METHODS FOR RESOURCE RECLAMATION IN UNLICENSED MOBILE WI-FI

INVENTORS:

STEPHEN GLENNON
KEVIN EDWARD MAHONEY
STEPHEN ARENDT
ZACKARY FOREMAN

1

08/16/19
Title: Methods for resource reclamation in Unlicensed Mobile Wi-Fi
Inventors: Zackary Foreman, Stephen G Glennon, Steve Arendt, Kevin Mahoney

Background of the invention:

This invention relates to another invention where we modify how Wi-Fi devices associate with a network such that they associate with a virtualized Access Point (AP) implemented as a combination of radio(s) (Wireless Termination Point(s) or WTP(s)), and an Access Controller (AC) which may be separated or combined with a WTP to implement traditional AP functionality.

In the associated invention (described in other invention disclosures and patent filings), rather than associating with a physical piece of hardware, identified by its MAC address, the Wi-Fi client associates with a virtual AP identified by a logical MAC address or Basic Service Set Identifier (BSSID). In order to perform this operation, the WTP hardware or software needs to support multiple BSSIDs, so it can dynamically instantiate a Service Set Identifier (SSID) specific to the client device.

Typically, instantiating an SSID with a device-specific BSSID takes resources that are limited. In order to support large numbers devices that may roam into range of the WTP over a period of time, resources associated with supporting a specific device must be reclaimed when the device is no longer in range or no longer served.

Disassociation from the network and reclamation of resources

The process described above causes resources to be consumed on an access point (or WTP) when a device comes into range and a device-specific SSID/BSSID is instantiated. In order to reduce ever-growing AP resource use as known devices come into range, methods are used to detect when to stop transmitting the device-specific SSID/BSSIDs, including the following:

  i)   When a device disassociates from the network through using a disassociation request, the network stops transmitting the device-specific SSID/BSSID for that device, reclaiming the resources associated with the device-specific SSID/BSSID.
  ii) The method of item i) above, where the network continues to transmit the device-specific SSID/BSSID for a period of time after a disassociation request is received from the device, and then stops transmitting the device-specific SSID/BSSID for that device, reclaiming the resources associated with the device-specific SSID/BSSID.
  iii) The method of item i) above, where the network continues to transmit the device-specific SSID/BSSID after a disassociation request is received from the device as long as packets from the de-cloaked MAC address are detected addressed to any destination MAC address, and then stops transmitting the device-specific SSID/BSSID for that device, reclaiming the resources associated with the device-specific SSID/BSSID. This maintains

the device-specific SSID/BSSID and allowing the device to connect, all the time that the device is within range of the network.

iv) The method of item iii) above where the transmission of the device-specific SSID/BSSID for that device continues after disassociation and while packets from the de-cloaked MAC address are detected addressed to any destination MAC address until a time-out is exceeded.

v) The method of item iii) above where instead of detecting packets from the decloaked MAC address, the reception of an ACK from the unicast beacon packets to that device is the means of determining that the device is still within range.

vi) The method of item iv) above where instead of detecting packets from the decloaked MAC address, the reception of an ACK from the unicast beacon packets to that device is the means of determining that the device is still within range.

vii) The method of item iii) above where instead of detecting packets from the decloaked MAC address, the WTP periodically sends RTS packets addressed to the device's de-cloaked MAC address, and the reception of a CTS packet indicates the devices continued presence.

viii) The method of item iv) above where instead of detecting packets from the decloaked MAC address, the WTP periodically sends RTS packets addressed to the device's de-cloaked MAC address, and the reception of a CTS packet indicates the devices continued presence.