March 2022

# METHOD TO SUPPORT IDENTITY PSK, CAPTIVE PORTAL AND ENHANCE ROAMING FEATURES FOR RANDOM MAC ADDRESS CLIENTS

Niranjan M M

Srihari Bhavanasi

# METHOD TO SUPPORT IDENTITY PSK, CAPTIVE PORTAL AND ENHANCE ROAMING FEATURES FOR RANDOM MAC ADDRESS CLIENTS

AUTHORS:
Niranjan M M
Srihari Bhavanasi

## ABSTRACT

As we know, wireless clients associate to the wireless network using the mac address assigned by the manufacturer of the Wi-Fi Network Interface Card (NIC). This manufacturer-assigned mac address, which is globally unique, is also known as Burn-In-Address (BIA). Use of this BIA everywhere raises the question of end-user privacy as the end-user can be tracked with Wi-Fi's mac address. Random MAC address solves the user privacy issues as per GDPR, but introduce limitations on some of the existing legacy wireless security methods and features which depends on MAC address to identify the devices such as, MAC address filtering, Identity PSK, Web authentication with captive portals, Web authentication using MAC filtering, DHCP with MAC address based IP binding, Location Tracking, User Defined Network, Device Analytics, MAC-based Policies, Troubleshooting, Forensic Usage, Roaming etc., There are techniques to address few of the above limitations such as EAP-TLS, DHCP with DUID, disabling the MAC randomization functionality etc., But there are no techniques to address security functionalities such as iPSK and "web authentication with captive portals" and also some of the features/services such as Location tracking, Telemetry, Roaming/Mobility etc., The techniques presented herein propose method to achieve iPSK, Web authentication with captive portals and roaming features even for random MAC address supported devices, yet maintaining the user privacy.

## DETAILED DESCRIPTION

As we know, wireless clients associate to the wireless network using the mac address assigned by the manufacturer of the Wi-Fi Network Interface Card (NIC). This manufacturer-assigned mac address, which is globally unique, is also known as Burn-In-Address (BIA). Use of

this BIA everywhere raises the question of end-user privacy as the end-user can be tracked with Wi-Fi's mac address. With the adoption of the new General Data Protection Regulation (GDPR) (EU) 2016/679, protecting the privacy of users and their personal data (i.e., protecting any Personally Identifiable Information [PII]) is the requirement for all network operators. Burned-in or fixed MAC address of a client is one of the key PII element and exposure of this can lead to the identification of a user through the user's device and it can also lead to correlation of that user's network profile over time and across the globe. To overcome the privacy issues due to fixed MAC address, device vendors, initially introduce random MAC address (aka locally administered MAC address [LAA]) and later it is standardised in IEEE802.11aq, but there are no industry standards on the use of the random MAC address for Wi-Fi. Each OS vendor is independently implementing on their own.

Although random MAC address solves the user privacy issues as per GDPR, but introduce limitations on some of the existing legacy wireless security methods and features which depends on MAC address to identify the devices such as

- MAC address filtering (MAC Denial Lists): "Deny access" to the devices listed in the MAC address filter database (blacklist).
- iPSK (Identity PSK): Provides method to use per device PSK and identify the device using MAC address.
- Web authentication with captive portals: Captive portals are web pages presented to the users during network connection (guest access). Captive web portals use the MAC address as the device anchor and so the user's authorisation state is connected to the MAC.
- Web authentication using MAC filtering (MAC Authentication): In this method, based on the MAC address filtering, web authentication (especially web pass through) is done.
- DHCP with MAC address-based IP binding (MAC-based IP Reservation): Provides method to statically allocate IP address to devices based on MAC address.
- Location Tracking: Provides way to identify and locate the devices using probe frames (scanning method), which carry MAC addresses.
- User Defined Network (UDN) (MAC Registration): Provides method for pre-registration of the devices (guest access) using MAC address as device identity.
- Telemetry - Device Analytics (Network Assurance): Uses MAC address to identify the device and to establish a connection between a scanning device and a connected device.

- MAC-based Policies: Parental control in home Wi-Fi routers enforce policies based on MAC address (of child's phone).
- Forensics Usage: In cases where public Wi-Fi has been used to commit online crimes, MAC addresses are a critical part of the forensic toolkit that can be used to correlate a device to a user.
- Troubleshooting: In connectivity troubleshooting workflows, the MAC address may be the only identifier for IT to get started in troubleshooting with product tools, logs, or packet captures.
- Roaming/Mobility: When client roamed from one AP/WLC to another, client may use new random MAC address during re-association phase.

Currently there are techniques to address few of the above limitations such as

- Using EAP-TLS (certificate-based authentication) with Globally Unique Identifier (GUID) or Device Unique Identifier (DUID) to identify the device and apply the policies.
- Using DHCP with DUID (DHCP Unique Identifier) support as in RFC https://datatracker.ietf.org/doc/html/rfc3315.
- Adding knob at the WLC/AP to "deny access" to clients with random Mac address (identify using LAA bit) and ask users to disable from the network profile of the device.
- Using MDM or other provisioning tool, IT can push a profile to devices that disables the MAC randomisation feature during onboarding.

But there are no techniques to address security functionalities such as “iPSK" and "web authentication with captive portals" and features/services such as Location tracking, Telemetry, Roaming/Mobility etc., Both enterprises and service providers are required to comply to the user privacy by allowing the user devices to use random MAC address. At the same time, there is a greater need for the enterprises and service providers to use the above impacted functionalities or services in their networks. Therefore, need an efficient and elegant approach to achieve these functionalities even for random MAC address supported devices yet maintaining the user privacy.

The techniques presented herein propose method to generate Unique Temporary Identifier (called Wireless Deployment Unique Temporary Identifier [WDUTI]) at the WLC for the wireless clients upon initial association and share it with the clients as part of vendor specific payload of

association response. Wireless clients share this with WLC/AP during DHCP handshake and later re-association phases. Further WLC/AP uses WDUTI to uniquely identify the client and map with right policies even though client uses Random MAC address in control and data traffic. Like generation of new random MAC address logic at the wireless client (for every 24hrs, upon DHCP renewal, upon re-association [to same or different SSID] etc., to address privacy issues, WDUTI will also be re-generated on the WLC based on the configurable timeout, reception of association/re-association frame, DHCP renewal etc., The generated WDUTI would contain details about the Roaming Domain, WLC ID, AP ID along with Client ID. Hence it helps to uniquely identify the client not only for re-authentication/re-association but also for client roaming across WLC/AP. The format of the WDUTI would be as mentioned in Figure-1.

The WLC ID and AP ID of WDUTI shall contain entropy (random) generated and signed using private key (aka attestation key) stored securely in tamper proof ACT2/TAM chip. Validating the signed entropy using PKI infra would help in quickly identifying clients whether they are roaming from Legitimate AP/WLC or Rogue/Compromised AP/WLC.

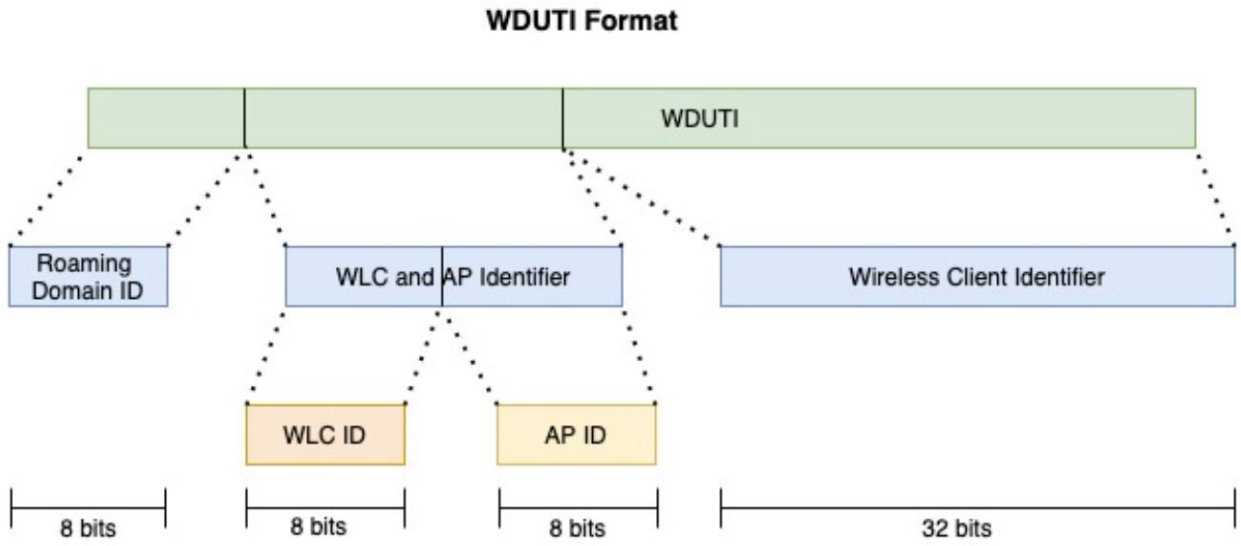


Figure-1

This method helps to improve client roaming and supports IPSK and web authentication with captive portal features even for clients with Random MAC address.

The technique presented herein is explained is steps as below:

- AP sends beacons on to the access network over 2.4G/5G/6G frequency band.
- Wireless clients send probe request to the AP (optional)
- AP sends back probe response to the wireless clients (optional)
- Wireless clients send association request to the AP
- If random MAC address is supported, wireless client sets locally administered MAC address (LAA) bit (it also referred as random MAC address) in all the frame/packets.
- AP forwards the association request to the WLC.
- WLC uses LAA bit and if this bit is set then consider, this wireless client supports random MAC address.
- If random MAC address is not supported, then WLC can do MAC address filtering and if wireless client is not part of blacklist, it sends association response to the wireless client (through AP). In other words, MAC address filtering on WLC does not holds good for wireless clients with random MAC address support.
- To uniquely identify the wireless client with random MAC address support, this proposed workflow is to continue support of iPSK, Web authentication with Captive Portal, Mobility etc., is as below. Same is applicable even for wireless client using Burned-in MAC address.
    - WLC generates Wireless Deployment Unique Temporary Identifier (WDUTI), which is a wireless network temporary identifier and allocated by Wireless LAN Controller (WLC) for the wireless client, during very first association of the wireless client by any of the WLCs/APs in roaming/mobility domain in a particular deployment.
    - WLC uses WDUTI to uniquely identify the wireless client.
    - WLC sends WDUTI to wireless client along with association response as part of vendor specific payload.
    - Wireless client stores WDUTI (per wireless interface or for a particular SSID or common for all wireless interfaces).
    - Wireless client uses this WDUTI to send in DHCP packets (viz., offer and request), re-association request frame, authentication request frame etc., to the WLC/AP.
    - WLC uses WDUTI received in these packets to uniquely identify the wireless client with random MAC address.

- Like generation of new random MAC address logic at the wireless client (i.e., for every 24hrs, upon DHCP renewal, upon re-association [to same or different SSID] etc.,) to combat privacy issues, WDUTI also will be re-generated on the WLC based on the timeout, reception of association/re-association frame, DHCP renewal etc.,
- With WDUTI being generated on the WLC, able to resolve many of the limitations of random MAC address support with respect to security and other features without compromising on Privacy (as provided by random MAC address feature).
- Newly generated WDUTI will be sent from WLC to wireless client in
  - Re-association response/Association response as vendor specific payload.
  - DHCP offer or DHCP acknowledge packets sent from WLC/AP to wireless client as vendor specific payload.
- The details of handling roaming scenarios, IPSK support and web authentication flows are as explained in detail under "Different Workflows".

Different Workflows:

A. Workflow of Roaming/Mobility:

- As mentioned above, WLC would allocate unique WDUTI for each wireless client. WDUTI will be such that, part of it carries WLC ID and AP ID. WDUTI is sent to wireless client as part of Association Response and during DHCP phase.
- Whenever wireless client roam from one WLC (Anchor WLC, say WLC-1) to another WLC (Foreign WLC, say WLC-2) within the mobility domain, as part of re-association request, wireless client sends WDUTI to WLC-2.
- Foreign WLC (WLC-2) identify the Anchor WLC (WLC-1) using WDUTI sent by the wireless client and retrieves information (such as Policy, Security [AAA information], QoS etc.,) pertaining to that wireless client from the Anchor WLC (WLC-1).
- Foreign WLC (WLC-2) applies the wireless client specific policies and send re-association response.
- As part of re-association response, it regenerates the new WDUTI and send it to the wireless client as part of vendor specific payload of re-association response.

- Later during DHCP renewal phase, wireless client sends the WDUTI (received earlier during association/re-association response) so that WLC identify the wireless client and map it to the right database (wireless client dB) maintained at the WLC.
- The WDUTI is available only within the wireless network deployment and unique in a specific deployment (ensured by Roaming Domain ID, WLC ID and AP ID).
- As WDUTI is regenerated frequently (viz., based on the administrator configuration, in association/re-association phase, in DHCP renewal etc.,) during the lifetime of the device/user session and hence device/user cannot be tracked based on WDUTI, in-turn preserving privacy without compromising on the wireless features.

Figure-2 depicts Roaming/Mobility workflow.

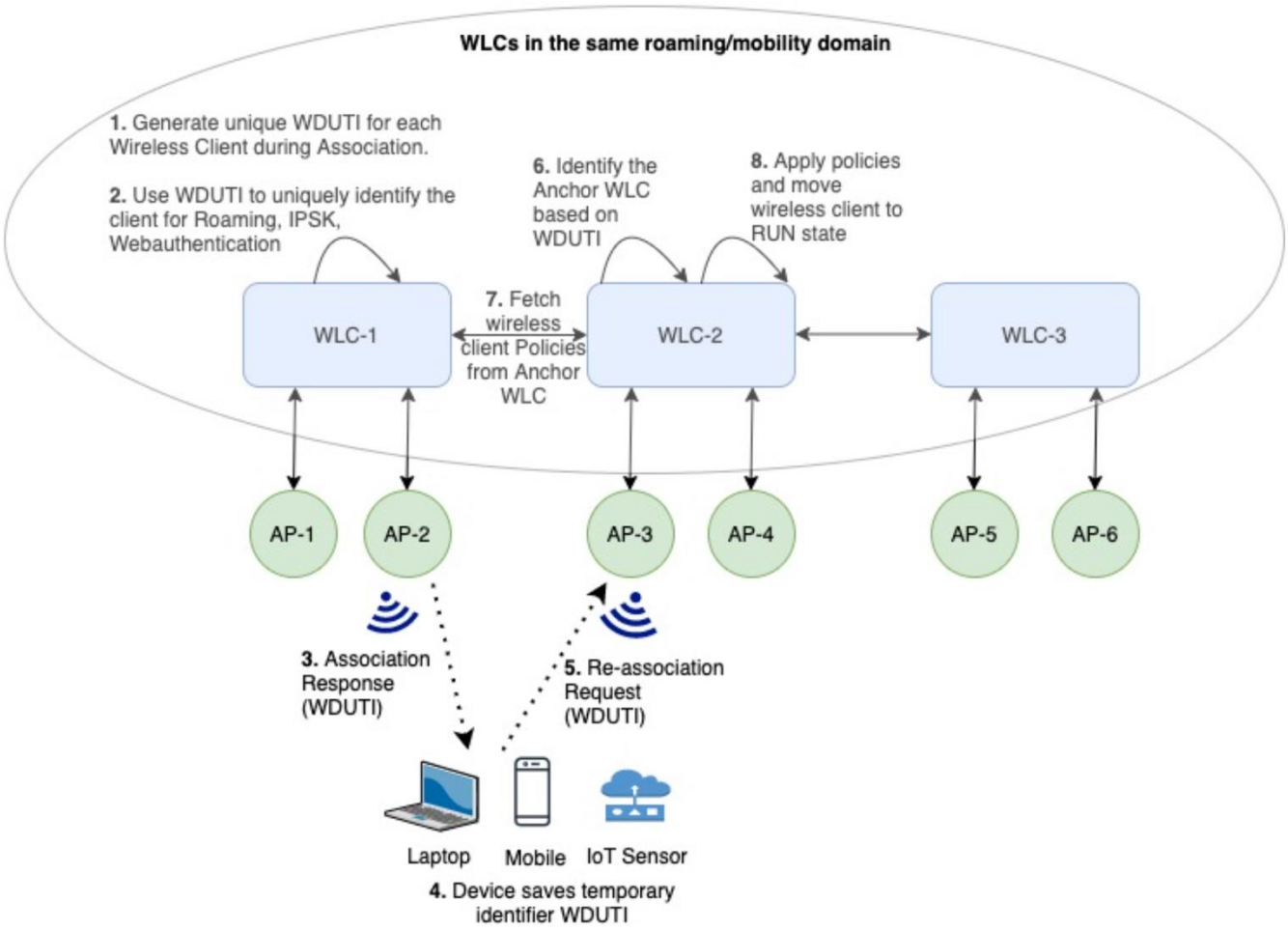


Figure-2

B. Workflow of IPSK (Identity PSK) support:

- SSID is configured with Pre-Shared Key (PSK) as security method.
- Wireless client detects the SSID and would initiate Association Request to the AP/WLC.
- WLC receives the Association Request and send Association Response back to the wireless client.
- As mentioned above, WLC would allocate unique WDUTI for each wireless client. WDUTI will be such that, part of it carries WLC ID and AP ID. WDUTI is sent to the wireless client as part of vendor specific payload of Association Response.
- This WDUTI is used to uniquely identify the wireless client and same is regenerated frequently to protect privacy of the user/device.
- As we know, IPSK security method require mapping of unique PSK to the device MAC address. But in case of Randomised MAC address, this mapping would fail.
- Hence as per this method, mapping unique/identity/private PSK (iPSK) to the WDUTI of the wireless client.
    - The very first authentication (before WDUTI is generated) is based on the default PSK. This helps in establishing the encrypted channel.
    - After onboarding with default PSK, trigger the re-authentication for iPSK (as identity/unique/private PSK which provides added security than common PSK) and the proposed WDUTI infrastructure will be utilised to solve the iPSK limitation with randomized mac address.

C. Workflow of Web authentication (captive portal) support:

- SSID is configured with web authentication as security method.
- As mentioned above, WLC would allocate unique WDUTI for each wireless client. WDUTI will be such that, part of it carries the WLC ID and AP ID. WDUTI is sent to wireless client as part of Association Response and during DHCP phase.
- After that whenever user try to access the website/internet, user would be redirected to web authentication captive portal page (AAA, or social login]). The redirect URL sent by the WLC, carry WDUTI for the captive portal to identify the device along with original URI.
- Upon successful authentication, Captive web portals use the WDUTI as the device anchor and so that user's authorisation state is connected to the WDUTI.

- During re-authentication (upon web authentication session expiry/timeout), WLC sends redirect URL along with old WDUTI and new WDUTI, so that captive portal can track and update the device anchor. Hence captive portal can do accounting on the user's device.

The techniques presented herein enhances the current roaming workflow by avoiding broadcast/multicast Mobile Announce packets sent across the WLCs of roaming/mobility domain. Moreover, this method helps to overcome the limitation on iPSK introduced by Random MAC address support. Additional, method helps to support web authentication captive portal even for clients with Random MAC address feature.