DHCP Service - Railways perspective

J Vijay Kumar, Instructor, IRISET
D Anandam, Instructor, IRISET

Abstract

Dynamic Host Configuration Protocol (DHCP) is one of most important tool in the repertoire of a network administrator. It allows automatic configuration of computers and other IP devices on the network. With VoIP telephony being inducted in the Railways, use of DHCP will become quintessential. This article examines DHCP and suggests a method for its configuration in Railnet so as to provide a reliable service meeting Railways special requirement.

1 Introduction

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.

DHCP employs a connectionless service model, using the User Datagram Protocol (UDP). It is implemented with two UDP port numbers for its operations. UDP port number 67 is the destination port of a server, and UDP port number 68 is used by the client. These ports are important if the DHCP server is protected by a firewall.

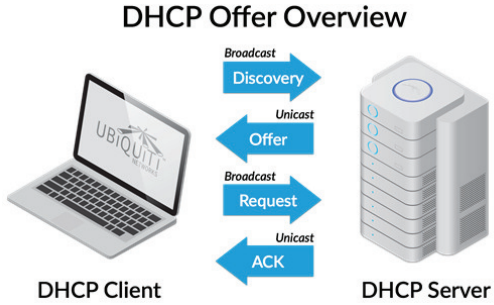

Figure 1: DHCP Offer Process

Figure 1 shows the DHCP process. DHCP process has four phases.

Dicovery In this phase the client that needs to get an IP address tries to discover a DHCP server in the network that might give it IP configuration as well as allot an IP address to it. It basically sends a broadcast in the LAN saying, "Hello! My mac address is aa:bb:cc:dd:ee:ff. can someone give me an IP address?"

Offer The DHCP server that receives the discovery message, offers an address to the client.

Request Now the client broadcasts a request to the DHCP server that offered an IP address to it to allow the lease of the IP address.

Acknowledgement The DHCP server, in response to the REQUEST, acknowledges the client and updates it database recording that the IP address has been alloted.

It is important to note here that the DHCP works using broadcast message and hence the server as well as the client should be on the same LAN segment. Further, the method described above allows more than one DHCP server to be present and working simultaneously on the same LAN. The client may get the OFFER from more than one DHCP servers and may REQUEST any one of them for the IP lease.

2 Usage of DHCP

Every device on a TCP/IP-based network must have a unique IP address to access the network and its resources. Without DHCP, IP addresses for new computers or computers that are moved from one subnet to another must be configured manually; IP addresses for computers that are removed from the network must be manually reclaimed.

With DHCP, this entire process is automated and managed centrally. The DHCP server maintains a pool of IP addresses and leases an address for a specific configurable time to any DHCP-enabled client when it starts up on the network. Because the IP addresses are dynamic (leased) rather than static (permanently assigned), addresses no longer in use are automatically returned to the pool for reallocation.

The network administrator establishes DHCP servers that maintain TCP/IP configuration information and provide address configuration to DHCP-enabled clients in the form of a lease offer for a specific configurable time.

Depending on configuration, the DHCP server may have the following methods of allocating IP-addresses:

Dynamic Allocation A network administrator assigns a range of IP addresses to DHCP, the client computer on the LAN has its IP software configured to request an IP address from the DHCP server during network initialization.

When a client-request is received by the DHCP server, it checks an unused IP and allocates the IP and related configuration to the client for a certain time period called lease-time. The client is not supposed to use the IP address beyond the lease time. The client therefore tries to get a new IP address before the expiry of a lease time. DHCP server may renew the lease for a particular client.

Static Allocation The DHCP server allocates an IP address based on a table with MAC address/IP address pairs, which are manually filled in (perhaps by a network administrator). Only requesting clients with a MAC address listed in this table will be allocated an IP address. This method is used to provide a fix, specific IP address to a client like a printer.

3 DHCP Relay

DHCP messages use broadcast to communicate initially. Therefore, for the messages to be exchanged between a DHCP client (PC) and DHCP server, both the client and server have to reside on the same LAN segment. That is because routers, by design, do not forward any broadcast data i.e. one with a destination MAC address of FF: FF: FF: FF: FF: FF and destination IP address as 255.255.255.255.

Thus a broadcast DHCP DISCOVER message sent by a client cannot be delivered to DHCP server(s) on different subnet(s) through a router shown in Figure 2. This looks like a show-stopper as we generally limit the broadcast domain by using VLANs[1] in Railnet. Hence, this means that all the different VLAN will have to be provided a DHCP server. This becomes unmanageable.

Or we may be innovative and provide one DHCP server and extend all the VLANs to the DHCP server and configure one interface of each VLAN on the server. This make the configuration difficult. The solution is **DHCP Relay**.

A DHCP relay works like a DHCP proxy. Via a DHCP relay agent, DHCP clients communicate with a DHCP server on another LAN segment to obtain IP configuration parameters. While configuring the DHCP relay, it is provided with the IP address of DHCP server. After receiving a DHCP request from a DHCP client, the relay agent sends the message to the DHCP server. It adds some more data to the message so that the DHCP server can understand where the message is coming from. It helps the DHCP server to understand what IP configuration to provide to the client.

Based on the specific information provided in the message, the DHCP server returns corresponding configuration parameters to the relay agent, which conveys them to the client. Figure 2 shows the process of DHCP with a relay agent configured.

With a DHCP relay configuration, we can now have one DHCP server in the Railnet that can provide IP addresses to each and every client (PC) in all the VLANs configured.

The model Railnet network with a DHCP server is shown in Figure 3. Figure 3 shows the generic Railnet LAN architecture with two L3 switches and two L2 switch stack. The L2 switch stack forms a ring with both the L3 switches. The DHCP server shown be connected to one of the L3 switch in a separate VLAN by itself. The L2 switch or the L3 switch can be made the DHCP relay to relay DHCP messages from the clients to the DHCP server.

4 DHCP Redundancy

When we use DHCP services in the network, it becomes one of the most critical services. Without DHCP services, the users will not get their IP configuration. Hence, it is essential that DHCP service be provisioned with redundancy. Fortunately, it is very simple to provision DHCP on Railnet with redundancy.

Let us assume that a LAN segment has two DHCP servers. When a client asks an IP address in the LAN, both the DHCP servers will OFFER the client. The client will accept any one of the OFFERs and REQUEST that DHCP server for an IP lease. This process will be repeated for other clients as well. Thus, some of the clients will get their IP address from one DHCP servers while other may get their IP address from the other DHCP server.

This is never a problem as long as both the DHCP servers do not allow the same IP address to the clients. If this happens, we will have IP clash in the network. This can be avoided if we configure the DHCP servers to allot different IP addresses. Let us say out LAN segment network

[1] Virtual Local Area Network

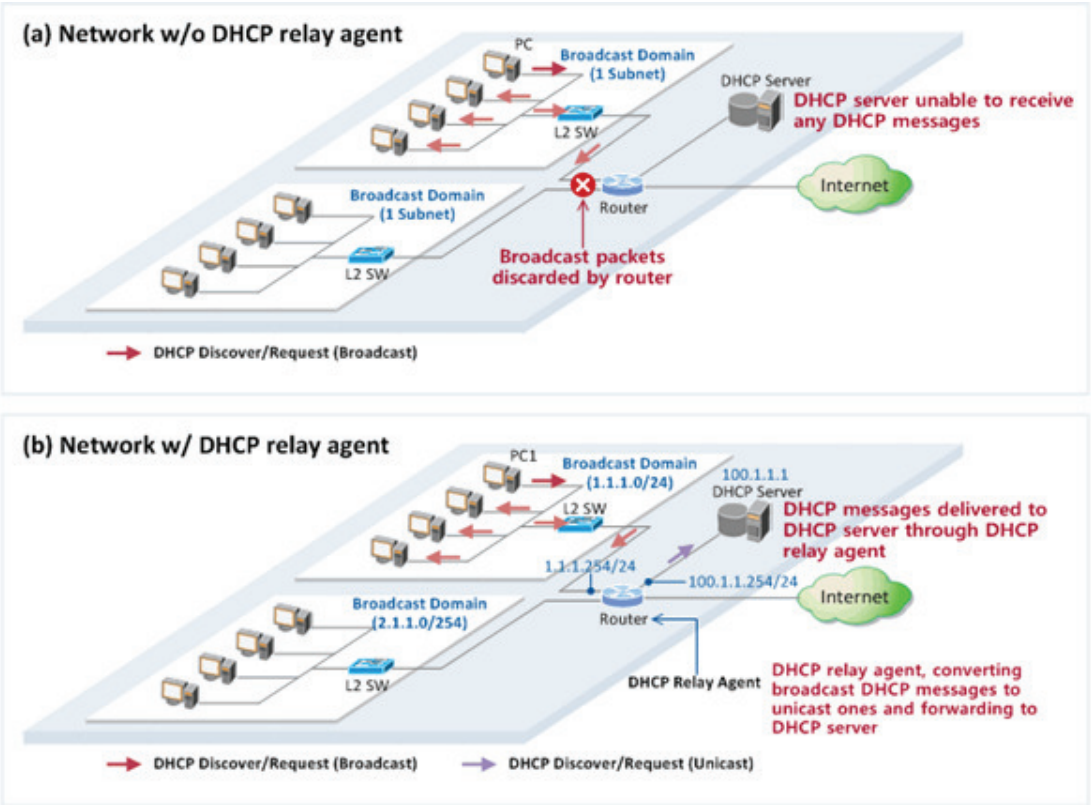

Figure 2: DHCP with no Relay Agent

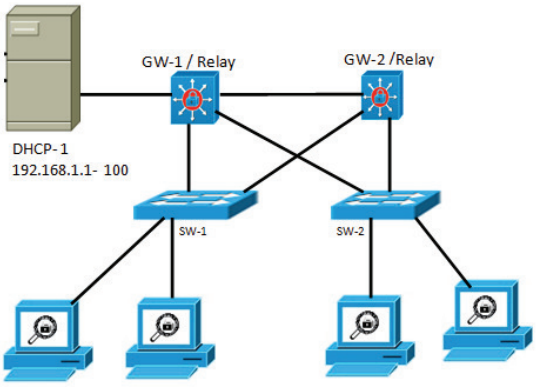

Figure 3: Railnet with DHCP

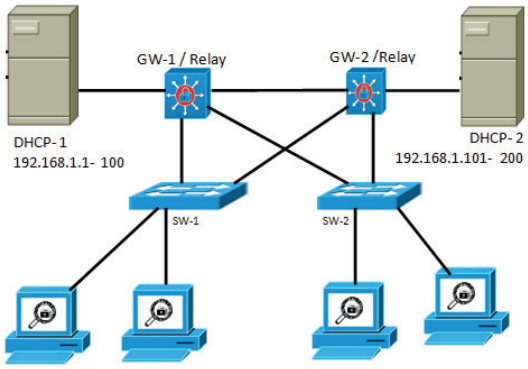

Figure 4: DHCP in Redundant Mode

address is 192.168.1.0/24. We may then configure DHCP server-1 to allot IPs from the range 192.168.1.1-192.168.1.100 and that DHCP server-2 to allot 192.168..101-192.168.1.200 address. Hence, if we take care of allotting two different IP range from the same network to the two DHCP servers, we have a simple mechanism of redundancy. Thus if one DHCP server fails, the other keeps serving the clients.

Figure 4 shows the standard Railnet LAN arrangement with two DHCP servers. The DHCP servers are connected to the L3 switch in their own separate VLANs. Generlly, the configuration should be done so that PCs of SW-1 will get the IP from DHCP-1 Server via GW-1 (the relay agent) & PCs of SW-2 will get IP from DHCP-2 Server via GW-2 (the relay agent).

The DHCP relay agent is configured with two

DHCP servers. Thus GW-1 will be configured to use DHCP-1 as the first DHCP server and DHCP-2 as the second DHCP server. In case, it cannot each DHCP-1, it will sue the services of DHCP-2 for this purpose. Similar is the case for GW-2.

5 DHCP Spoofing and Snooping

The base DHCP does not include any mechanism for authentication. Because of this, it is vulnerable to a variety of attacks. These attacks fall into three main categories:

1. Unauthorized DHCP servers providing false information to clients.

2. Unauthorized clients gaining access to resources.

3. Resource exhaustion attacks from malicious DHCP clients.

Because the client has no way to validate the identity of a DHCP server, unauthorized DHCP servers (commonly called "rogue DHCP") can be operated on networks, providing incorrect information to DHCP clients.

This can serve either as a denial-of-service attack, preventing the client from gaining access to network connectivity or as a man-in-the-middle attack. Because the DHCP server provides the DHCP client with server IP addresses, such as the IP address of one or more DNS servers. An attacker can convince a DHCP client to do its DNS lookups through its own DNS server, and can therefore provide its own answers to DNS queries from the client. This in turn allows the attacker to redirect network traffic through itself, allowing it to eavesdrop on connections between the clients and network servers it contacts, or to simply replace those network servers with its own.

Because the DHCP server has no secure mechanism for authenticating the client, clients can gain unauthorized access to IP addresses by presenting credentials, such as client identifiers, that belong to other DHCP clients.

This also allows DHCP clients to exhaust the DHCP server's store of IP addresses by presenting new credentials each time it asks for an address, the client can consume all the available IP addresses on a particular network link, preventing other DHCP clients from getting service.

DHCP spoofing is simply when an attacker enable a rouge DHCP server on a network. The rouge DHCP server will start replying to those clients "closer" to it than to the real DHCP server who are sending DHCP discovers/requests. Rouge DHCP server would provide those clients with wrong information like wrong default gateway, DNS etc. so it would stop the traffic from being routed correctly.

To mitigate this kind of attack, configure DHCP snooping on a switch. DHCP snooping implies that the switch will start looking into the DHCP messages flowing through it and take decisions based on these. For understanding DHCP snooping we need to understand the concept of trusted DHCP server and trusted ports.

Trusted DHCP Server Trusted DHCP servers are those that the switch will allow messages to and from. Thus if we specify a trusted DHCP server then the switch will not allow any DHCP message from and other server. This will effectively not allow any spoofing.

Trusted DHCP Ports The Trusted DHCP ports are those were a DHCP server are allowed to exists. This will also allow the swicth to stop rouge DHCp messages flowing in the network.

By default, all ports in the switch would be in untrusted state until we set them manually to trusted state. The ports that should be set as trusted are those where the real DHCP server is connected, trunk ports and all the ports down the path where the real DHCP server packets are traveling towards the clients. By doing this, any rouge DHCP server packet would not be able to go through those un-trusted ports.

6 Pros & Cons of DHCP

The advantages of DHCP are as under.

1. Reliable IP address configuration. DHCP minimizes configuration errors caused by manual IP address configuration, such as typographical errors, or address conflicts caused by the assignment of an IP address to more than one computer at the same time.

2. Reduced network administration. DHCP includes the following features to reduce network administration:

   (a) Centralized and automated TCP/IP configuration.

   (b) The ability to define TCP/IP configurations from a central location.

(c) The ability to assign a full range of additional TCP/IP configuration values by means of DHCP options.

(d) The efficient handling of IP address changes for clients that must be updated frequently, such as those for portable computers that move to different locations on a wireless network.

(e) The forwarding of initial DHCP messages by using a DHCP relay agent, which eliminates the need for a DHCP server on every subnet.

The disadvantages of DHCP are as under.

1. If there are multiple DHCP servers on a network, one DHCP server does not know which IP addresses have been assigned by the other DHCP servers.

2. DHCP clients cannot communicate with a DHCP server on another subnet without a DHCP relay agent.

7 Conclusion

DHCP should be used in the Railnet. Redundant DHCP configuration as described in this article can be used for setting up a reliable and redundant DHCP service. With the size of Railnet LAN increasing, and manpower cost increasing every day, it is important that automation be relied upon as much as possible. DHCP can be a good candidate for enabling in Railnet to reduce some of the load on our manpower.

The information / views expressed in this paper is of the authors and are based on their experience. Comments / observations may be sent to the author at vijaymanju186@gmail.com.

Sri J Vijay Kumar has worked in the then South Eastern Railway at Palasa in Waltair Division. He is experienced in the field of 7GHz Microwave and Data Networks of Indian Railway. He has worked in the computer lab of IRISET and has been instrumental in evolving the computer lab to its current level of sophistication. He has also contributed to the formation of network lab in IRISET and is currently working as Instructor in Networking lab at IRISET. He has also played a key role in setting up the virtual classroom at IRISET where training is imparted to the zonal Training school across Indian Railways from IRISET.

Sri D Anandam has an experience of 27 years in Indian Railways. He has worked in SCR and is experienced in the fields of Microwave, Wireless, IP network, exchanges etc. He was instrumental in strengthening and augmentation of SCR's Railnet. He has also commissioned exchanges over SCR. He is currently working as Instructor in IRISET. He has played a key role is setting up the networking and network-security labs at IRISET. He also takes care of all the IT infrastructure of IRISET.