batman-adv - Bug #351

Issues with batadv_gw_out_of_range

03/13/2018 10:25 AM - Linus Lüssing

Status:	New	**Start date:**	03/13/2018
Priority:	Normal	**Due date:**	
Assignee:	batman-adv developers	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			

Description

I'm getting the impression that batadv_gw_out_of_range() is broken or even never worked as intended. gw_out_of_range() is only called if DHCP_TO_SERVER is set in interface_tx(). which is only set to DHCP_TO_SERVER in the is_multicast_ether_addr(ethhdr->h_dest) branch in interface_tx(). However, the kerneldoc for gw_out_of_range() says that for multicast destinations it should always return false which means, DHCP packets to a server would never get dropped in interface_tx() due to being "out-of-range". So clients might have been more sticky to dhcp servers than they should have.

And now with multicast TT entries things might get worse... I think there might be DHCPv4 packetloss if some node were to claim FF:FF:FF:FF:FF:FF via TT (the current multicast code does not announce this. however, a broken or malicious node might). And for DHCPv6, the multicast code will currently announce 33:33:00:01:00:02/33:33:00:01:00:03 so that, DHCPv6, might have become broken with the added multicast code, I suspect.

History

#1 - 05/22/2018 09:28 PM - Linus Lüssing

The latter issue was fixed with:

- batman-adv: fix packet loss for broadcasted DHCP packets to a server

The former might be fixed with the following, untested patch:

- batman-adv: fix gateway-out-of-range check