Enterprise AP - Piggyback information through DHCP

Ryan Hsu | EnGenius Technologies

I - Introduction

We use the framework of the Dynamic Host Configuration Protocol (DHCP) to pass configuration information to the host in layer 3 network equipment. As processor power gets stronger, we would also want to carry related information in access point. The framework to carry information in IPv4 and IPv6 are quite different. This paper provides the design direction for both.

II -Dhcpv4 Design Consideration

In IPv4, configuration information is carried in tagged data items that are stored in the 'options' field of the DHCP message. In layer 3 network equipment, the options can be added by the DHCP relay agent. In an access point device, however, the options can only be added by "tampering" with the packet when the DHCP packet passes through.

In an access point device, the WiFi interface and Ethernet interface are bridged together. To intercept the packet, we can add an iptables rule in the start of the chain (raw, PREROUTING) to make the DHCP packet (UDP, destination port 67) go to nfqueue. In the nfqueue call back function, the packet can be re-packed with options we need and then resent.

Since the modified packets are broadcast packets, it is necessary to filter the same packets propagating from the bridge interface. To filter the same packet, we can create a drop rule in ebtables (filter, FORWARD, UDP, destination port 67).

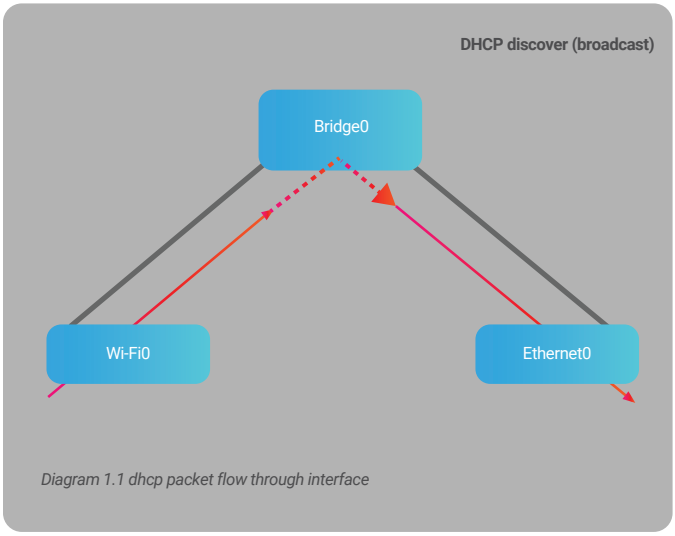


Diagram 1.1 dhcp packet flow through interface

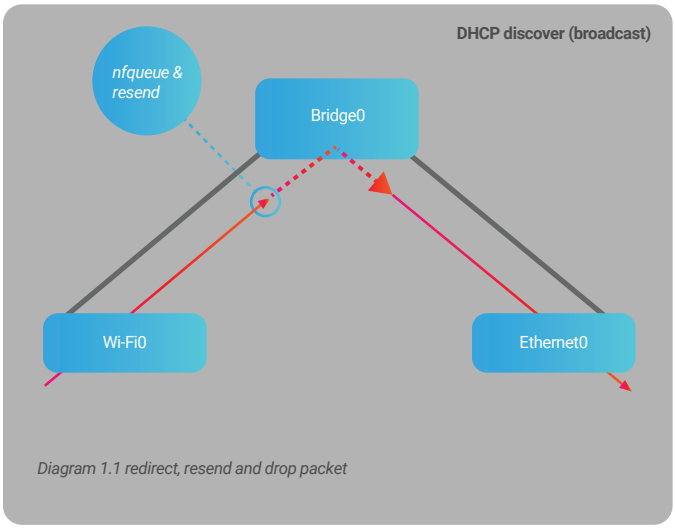


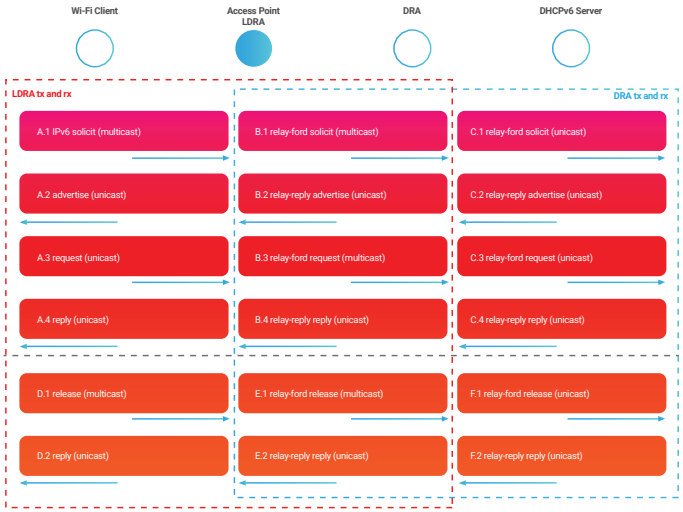
Diagram 1.1 redirect, resend and drop packet

III - Dhcpv6 Design Consideration

In Internet Protocol Version 6 (IPv6), things get more complex. When the packet passes to the relay agent, the agent does not tamper with the packet but sends to the server a relay-forward packet with the original packet inside. The options are added in the relay-forward packet but not the original packet.

RFC 6221, Lightweight DHCPv6 Relay Agent (LDRA), was submitted for this scenario. In this scenario, the WiFi client connects the access point with the LDRA, the access point (LDRA) forwards the packet to DHCPv6 Relay Agent (DRA), and the DRA forwards the packet to the DHCPv6 Server.

To bring configuration information into the relay forward packet, implementing an LDRA into the access point is necessary. There are several implementations of DRA (dibber-relay or isc-dhcp-relay) allowing us to slightly modify the DRA to LDRA.



Observe the transmit/receive packets of LDRA and DRA in Diagram 3.

Comparing LDRA to DRA, we can find:

1. The receive packets from WiFi client (solicit, advertise, request, reply, release) are exactly the same. (Diagram 2. A.1 ~ A.4, D.1~D.2 and Diagram 3. A.1 ~ A.4, D.1~D.2)

2. The packets between LDRA and DRA, and the packets between DRA and DHCPv6 server have the same format with different destinations. (In Diagram 2, B.1 vs. C.1, B.3 vs. C.3, E.1 vs. F.1.

With DRA source, we can modify these cases, change the destination to multicast address(FF02::1:2).

IV - Dhcp Relay Information

RFC 3046 defines DHCP relay information with options that can be carried in the DHCPv4 message. RFC4649 defines options which can map DHCPv4 options. For an enterprise access point, we care about vendor information and interface information. In DHCPv4, the option is 82 (curcuit id, remote id) and in DHCPv6, the options are 37 (remote id), 18 (interface id), and 16 (vendor id). This information can be added in the nfqueue callback when we need them in IPv4 and be added in LDRA when we need them in IPv6.

REFERENCES

1.RFC 6221 Lightweight DHCPv6 Relay Agent

2.RFC 3046 DHCP Relay Agent Information Option

3.RFC 2132 DHCP Options and BOOTP Vendor Extensions

4.RFC 4649 Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option

5.RFC 3315 IPv6 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

EnGenius Technologies | 1580 Scenic Ave. Costa Mesa, CA 92626

Email: partners@engeniustech.com | Website: engeniustech.com

Version: 1.00 04/2020