**Dynamic Host Configuration Protocol (DHCP)**

Thomas Hoffman

Taha Siddique

Percentage of Participation:

Thomas Hoffman: Introduction, Background, Address Allocation, Security Issues

Taha Siddique: Rationale, Request for Comments, DHCP for IPv6, Conclusion

**Introduction**

Dynamic Host Configuration Protocol, or DHCP, is a very widely used network protocol. DHCP was first mentioned in RFC 1531, which was released in October 1993. This version had many flaws, which led to an updated RFC 2131 in March 1997. RFC 2131 is still the standard for IPv4 networks today. On a basic level, DHCP allows devices to request Internet Protocol parameters from a network server. One of the main parameters DHCP provides is automatically allocating IP addresses to these devices when they are requested.

**Background**

DHCP uses UDP to transport messages. The main reason for this addressing issues that come along with the protocols purpose. Most of the messages that are exchanged when using DHCP are broadcast throughout the local network, so there is no specific destination until the end of the transmission. With this, it’s unreasonable to attempt to set up a reliable TCP connection between the client and host. DHCP has the client and servers communicate on UDP port 67 for the server destination port and port 68 for the client destination port (Kozierok, 2005).

**Address Allocation**

DHCP has three methods of allocation for IP addresses. The most popular of these is dynamic allocation. With dynamic allocation, DHCP will assign the IP address to the client for a finite time period. This lease time is able to be set and changed by the network administrator. Once the lease time is over, or if the client releases the IP address, the IP address is reclaimed by the network and can be given to a new client. The other two methods do not allow the network to reuse an IP address. In automatic allocation, an IP address is permanently assigned to the client. With this, if a client leaves the network and returns, they will retain the same IP address. In the time that the client is off the network, the IP address is unable to be used. Manual allocation works similarly to this, except the IP address is manually assigned by the network administrator. DHCP has no responsibilities except to pass this preset network address to the client when it is requested. There are certain situations where manual or automatic allocation would be preferred, but in most situations, dynamic is the mechanism of choice.

The allocation of IP addresses is done with a scripted client-server interaction. First, the client will broadcast a ‘DHCPDISCOVER’ message to its local subnet with option parameters of network address and lease time preferences. The server will respond with a ‘DHCPOFFER’ message with an available network address. The server doesn’t necessarily have to reserve the address that was sent in this message, but some still choose to do so since it increases the protocol’s efficiency. When the client receives this message from the server, it will choose which network address offered that it will like to accept. The client will send out a ‘DHCPREQUEST’ message that has the server who’s offer has been accepted as well as the network address that the client would like to accept. When the server receives the ‘DHCPREQUEST’ message, it will respond with a ‘DHCPACK’ message that has additional parameters for the client’s network configuration. If the server was unable to handle the ‘DHCPREQUEST’ message from the client, whether because the network address is no longer available or for other reasons, it will reply with a ‘DHCPNAK’ message instead of the ‘DHCPACK’. The ‘DHCPNAK’ will tell the client to restart the process. If the client receives the ‘DHCPACK’, it is now fully set up with this allocated IP address. If the client wants to release the IP address as mentioned with dynamic allocation, it will send a ‘DHCPRELEASE’ message to the server. A client is able to request a previously owned IP address by dropping some of the initialization messages sent in the beginning (Droms, 1997).

**Security Issues**

Since DHCP uses UDP and Internet Protocol, it is expected that it would inherit some of the security flaws. An unauthorized DHCP server can be easily set up. This allows for malicious activity including sending false and/or excessive information to a client. It may also send routing information that isn’t correct to a client. This is known as spoofing. On the other end, a client could pose as another client and intercept the data that was intended for another client. Doing this, a malicious client could become a resource hog by retrieving all of the resources available. This causes legitimate clients to have no resources available for use (Droms, 1997).

**Rationale**

DHCP is a very significant protocol and there are many reasons one might use it over manual IP address configuration. First, DHCP makes setting up networked devices simple, as users will not need to know the specifics of IP address configuration and can let it be automated.

Using DHCP will generally lessen the burden placed on the network administrator. DHCP takes over the tedious task of setting each IP address configuration that the network administrator does not usually need to worry about. Without DHCP, the administrator would need to manually remove IP addresses when devices are permanently removed from the network. Additionally, if you have static IP addresses set for your devices, then it is easier to make network changes. Rather than having to go to each device and change the configurations, with DHCP the network admin can simply make the change on the server and it should go through to all of the devices (Locutus, 2007). This is increasingly important with the increased connectivity we are seeing with the Internet of Things. Some appliances and integrated devices might not allow for easy setup without DHCP. Lastly, using DHCP instead of manually setting IP address configurations eliminates a lot of human error, as the server cannot make any typing mistakes like a human could (“What is DHCP”, 2003).

**Request for Comments**

There are two very important Request for Comments (RFC) in regards to Dynamic Host Configuration Protocol (DHCP), namely RFC 1531 and RFC 2131. RFC 1531 is the initial documentation defining DHCP's format, method, and usage specified in 1993. The document was quickly replaced with RFC 1541 because it contained errors that were introduced during editing. In this document, the author explains that DHCP expands upon the previous BOOTP technology by eliminating the need for the manual configuration of BOOTP. Additionally, the initial format for the DHCP message and design for the interaction between devices using DHCP is specified in this RFC (Droms, 1993).

Four years later it was revised in RFC 2131, because there was several overlooked issues with the original version. There were several changes that came with RFC 2131. First, the author added a new DHCPINFORM message type that is used to get several local variables. This message is needed if a device was manual configured, as it allows the device to obtain other needed information such as network mask, gateway, domain name, host name, DNS address, etc. Also this RFC removed a previously set minimum lease time that was specified in RFC 1531. The last major change was the new version allowed a network admin to set the DHCP server to only respond to certain devices based on a previous authentication or vendors (Droms, 1997).

**DHCP for IPv6**

With the increased and imminent usage of IPv6, a modified version of DHCP is needed to allocate the new addresses. This version was specified in 2003's RFC 3315, and the protocol is named DHCPv6. With this new protocol, DHCP is able to allocate and configure IPv6 addresses. The new DHCPv6 does not use a MAC address, but instead uses a Device UID (DUID). This is because a host can now have multiple IP interfaces. DHCP uses this new DUID and generates an IP address and necessary fields for it (Droms, 2003).

**Conclusion**

In summation, Dynamic Host Configuration Protocol is an integral piece of technology with today's networks. DHCP allows simple configuration and allocation of IP addresses, which enables the average person to connect their device to a new network without much trouble. DHCP has been used in networking to assign IP addresses for a long time now, and with refinements will be capable of use in new IPv6 networks. Clearly, DHCP is an incredibly useful and widespread protocol that will last for well into the future of networking.

Second sentence under background needs fixed I think

a source I used did not have author names, I think article title and date are proper for inline citations