INVENTION DISCLOSURE

1. **Invention Title.**

Load balancing in MDU scenarios- Wifi sharing

2. **Invention Summary.**

In the current MSO deployments in an MDU, it becomes really difficult to sustain the throughputs when there is a sudden influx of people in a MDU. This disclosure provides ways to tap the potential of neighboring APs in the MDUs (assuming these neighboring APs are not loaded and are nearby to the serving AP).

3. **Invention Description**.

Consider the following use case:

A single MSO is responsible for Wifi in an MDU complex. Assume there is 1 AP/MDU. Each AP is configured to handle 'x' clients. MDU1 has AP1 from vendor1. MDU2 has AP2 from vendor2 and so on. In a scenario wherein the host of MDU1 has a party at his/her place, then assuming that about y guests show up (y>x). In this case, there is no way that AP1 can handle so much traffic. Due to which, according to the current deployment scenarios, either of the 2 cases are bound to happen at MDU1:

- All the y clients (assuming each person in MDU1 has 1 client) will get associated to AP1, but none of them will run meaningful throughputs. (Meaning the throughputs will be extremely slow for all of them)

- Only 'n' (n<x) clients will get associated (based on how n has been configured by the MSO. 'y-n' will have to either depend on 3G/4G for connectivity)This is where tapping the potential of AP2 in MDU2 is very useful in such a scenario.

Solution: If AP1 knows its neighbors AP2, AP3 since they belong to the same MSO (Please see Common APIs for neighbor list building) there should be the concept of load balancing among the APs.

This could be done in the following way:

AP1 requests AP2 for a temporary password (say for 5 hours may be). This password can then be given to the additional guests. Assuming AP2 is not heavily loaded, the additional guests can smoothly be given enough BW so that they get the min. throughput rates. The user of AP2 (MDU2 resident) will not be charged for those 4 hours for the additional traffic that is being generated. Instead, owner of MDU1 pays on a per hourly basis for the number of hours that the password has been leased to him/her.

There has to be a cap on the number of times that the guest password is generated from the neighboring APs. Note that this scenario can be implemented only when the MDUs are close by which means that the target-AP is in close proximity to the serving AP. This assures that the additional traffic on the target-AP can be handled well. Once AP1 gets the temporary password from AP2, the clients that haven't been associated at all to AP1 ('y-n' clients) will be given that password and they can directly associate with AP2.

Common APIs for neighbor list building

INVENTION DISCLOSURE

Case 1: WLC and APs are from a single vendor.
The deployed APs are from the same vendor, which talk to a common WLC.
A neighbor list can be built on each AP by the WLC since the WLC sees all the deployed APs.Also, AP to AP handover/client mobility is through the WLC.

Case 2: APs are from different vendors with corresponding WLCs; same SSID.
In such scenarios, the client performs a handoff to the neighboring AP only if the SSID is same (Community Wifi, Wifi in stadiums, hotels, conferences etc.) Since the services are from a single MSO, the WLC database can be configured to include basic information about all the APs in the MSO deployment of that area.

Case 3: APs are from different vendors with corresponding WLCs; different SSID (the most common MDU scenario).

In this case, AP1 would report all the other APs as rogue to its WLC.

Since both the APs are operating in a single MSO network, they shouldn't consider each other as rogue even though they are from different vendors. Hence, this would call for an API to be defined on each of the APs. This API should be MSO network centric but vendor agnostic.

A common API on both the APs would ensure that there would be no rogue APs in an MSO network. The 1st step is to authenticate the APs with the MSO network to make sure that both of them are not rogue. Then, it involves building up the neighbor list at each of the APs.

Note: On the other end of this load balancing spectrum, if say an AP is not loaded at all specially during the nights when no client attaches to the AP/certain weekdays when the clients are not present; (basically when there are no clients authenticated + associated to that AP) then the CMTS should signal that AP to get into sleep mode.

Briefly outline the potential commercial value and customers of the invention.

Would be helpful in dense MDU AP deployment scenarios. Also in the dorms of schools and universities.

4. How is this invention different from existing products, processes, systems?

I do not think tapping the potential of an underloaded, neighboring AP has been utilized so far. Also, since the owner of the MDU pays for the additional services that he/she gets from the neighboring MDU-AP, it is a good way to generate revenue especially when there is a sudden influx of people in need of Wifi services with sustainable throughputs.