INTERNATIONAL JOURNAL FOR TRENDS IN ENGINEERING & TECHNOLOGY
VOLUME 20 ISSUE 1 –FEBRUARY 2017 - ISSN: 2349 – 9303

Assigning Static Ip Using DHCP In Accordance With MAC

J.Ramprasath[1]
[1] *Dr.Mahalingam College of Engineering and Technology,*
Department of Information Technology,
jrprasath@gmail.com

M.Aswin Yegappan [2]
[2] *Dr.Mahalingam College of Engineering and Technology,*
Department of Information Technology,
withaswin5115@gmail.com

Dinesh Ravi [3]
[3] *Dr.Mahalingam College of Engineering and Technology,*
Department of Information Technology,
dineshravii96@gmail.com

N.Balakrishnan [4]
[4] *Dr.Mahalingam College of Engineering and Technology,*
Department of Information Technology,
balki91@gmail.com

S.Kaarthi [5]
[5] *Dr.Mahalingam College of Engineering and Technology,*
Department of Information Technology,
kaarthi94@gmail.com

Abstract— The paper "Assigning Static IP Using DHCP In Accordance With MAC" aims at automatically assigning IP address into a machine with respect to the MAC address of the machine. DHCP is a network protocol that enables a server to assign IP address to computers automatically from a defined range of numbers that is configured for a given network. Integrating DHCP through the kernel the allocation of IP is carried over. Initially the IP's are fed statically for the mac addresses along with which the reservations are added and filters are applied. Once this process is completed the IP's with respect to its corresponding machine's mac address will be allocated dynamically to the machine whenever it is identified by the DHCP.

Index terms- Assigning Static IP,Defined range, kernel, dynamic addressing capabilities

1. INTRODUCTION

The project is entirely dealt upon the existing DHCP protocol. It is available as a service in most of the server operating system. DHCP is a client/server protocol that will automatically assign IP to host with its IP address and other related configuration that is assigned to the particular client such as the subnet mask and default gateway. RFCs 2131 and 2132 define DHCP as an IETF standard based on BOOTP, a protocol with which DHCP shares many implementation details. DHCP allows hosts to obtain required TCP/IP configuration information from a DHCP server.

With DHCP, this entire process will be automated and managed centrally by a server which is configured using DHCP protocol. The DHCP server maintains a pool of IP addresses and the leases of those addresses to any DHCP enabled client when it starts over a network. Since the IP addresses are dynamic they can be assigned instantly (leased) rather than static (permanently assigned), addresses are no longer in use are automatically returned to the pool for the purpose of reallocation. The lease period being 999 days for a DHCP service is more than enough. The paper focuses on two things one being the MAC address detection and the other adding reservation.

Protocols like BOOTP and DHCP are used to detect the MAC address of the machine. For that purpose, we should enable the DHCP services in the client machines. Only then the server will be able to detect the MAC of the particular machine. Similarly, the DHCP service should be enabled in the server machine. Once a client machine is turned on the server will detect the machine's MAC and will be displayed in the DHCP protocol of the server machine. Once all the MAC address of a computer is detected we will assign each MAC address with an IP address and we can use two modes in assigning IPs they are BOOTP and DHCP. Once this reservation is added they will be automatically discovered and offered to the clients by the server.

2. LITERATURE SURVEY

DHCP predominantly works on a client-server model. Being a protocol, it has its own set of messages that are exchanged. When the client computer (or device) boots up or is connected to a network, a DHCPDISCOVER message is sent from the client to the server. When the DHCP server receives the DHCPDISCOVER request message then it replies with a DHCPOFFER message. The client forms a DHCPREQUEST message in reply to DHCP OFFER will create a message and will send it to the server indicating it wants to accept the network configuration sent by the DHCPOFFER message. Once the server receives DHCPREQUEST from the client, it sends the DHCP ACK message indicating that now the client is allowed to use the IP address assigned to it. The main drawback here is that there is no guarantee that the machine will be assigned with the same IP address overtime. This is a serious drawback identified that which user is currently using the machine in a network, that too of a fraudulent activity is detected in a network too cannot be identified

with the user who is doing it because there is no fixed or trusted information about the user who is using it so this will become very difficult task to be rectified so this system is overcome this effect in the network. This is the drawback that we are modifying in our system.

3 PROPOSED SYSTEM

Initially enable DHCP service in both Client and Server machines. Once a client machine is turned on the machine will make its MAC address and its personal details to be discoverable in the network, the DHCPDISCOVER protocol in the server will sense the MAC address of the client machine and sends the MAC information of the machine to the server. The server will identify the MAC address and will check with the reservations added by the server administrator. For each reservation found for a sensed MAC address it will be allocated an IP address that is predefined. The IP address will be sent to the client machine by the DHCPOFFER service using the UDP protocol and will wait for the acknowledgment from the client that it has accepted the IP address. Each MAC address will be added with a reservation, so we can reduce the fraudulent activities in the network because we will have the complete information of the user and if we detect any fraudulent activity in the network we can immediately find who is the person responsible for such activity and we can reduce such activities in future.

Mac Address Detection

Using protocols like BOOTP and DHCP we will detect the MAC address from the kernel running in the DHCP client system and send to the DHCP server.

IP Address Scope Configuration

Scope is a feature that is already available in the Windows Server Operating System that will enable us to create new scope. In this scope configuration has subdivisions they are

Address pool

By default, the router acts as a DHCP server . The router assigns IP automatically when the client is enabled with DHCP Client, DNS server, and default gateway addresses to all computers connected to the common LAN. The default gateway address is nothing but the LAN address of the router.

Address leases

A DHCP-enabled client obtains a lease for an IP address from a DHCP server. Before the expiration of lease, the DHCP server must assign a new lease for the client [1]. Leases are retained in the DHCP server database approximately one day after expiration.

Reservations

DHCP Reservation is an advanced feature on the Linksys Wi-Fi Router. The reservations are especially useful for setting up a computer network as well as wired or wireless network for devices like printers, network storage, server computers, or game device that you want to have access using a specific IP Address [4].

Scope options

Lease duration values that are assigned to DHCP clients will receive allocated IP addresses dynamically. Any DHCP scope options is configured for assignment of IP address to the DHCP clients, such as DNS server, router IP address, and WINS server address [4].

Access Control List

An ACL, with respect to a computer file system, specifies which users or system processes are given access to objects, as well as what operations are allowed on given objects in that particular request. In each entry in a typical ACL specifies a subject and an operation. For this instance, if a file object has an ACL that contains (person1: read, write; person2: read), this would give person1 permission to read and write the file and person2 to only read it [4].

4 CONCLUSION

The DHCP protocol is being used widely and is used every day by almost everyone who connects their machine to a network. All network engineers must have at least a basic knowledge of how this process is and how the network flow works and how it can be configured to make the network secured and efficient. The limitations in the existing system are identified and we have taken into consideration and developed this system of adding reservations to overcome it. Thus, the fraudulent activities that take place in the network is been minimized. The users causing the fraudulent activity are spotted in this system because we have the user machine's personal details (MAC and IP address).

It is true that with these dynamic addressing capabilities, The Network Managers can save money, time and make their networks more robust and secure. DHCP has grown from a tool to simply apply IP addresses to a link-local interface to a multifaceted networking tool, which is invaluable for the maintenance of large-scale networks. IP Addresses can be allocated and de-allocated across the whole world, due to Relay Agents and DHCP servers. As network architecture and capabilities change, DHCP has continued to change a long side in offering Network Administrators more automation in the allocation of addresses, and much more speed in renewing of leases to the particular nodes. With application of IPv6 multicast abilities, DHCP's abilities will also increase in terms of accessing multiple nodes at a single time. It can be concluded from this that even though DHCP is an integral part of the Internet and an established protocol in network management, it still has to make constant changes and evolve, in order to coexist with the changing and evolving world of networking.

Now the system developed by us is limited with number of gateways in the network. In future, it can be enhanced with creating a network of more than one gateway and it can be sub netted and super netted.

5 REFERENCE

1. P. Wu et al., "Transition from IPv4 to IPv6: A State-of-the-Art Survey," IEEE Comm. Surveys & Tutorials, Dec. 2012, pp. 1407–1424.

2. B. Carpenter et al., Transmission of IPv6 over IPv4 Domains without Explicit Tunnels, IETF RFC 2529, Mar. 1999; www.ietf. org/rfc/rfc2529.txt.

3. E. Nordmark, Stateless IP/ICMP Translation Algorithm (SIIT), IETF RFC 2765, Feb. 2000.
4. G. Tsirtsis et al., Network Address Translation-Protocol Translation (NAT-PT), IETF RFC 2766, Feb. 2000; www.ietf.org/rfc/rfc2766.txt. 5. B. Carpenter et al, Connection of IPv6 Domains via IPv4 Clouds, IETF RFC 3056, Feb. 2001;.
5. T. Mrugalski et al., "DHCPv6 Options for Configuration of Softwire Address and Port Mapped Clients," IETF Internet draft, work in progress, Mar. 2014.
6. M. Boucadair et al., "(DHCPv6) Options for Shared IP Addresses Solutions," IETF Internet draft, work in progress, Dec. 2009.
7. Q. Sun and Y. Cui, "DHCPv6 Option for IPv4 Configuration," IETF Internet draft, work in progress, Feb. 2013.
8. B. Rajtar et al., "Provisioning IPv4 Configuration over IPv6 Only Networks," IETF Internet draft, work in progress, Feb. 2014.
9. Y. Cui et al., "DHCPv4 Behavior over IP-IP Tunnel," IETF Internet draft, work in progress, July 2011.
10. O. Troan, "DHCPv4 over A+P Softwires," IETF Internet draft, work in progress, June 2013.
11. Y. Cui et al., "DHCPv4 over IPv6 Transport," IETF Internet draft, work in progress, Oct. 2013.