As part of community Wi-Fi network deployments, operators are enabling 2 SSID on residential Wi-Fi GWs

- Private SSID – for use by broadband subscriber at home
- Public SSID – for use for other customers (e.g. broadband subscribers out of range of their private SSID)

The clients accessing the network through private SSID have prioritized access to the Wi-Fi resources and as a result higher QoS compared to the clients connected through the public SSID. One way to achieve this traffic prioritization is to apply different policies on the IP flows originated from or destined to clients connected through public and private SSIDs.

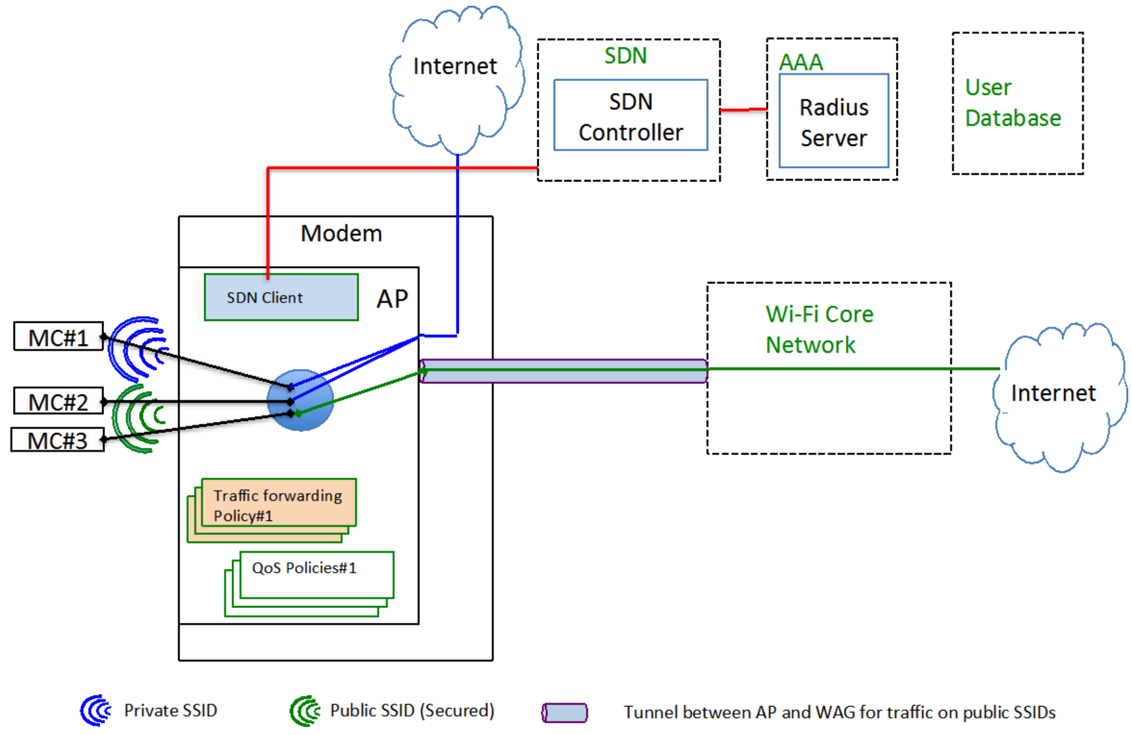
One common problem encountered in community Wi-Fi networks is that as a broadband subscriber moves from out-of-range of private SSID to in-rage of private SSID, subscriber device remain on public SSID. One of the solutions provided so far is that AP learns the MAC addresses of clients that have previously connected to its private SSID and once such clients are in its range, the AP blocks their association requests to the public SSID. However this solution is not full proof for the following reasons:

- The clients whose association attempts to the public SSID have been blocked continue their association attempts to the public SSID (not the private SSID) and their attempts continue to be blocked.
- If clients attempt to associate through public SSID is blocked, clients will not attempt association to the public SSID even if they are out of range of the private SSID.

In this disclosure, we propose an alternative solution

- The AP accepts the association requests of clients to the public SSID even when the user is inside the house and private SSID is available. Instead of forcing the client to move to the private SSID, the policies such traffic forwarding scheme and QoS on the AP for this particular client should be dynamically configured by the network to match the policies used for the clients on the private SSID. This method, while difficult and not practical in the past, is becoming more and more feasible with the advent of the concepts such as Software Defined Networking (SDN), CPE virtualization and Network Function Virtualization (NFV)
- At the time of user authentication, the Wi-Fi core network will learn that the client is trying to attach to the Wi-Fi network using the Public SSID while the user is inside the home. The network uses this information to instruct the AP to use traffic forwarding and QoS policies for this client to match that of the clients on the private SSID.

The picture below demonstrates an example implementation of such a system:



- To avoid security risks, both private and public SSIDs must be secure (private SSID: WPA2-PSK and public SSID: WPA2-Enterprise). AAA should integrate the subscriptions and authentication of both DOCSIS and Wi-Fi. The AAA should link the following:
  - MAC address of the Wi-Fi device
  - User name and password of the Wi-Fi subscription
  - MAC address of the CM
  - Device certificate of the CM
- The device first authenticates to the AAA over the public SSID with WPA2-enteprrise (EAP-TTLS). Once authenticated, the SDN controller would need to receive the AAA authorization message and recognize the authenticated device's MAC address is linked it to the CM subscription. The SDN controller would then need to instruct the AP to route only this device's traffic, and not others on the public SSID, to the private LAN side of the router and NAT function in the AP.
- We would not need to worry about MAC address spoofing on the secure SSID since a rogue device needs to be authenticated with the AAA in order to be able to establish a crypto-sync on the public SSID. The AP will need to check for the correct crypto sync before accepting packets from the device.