

Forum:[Hack Forums](#)

Thread: [Guessing the NAP \(Bluetooth hacking\)](#)

Swiminter - October 12, 2024, 8:16 am

Ubertooth is a great device and tool to discover the UAP+LAP.

For my needs, I must have the entire BD_ADDR correct. The most common way to find the missing part (NAP) is to bruteforce the OUI list with addresses that ends with the UAP and try to smartly relate to the type of device. That way you minimize the number of potential addresses to check (averaging around 30-40 addresses).

If I try to establish a connection with a wrong address and it falls (which is good) I can try another, but the device will show a notification (that's bad).

So bruteforcing with connection is not the right way.
Ping is better.

My problem is that I don't know how to ping an exact address. All the tools are working even if the NAP is wrong (if the UAP+LAP are correct it's enough). Tools like l2ping, hcitool etc.

For example, if my device's address is 01:02:03:04:05:06 I can ping to xx:xx:03:04:05:06 (x can be any value) and the ping will still work.

I want to ping an address and receive an answer only if the entire address is correct.

Anyone knows how can I achieve that?
Which tool? Maybe a different way?

Donelsen - November 20, 2024, 1:52 am

Find [deleted] through telegram