be obtained via *DHCPINFORM* requests [1]. However, *DHCPINFORM* messages are not commonly implemented. If manually configured IP addresses conflict with DHCP clients without notifying DHCP server, we cannot regulate their misuse and network disaster may occur. Furthermore, the new *DHCP reconfigure extension* option [4] can only be used for cooperative DHCP clients, not DHCP-unaware hosts.

In order to make the most of DHCP, we have to strengthen its power of regulation. New options such as *DHCPINFORM* and *DHCP reconfigure extension* have to be enforced and integrated into the infrastructure to make DHCP clients more manageable. In addition, there must be a mechanism to force DHCP-unaware hosts to cooperate with DHCP management policy. Once non-cooperating hosts are detected, we will alert them by *DHCP FORCERENEW* or RHCP (Remote Host

Proceedings of the 26 th Annual International Computer Software and Applications Conference (COMPSAC'02)
0730-3157/02 $17.00 © 2002 **IEEE**

Configuration Protocol) [5] messages. That means intranet hosts need to be extended by DHCP/RHCP processing modules to receive instructions from management server, in this case, a DHCP server. If they still don't abide by the instructions, we will restrict their network access rights at bridges. With appropriate enforcement of network access control in MAC bridges, we can compensate the disadvantages of DHCP mechanism and local conflicts can be reduced to the minimum. On the other hand, MAC bridges can also be enhanced with address allocation flexibility. Mechanisms for access control and notification of invalid connection attempts are possible in this infrastructure.

2. Motivation

In our previous work [6], a mechanism for extending DHCP capabilities with MAC-layer user authentication was proposed, as shown in Fig. 1.

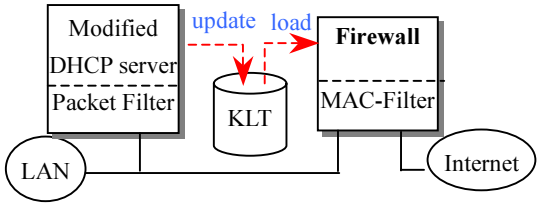

Fig. 1 shows the infrastructure of DHCP-Firewall combination in our previous work [6] where KLT is the Kernel Lease Table that maintains DHCP lease information at kernel level.

As shown in Fig. 1, DHCP server was coupled with firewall in order to regulate local hosts from network address misconfiguration. However, firewalls are not always deployed in all kinds of network configurations although it's better to have one. In ordinary LAN environment, bridges and routers are more widely used.

In traditional Ethernet, hubs are used as a multiport repeater connecting local hosts. Traffic generated at one port will be forwarded to all other ports in a hub. However, since the nature of Ethernet is CSMA/CD (Carrier Sense Multiple Access/Collision Detection) bus, as the number of hosts in a domain grows, the chance of packet collision becomes much higher. Therefore, bridges are commonly adopted in a local area network to avoid unnecessary packet collisions among different hosts. For example, consider a small enterprise consisting of several departments in the same building. Traffic inside each department has better be contained within its own collision domain.

As the number of hosts grows, the extraordinary broadcast packets may cause unnecessary traffic in a LAN. Therefore router goes one step further in containing broadcast packets in each domain. As new technology evolves, switches are getting more attention. Layer 2 switches are just bridges with more fancy features such as VLAN (virtual LAN) and full-duplexing on separate port, and layer 3 switches incorporate network layer address handling functions except routing. In such environment, we can actually combine DHCP server with layer 2/3 switches since all packets must go through these switches.

Network planning had to accommodate building structure and wiring in the old days, and it's usually annoying and complicated. Thanks to the new transmission media, we may also want to deploy wireless LANs [7] as less wiring is needed in most of the offices. In such cases, wireless access points become the bridge between wired and wireless networks.

3. DHCP-based Management

3.1. Infrastructure

As a matter of fact, we can enforce access control in whatever types of MAC bridges. Our main idea is to combine the resource management function of DHCP server and the access control function of bridges. Manually configured hosts are encouraged to utilize *DHCPINFORM* or RHCP messages to inform DHCP server of their network address configurations. Alternatively, a simple registration step may be used for each new user or a user with a new NIC (network interface card) prior to his first Internet connection as in our previous results [6]. As shown in Fig. 2, a general infrastructure for DHCP-based management is illustrated.

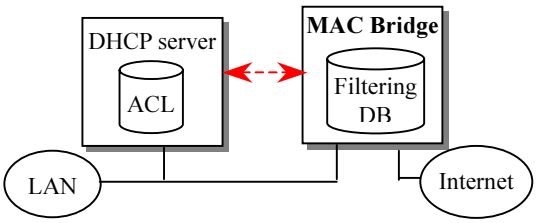

Fig. 2 shows the basic infrastructure of DHCP-Bridge Combination.

The idea is simple: we keep track of an access control list (ACL) of hardware address and network address pairs for authorized hosts, namely *(MAC, IP)* pairs, and then enforce the ACL by the Filtering Database in MAC bridges [8]. Our policy is to protect those hosts that are pre-configured (externally configured hosts like servers), registered, or DHCP-aware. For all other hosts, we will not protect their packets from being filtered. All packets with unauthorized *(MAC, IP)* pairs will be dropped by bridges.

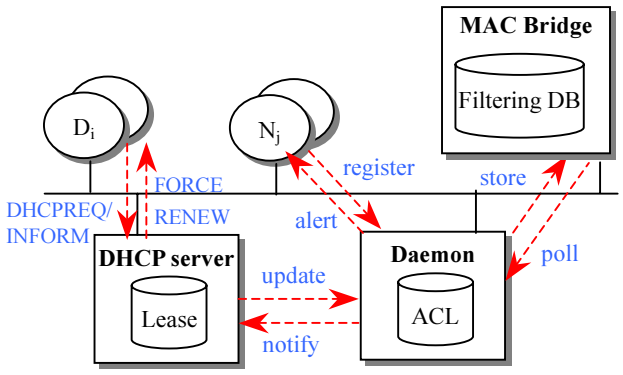

Fig. 3 shows the interactions among DHCP server, Monitoring Daemon and MAC bridge, where D_i denotes DHCP clients and externally configured hosts that are DHCP-aware, and N_j denotes DHCP-unaware hosts.

In Fig. 3, a common network configuration where hosts are connecting through MAC bridges to the Internet is illustrated. In this infrastructure, two components are needed: DHCP server for resource allocation and a monitoring daemon for keeping an access control list (ACL). ACL is corresponding to the Filtering Database in MAC bridge which actually performs packet filtering and forwarding. On the one hand, monitoring daemon is responsible for receiving ACL update requests from DHCP server and enforcing ACL modifications into Filtering DB on MAC bridge. On the other hand, it is responsible for polling statistics of packets flowing through MAC bridges, and sending notifications of illegal connection attempts to DHCP server. Therefore, it is the "bridge" or "proxy" between the DHCP server and MAC bridges.

For DHCP-unaware hosts, registration is needed as an authentication for hosts. In our infrastructure, registration server can be put on the same host as monitoring daemon. Therefore, monitoring daemon is also responsible for receiving registration requests and sending *Force Register* messages in response to illegal connection attempts from hosts without registration.

3.2. Basic Operations

The basic operations among the key components of our infrastructure for DHCP-based management work as follows:

(1) Hosts Authentication and ACL Collection

For DHCP clients, it's mandatory to make lease allocation or renewal requests (*DHCPDISCOVER* / *DHCPREQUEST*) to DHCP server. It is therefore natural for DHCP server to verify and authenticate their MAC addresses in the process of handling their requests. Note that our DHCP server will check not only the '*Client Identifier*' option but also the '*chaddr*' field [1] in DHCP requests and match them with the authentic MAC address in the Ethernet header of packets. Therefore, only one legal IP address at a time can be allocated for each MAC address, hence for each Ethernet adaptor. This keeps malicious hosts from allocating new addresses without releasing them as described earlier in the introduction, even if malicious hosts are DHCP-aware.

For externally configured hosts, such as intranet servers, system administrator may choose to configure their leases manually in DHCP server, or in a more dynamic way, configure them to notify DHCP server of their externally configured IP address via *DHCPINFORM* messages if supported. Although *DHCPINFORM* is specified in RFC 2131 [1] as a required feature, not many externally configured hosts support this option.

DHCP leases maintained on DHCP server will be translated into ACLs and upated accordingly on daemon, which will then be enforced into Filtering Database on MAC bridge.

For DHCP-unaware hosts, authentication can be done by our registration server as in [6], and their *(MAC, IP)* pairs will also be marked as legal in the process of registration.

(2) ACL Enforcement and Notification

Since a transaction log is kept for recording any illegal connection attempts on MAC bridge, packet statistics can be periodically polled by daemon and a list of illegal *(MAC, IP)* pairs can result.

For DHCP clients on the list, daemon will notify DHCP server which will then send *FORCERENEW* messages to notify DHCP-aware hosts of their illegal *(MAC, IP)* pairs. This will trigger renewal of DHCP leases.

For DHCP-unaware hosts on the list, they will be alerted directly by daemon via RHCP messages and re-registration will be triggered.

3.3. Client-Server Interactions

As illustrated in Fig. 4, there are four possible cases of client-server interactions in our infrastructure. First of all, when DHCP client C_1 obtains its lease through normal DHCP procedures as shown in Fig. 4(a), DHCP server S will inform monitoring daemon D of a valid pair (MAC_{C1}, IP_{C1}). The monitoring daemon will then pass the updated part of ACL to bridge B. Packets from C_1 can then pass through the bridge.

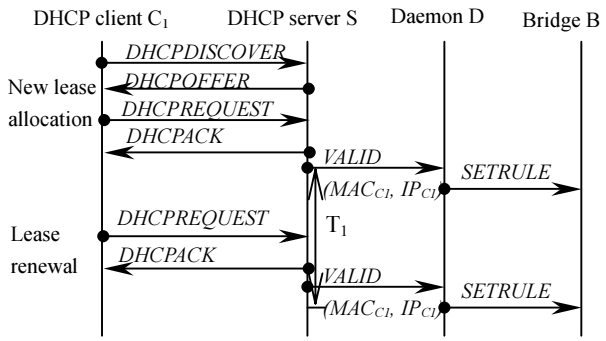

Fig. 4(a) shows the first case of client-server interactions where DHCP client C_1 allocates and renews its lease automatically in normal cases.

Secondly, after time duration T_1 DHCP server S finds out that the lease of DHCP client C_1 will soon expire. If C_1 renews its lease automatically, things will go in its normal way. However, as illustrated in Fig. 4(b), if C_1 doesn't renew its lease, DHCP server will send a *FORCERENEW* message [4] to force C_1 into *RENEW* state. Then C_1 will try to send *DHCPREQUEST* message to renew its existing lease as in normal cases. If for some period of time τ_1 (a configurable parameter) C_1 still doesn't renew its lease, DHCP server will inform the monitoring daemon of an invalid pair (MAC_{C1}, IP_{C1}) and packets from C_1 will be prohibited from passing through bridge B. If C_1 renews its lease at a later time, DHCP server S either allocates a new lease or renews the old one, and informs the monitoring daemon of such changes.

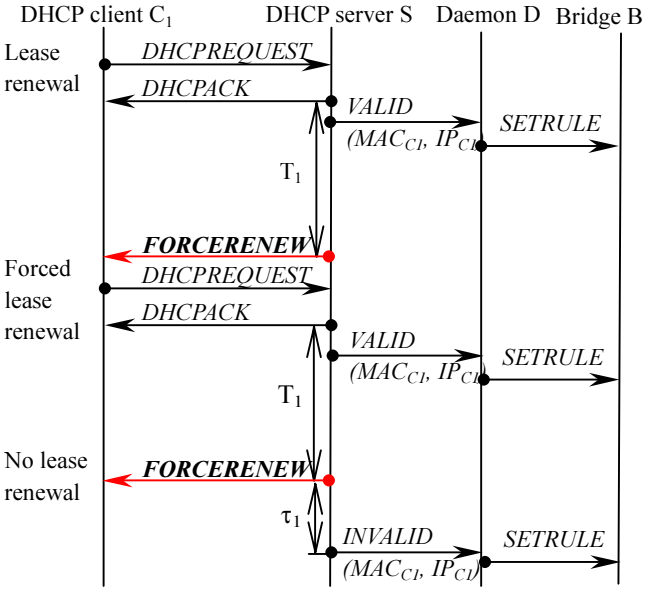

Fig. 4(b) shows the second case of client-server interactions where DHCP client C_1 renews its lease automatically in normal cases. If C_1 doesn't renew after lease expires, DHCP server S will send *FORCERENEW* message to it. If for some period of time τ_1, C_1 still doesn't renew its lease, (MAC_{C1}, IP_{C1}) will be marked as invalid pair.

Thirdly, when a non-DHCP host D_1 registers to monitoring daemon via some registration procedure or notifies to DHCP server S via *DHCPINFORM* messages, monitoring daemon will inform the valid pair (MAC_{D1}, IP_{D1}) to bridge B. D_1 will then be able to connect through the bridge. The process is shown in Fig. 4(c).

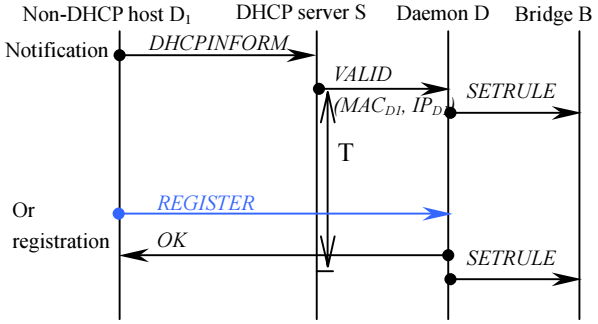

Fig. 4(c) shows the third case of client-server interactions where non-DHCP host D_1 notifies with *DHCPINFORM* message to DHCP server or registers via registration client to Daemon D.

Lastly, when a manually configured host N_1 makes its connection attempts as shown in Fig. 4(d).

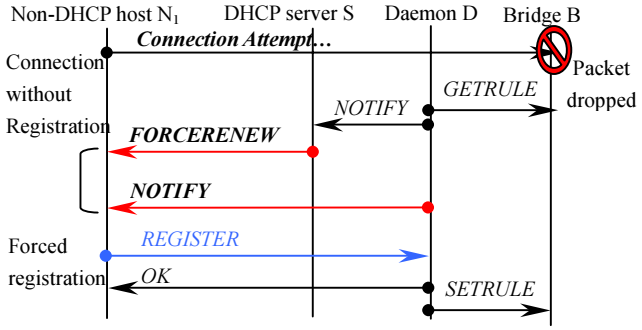

Fig. 4(d) shows the fourth case of client-server interactions where non-DHCP host N_1 attempts to connect without registration. N_1 will be denied of Internet access until registration is completed.

Since N_1 is not registered to monitoring daemon D, bridge B will by default drop its packets and mark (MAC_{N1}, IP_{N1}) as invalid. Daemon D will periodically poll from the system logs of bridge B and get the list of such illegal hosts. Then daemon D will either send *RHCPRENEW* messages to these illegal hosts one by one or notify DHCP server S, which in turn sends *FORCERENEW* messages. When N_1 receives such messages, it can either respond with registration requests

to daemon D or it can send *DHCPINFORM* message to DHCP server S. If neither was done, after a period of time τ_1 (a configurable parameter), DHCP server will inform daemon D of an invalid pair (MAC_{N1}, IP_{N1}) and N_1 will be prohibited from passing through bridge B as in the second case above.

4. Deployment Issues

In a switched environment, our DHCP-based management infrastructure can be illustrated as in Fig. 5.

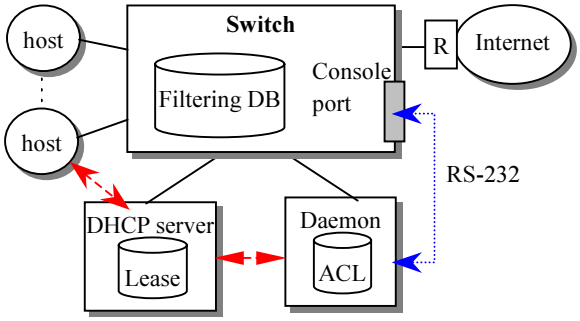

Fig. 5 shows the DHCP-based management infrastructure in a switched environment.

Monitoring daemon is configured to connect through two interfaces: an Ethernet link to contact with DHCP server and other hosts, and a RS-232 link to collect information from and enforce rules to the switch. Note that DHCP server could be standalone or integrated with monitoring daemon. If DHCP server is combined with monitoring daemon, some traffic can be reduced but the load would be higher. Slight overhead under such switched environment is inevitable unless the daemon/DHCP server modules could be hardwired into the switch.

For ordinary layer 2 switches, Filtering Database can be accessed in many ways, for example, through the web interface, Telnet, SNMP (Simple Network Management Protocol) [9], or via a console port dedicated for management purposes, as in the case of 3Com SuperStack II Switch 3300XM [10].

In the case of wireless bridges, access points are often hardware-based, which is difficult to configure dynamically according to our needs. Therefore, in our solution, a software AP is incorporated into the infrastructure on which we can build Filtering Database for regulating the traffic across it as shown in Fig. 6.

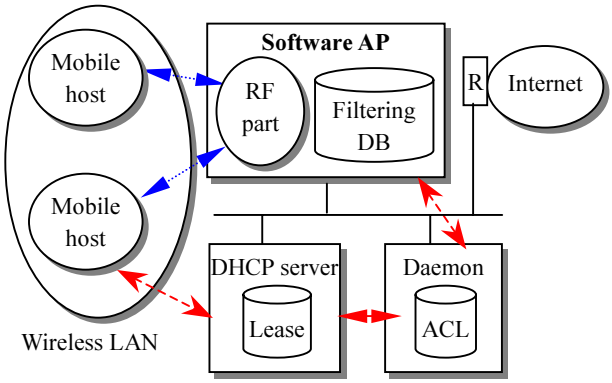

Fig. 6 shows the DHCP-based management infrastructure in a wireless environment.

However, there are some differences between these two infrastructures. Firstly, monitoring daemon needs not but would be better integrated into the software AP as a module. In the case of wired environment, a daemon module cannot be integrated into a hardware-based switch unless the switch is re-designed to do so. That's the reason why we incorporate a software-based AP instead of hardware-based one. Actually, we could also use normal hardware-based AP since under normal configurations it will eventually connect through switches somewhere in the switched environment. The advantage of software AP is its flexibility and access control at the very first point of attachment for mobile hosts.

Secondly, DHCP server will usually be on the Ethernet-side of the AP rather than the RF-side. That means DHCP requests from mobile hosts will pass through the software AP to DHCP server that incurs overhead for both wireless LAN and the Ethernet. If DHCP server is also integrated into the software AP, more traffic will be reduced on both wired and wireless networks.

5. Implementation Issues

5.1. Layer 2 vs. Layer 3 Switches

For layer 2 switches, only MAC addresses are inspected and added into packet filtering rules of Filtering Database. Such level of control is not tight enough in some cases as shown in the following IP-spoofing example.

In the first place, when hosts A and B with (MAC_A, IP_A) and (MAC_B, IP_B) respectively are trusted by our server, layer 2 switch will mark MAC_A and MAC_B as authorized. However, when trusted host A tries to send packets using the same IP address as trusted host B, layer 2 switch will not notice invalid packets from (MAC_A, IP_B) since the Filtering Database lacks layer 3 information

when trying to keep track of invalid host connections. This will cause big problems since unauthorized hosts can gain access rights in this way.

On the other hand, with layer 3 switches, the problem can be solved since the Filtering Database could contain both layer 2 and layer 3 information, i.e. all valid *(MAC, IP)* pairs. In the above example, layer 3 switch will mark (MAC_A, IP_A) and (MAC_B, IP_B) as authorized pairs. When host A starts sending spoofed packets with (MAC_A, IP_B), layer 3 switch will notice these spoofed packets and no access will be allowed from host A.

5.2. Integrated vs. Separated Modules

In our infrastructure, monitoring daemon and DHCP server are separated for illustration purpose only. In real implementation, we could have combined these two modules and experienced less overhead for inter-process communications. However, as individual functional modules, DHCP-related functions are better put together in a DHCP server module while communications between DHCP server and bridges in another separate monitoring module. That would be a cleaner design.

5.3. DHCP vs. RHCP options

In RFC 3203 [4], it's not clearly specified when and how to trigger *DHCP FORCERENEW*. In our infrastructure, it's triggered by illegal connection attempts of DHCP-unaware hosts. With the installation of appropriate DHCP/RHCP modules on them, notification can be done via *DHCP FORCERENEW* or RHCP messages.

6. Conclusion

As new network technologies and applications are being developed, intranet management plays a critical role in both wired and wireless networking environments. Even with the widespread deployment of DHCP mechanism, there would still be more problems if it couldn't be enforced among DHCP clients as well as manually configured hosts.

In this paper, we proposed a management infrastructure that strengthens DHCP with MAC bridges such as Ethernet switches and wireless access points. We also showed some possible uses of new DHCP options like *DHCPINFORM* messages and *DHCP reconfigure extension*. The advantage of this combination of DHCP server and MAC bridge is two fold. Firstly, functionality of MAC bridge can be enhanced by address allocation flexibility. Secondly, DHCP mechanism can be strengthened by MAC bridge. If this management scheme is carried out over the whole intranet, both DHCP clients and DHCP-unaware hosts can be regulated under the same infrastructure. Local configuration conflicts can thus be reduced to the minimum, and a better networking environment can be expected.

7. References

[1] R. Droms, "Dynamic Host Configuration Protocol," *RFC 2131*, IETF, March 1997.

[2] S. Alexander and R. Droms, "DHCP Options and BOOTP Vendor Extensions," *RFC 2132*, IETF, March 1997.

[3] W. Wimer, "Clarifications and Extensions for the Bootstrap Protocol," *RFC 1542*, IETF, October 1993.

[4] Y. T'Joens, C. Hublet and P. D. Schrijver, "DHCP reconfigure extension," *RFC 3203*, IETF, December 2001.

[5] J. H. Wang, Tzao-Lin Lee, and Hsi-Hui Lin, "Remote Host Configuration Protocol: Configuring a Remote Host in a User-Friendly Manner," *Proceedings of the 14th International Conference on Advanced Science and Technology (ICAST 98)*, pp. 303-314. Illinois, U.S.A., April 1998.

[6] J. H. Wang and T. L. Lee, "Extending DHCP with MAC-Layer User Authentication," *Proceedings of the 1st International Workshop on Software Engineering and Multimedia Applications*, pp. 151-155, Baden-Baden, Germany, August 1999.

[7] IEEE Standard for Information Technology – Telecommunications and Information Exchange between System – Local and Metropolitan Area Networks – Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, *ANSI/IEEE Std 802.11-1999 Edition*, 1999.

[8] IEEE Standard for Information Technology – Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Networks – Common Specifications – Part 3: Media Access Control (MAC) Bridges. *ANSI/IEEE Std 802.1D, 1998 Edition*, 1998.

[9] J. Case, M. Fedor, M. Schoffstall, and J. Davin, "A Simple Network Management Protocol (SNMP)," *STD 15, RFC 1157,* IETF, May 1990.

[10] 3Com Corporation, *SuperStack II Switch: Management Guide*, April 1999.