WiFi Optimizations to Improve SSID Priority to Enhance Overall Quality of Experience

Ivan Ong
Comcast

Abstract

Mobile devices (laptops, tablets, and phones) may not associate with the best Wi-Fi access point when returning to a home network. This paper will explore how to tune parameters on the PHY and MAC layer of 802.11 to improve association in the absence of a controller or without the need of a third party connection manager app to ensure prioritization from the client itself. It will also include an empirical analysis of the behavior of certain clients as they attempt to associate to their residential wireless gateway routers and conclude with some guidelines for potential tuning parameters.

Introduction

The preference from a service provider's perspective is for a user's mobile device to associate to their home network to ensure proper policies are applied and downloadable content (eg. Podcast, personal video) is able to synchronize but devices often associate to less desirable networks. In part, this is due to the vast array of mobile operating systems and how they decide to associate to a Wi-Fi network. For example, an iOS device merely relies on the last known service set identifier (SSID) when performing a Wi-Fi network selection; this can be problematic because not all networks are equally desirable but iOS does not provide any facility to specify priorities or preferences among Wi-Fi SSID. To add to the complexity of Wi-Fi SSID selection, Apple's iOS Deployment Reference documentation states that the current basic service set identifier (BSSID) connection will be maintained until the RSSI level crosses a -70dBm threshold [4]. This is a complex issue in a multi-dwelling environment where a user's mobile device has associated to a public or neighboring SSID and, upon return to home, is unable to intelligently associate to the home network.

WiFi Scanning

Before exploring the potential of MAC and PHY layer parameter tuning, it is critical to understand the fundamentals of an 802.11 client joining a network. This three stage process consists of [5]:

- Probing
- Authentication
- Association

In the probing stage, a mobile client supports both active and passive scanning; in active scanning (See Figure 1), probe requests are sent at defined intervals to look for either any SSID or specific SSID defined within the frame. Access Points (AP) can then respond to these probe requests to begin the second part of the three stage process of joining a network. In passive scanning (See Figure 2), the client radio cycles through each [operating] channel listening for beacons that may be advertising their SSID. If it receives multiple beacons from various neighboring APs for the same SSID, it will then attempt to associate to the best received signal strength indicator (RSSI) level.

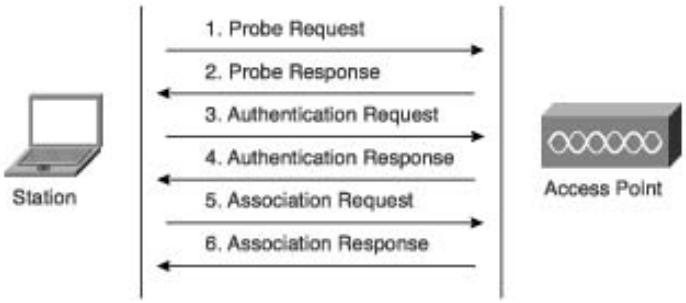

Fig 1: Active Scan

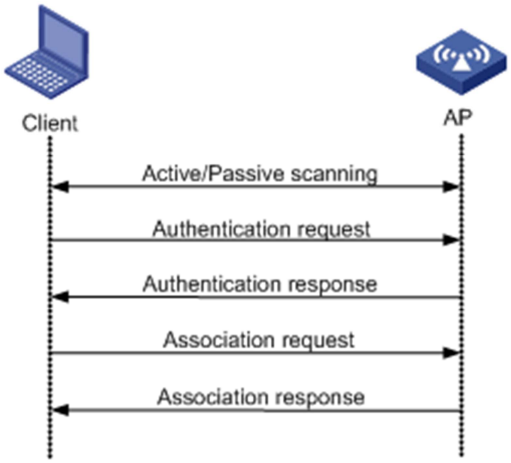

Fig 2: Passive Scan

Once the scanning process has been completed and the client has made a decision to join a network, it will need to authenticate against the AP. Upon successful completion of the authentication process, the association stage will then begin (refer to Figure 3).

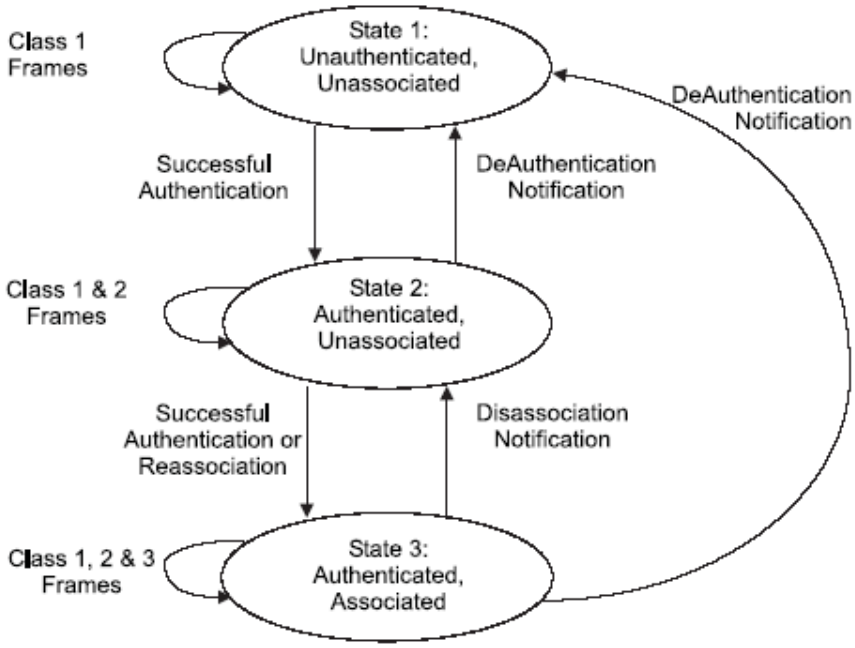

Fig 3. State Machine for Client Association

802.11 Frame Format

The 802.11 Frame format is represented in Figure 4, it is the underlying foundation for Wi-Fi communication in terms of information between client and AP. The structure consists of a MAC header, frame body, and frame check sequence (FCS). The first two bytes of the frame structure specifies the Frame Control block (see Figure 5) which further defines 'control' information to assist the type of information necessary for the receiver on how to process the MAC frame.

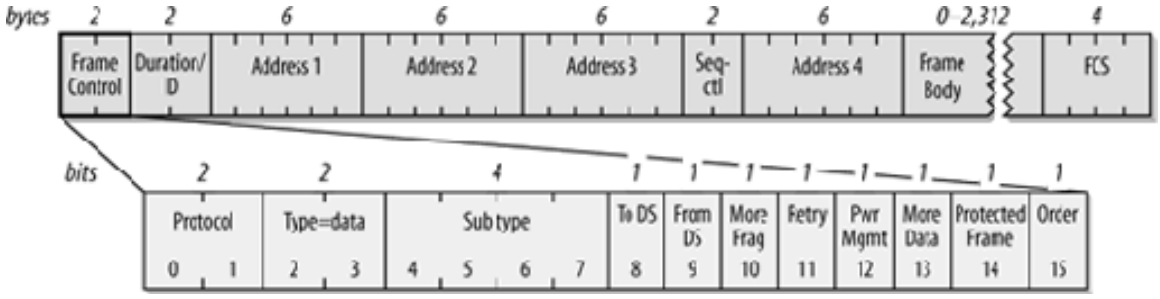

Fig 4: 802.11 MAC Frame Format

The third block of the frame control subfield 'subtype' is a byte block to indicate the type of control frame that is being transmitted. The following are a subset of subtype values and the control frame identified:

Subtype Value	Subtype Name
0000	Association Request
0001	Association Response
0100	Probe Request
0101	Probe Response
1000	Beacon

Table 1: Frame Control Field

By performing some basic parameter tuning on the MAC layer of a home wireless gateway router, the home SSID can be optimized as the preferred network of choice. In particular, Beacon Interval is a MAC layer attribute existing on most Wi-Fi chipsets that may potentially be exploited to optimize SSID prioritization.

Beacon Interval

Beacon frames are used in communicating the SSID information from an access point (AP) to the station (STA) or client. The beacon interval block is defined within the MAC header's frame body as a 2 byte mandatory value. 16 bits are used to define one time unit which typically correlates to 1 millisecond. Figure 5 provides the layout of the beacon interval block located within the frame body of the MAC header.

Within the 802.11 WLAN frame, the subtype block defining a beacon in binary is 1000 (or subtype 8), this value is conveniently visible when decoding beacon type frames in a packet sniffing tool such as Wireshark. The interval of when a beacon is transmitted is typically set at 100ms as a default value. Each SSID constitutes its own beacon frame, so as an example, if there are 10 SSID defined on an AP, it would mean a beacon frame is transmitted 10 times per second, each unique SSID will be advertised every 100ms and cycle each second. In the case of a residential wireless router, there are typically 3 SSIDs defined with potential SSID to be added in the very near future. The 3 SSIDs will be broadcasted every 100ms and cycles every 300ms. There are no control mechanisms to manage beacon transmission; they are subjected to the same 802.11 CSMA/CA algorithm for when to transmit.

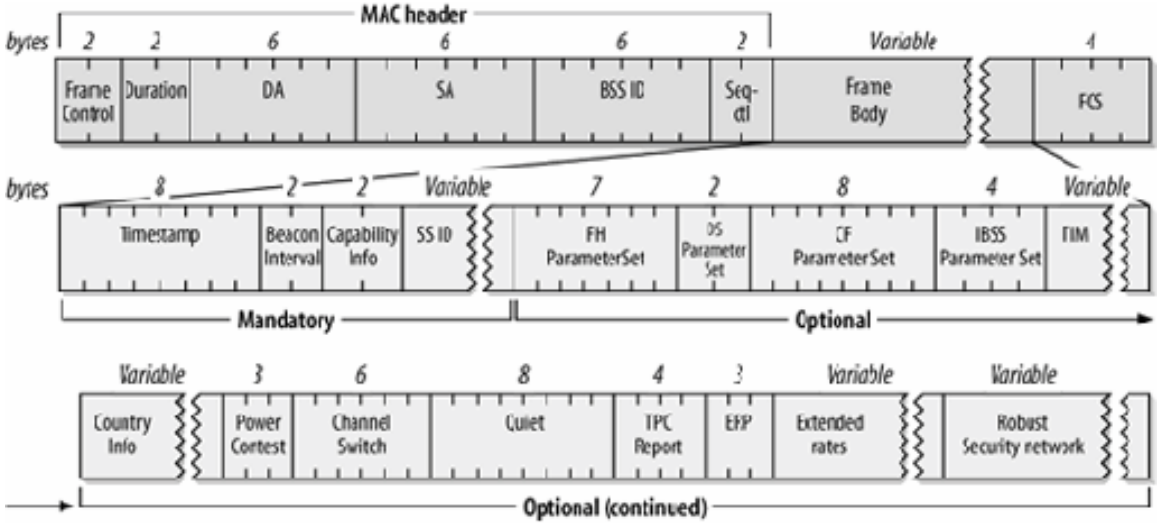

Figure 5: Beacon Frame structure

Proposed Logic and Implementation

Building on our understanding of the 802.11 frame structure, we now describe three approaches to ensuring prioritization of home SSID over that of a public one. The first approach incorporates scheduling based on fingerprinting the behavior of the client. The second introduces a simple algorithm to drop all initial probe requests to a public SSID, hence, increasing the probability that the innate client connection manager will select the home SSID. The third requires account validation of the device to ensure the client is at home and issuing a disassociation frame and forcing a re-association to the home SSID.

Prior to describing and understanding the three SSID prioritization approaches, it is important to understand the behavior of the proposed tweaks to the MAC layer frame such as beacon interval values. The results of some empirical and lab experiments involving beacon interval manipulation will provide a more informed perspective on the first proposed methodology and how that relates to second and third methodology. Once the analysis of the experiments is understood, the logic and algorithms make more sense.

Analysis of Client Behavior

I conducted an empirical analysis of client behavior given the use case of returning to the user's residence after a day of associating to hotspots or non-home SSID.
The results will be discussed in the following sections, the behavior differs slightly between the test clients involved in the experiments. Four scenarios were evaluated:

- Non-Chambered with network preference defined
- Non-Chambered with no network preference defined
- Chambered with network preference defined
- Chambered with no network preference defined

Experiment

An attempt to simulate MAC layer tuning lead to the following basic experiment:

- Increasing beacon interval for a public SSID to be longer than that for a private SSID on a residential wireless gateway router. The private SSID beacon interval will remain at default value of 100ms to avoid interfering with a pre-existing client response to anything other than the default value

The setup of the experiment occurred in two environments: chambered and non-chambered in a residential setting. The equipment consists of two Ericsson AP6120 Access Points (AP) with DOCSIS backhaul, each with the ability to configure beacon interval rates per radio. The clients consist of an Ipad Mini, Samsung Galaxy S4, and Windows 7 laptop. The test case separated each AP into two distinct SSIDs on different channels. Only 5 GHz radios were utilized to ensure a cleaner spectrum to test in. Beacons ranging from 125ms, 150ms, 200ms, 300ms were configured on the secondary AP to simulate the delayed frequency in beacon broadcast. The default 100ms value was held constant, 10 sampling runs per radio were performed, then configuration would be switched on each AP to ensure that there was no BSSID dependency or hardware affinity by the client.

Test Devices	Model	Description
Windows 7 Laptop	Dell Precision M4500	Intel Centrino Ultimate N 6300A/G/N wifi card, Windows 7
Apple Ipad Mini 2	ME276LL/A	802.11A/B/G/N dual band , iOS 8.3
Samsung Galaxy S4	SGH-M919	Android 4.4.4 (kitkat), 802.11A/B/G/N/AC

Table 2: List of clients used in test

I. Non-Chambered Experiment with Network Preference Defined

A real world approach to this experiment was conducted in a residential setting with both APs connected to cable modems so they can be remotely accessed. The same SSID was broadcast on different channel to avoid co-channel interference, the client used were an Apple Ipad Mini 2 and Samsung Galaxy S4 mobile phone. The average RSSI was logged around -40 to -50dB, or more. The SNR was measured from the same location as the clients using a Fluke Wi-Fi Air analyzer provided values around 40-50dBm. See Figure 6 for the test setup

Both iOS and Android test clients were associated to public hotspot SSID and then introduced to the non-chambered test environment. The Android test client associated to the 100ms AP in all sampling runs and to the private SSID as the beacon interval increased for the public SSID. The iOS test client tended to associate to the last known SSID which was the public SSID in all sampling runs. The explanation for this could be attributed to the fact that iOS innate connection behavior favors the last known private SSID which was the public SSID as indicated in the iOS Deployment Reference Guide [4]. Even as the beacon interval increased on the public SSID, it did not steer the iOS test client to the private SSID. This behavior was tested only on one specific client with one version (iOS 8.3).

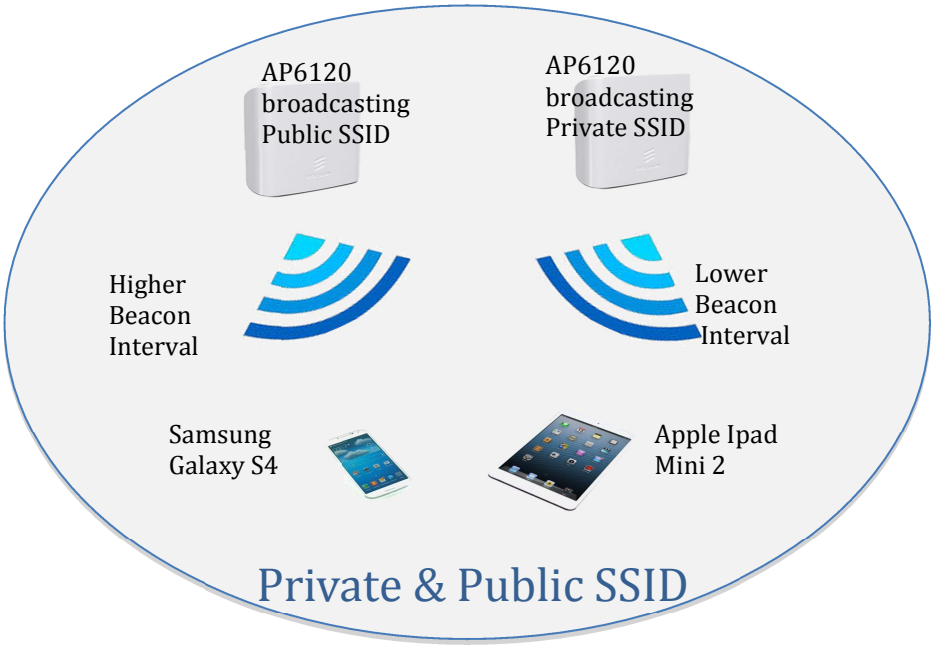

Figure 6: Non Chambered Experiment Setup

An important caveat to note here is the simulated analysis is performed on two separate radios/AP on different channels. Access to a reference Wi-Fi MAC layer to tweak beacon interval per SSID would have been preferred, but due to slow or lack of response from various vendors, we used a simulated approach instead.

II. Non-Chambered Experiment with No Network Preference Defined

The environment remained the same as in the prior experiment; the only difference was no network preference was defined on the test clients. After each sampling run, the networks were 'Forgotten' and Wi-Fi interface was disabled and re-enabled.
A sample of 10 runs was performed per client before alternating the values on each AP to ensure no hardware affinity. The results are summarized in Table 2

When Beacon Rate Increases to: /Devices	Apple Ipad Mini (% tendency to associate to 100ms radio)	Samsung Galaxy S4 (% tendency to associate to 100ms radio)
125ms	80%	55%
150ms	65%	45%
200ms	65%	50%
300ms	50%	60%

Table 3: Non-Chambered with no Network Preference Experiment Results

Based on the empirical analysis of the non-chambered experiment, there are tendencies for the Ipad Mini client to associate to an SSID with lower beacon interval (100ms). As the Beacon interval increases, there is a lesser tendency to associate to the AP with 100ms setting. There is still a minimum of 50% improvement in associating to the lower beacon interval radio.

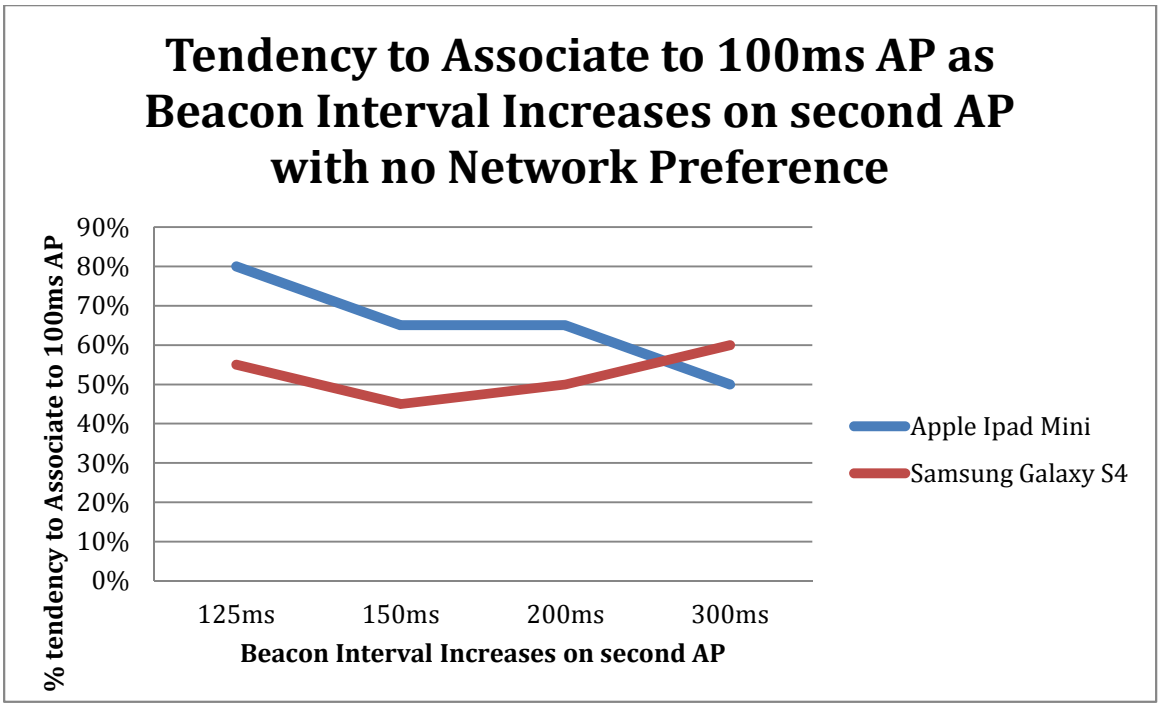

Figure 7: Chart inferred from Table 2

For the Samsung Galaxy S4, the reverse behavior is observed. As the beacon interval increases, there is a slight tendency to associate to the lower beacon interval AP (100ms). The overall results yielded a positive observation of an innate tendency by both iOS and Android connection manager to lean towards lower beacon interval SSID in the presence of differing beacon rates. Referencing Figure 7, the iOS test client, an Ipad Mini 2, has an 80% probability of associating to the default 100ms radio as the other radio's beacon interval increases. Even when beacon interval increases to 300ms on the secondary radio, there is still a 50% likelihood it favors the default 100ms beacon interval radio.

III. Chambered Experiment with No Network Preference Defined

In this environment, each AP was place in a separate chamber with each radio cabled to another chamber containing a laptop running windows 7, (see Figure 8). Each radio was broadcasting on different channels to avoid co-channel interference. Separation between adjacent channels was accounted for to ensure adjacent interference wouldn't skew the results. The average RSSI was logged around -47dBm as reported by both AP. The Wi-Fi radio on the laptop was then enabled and disabled for each sampling run to determine to which AP it would associate. No priorities were set in the laptop's connection manager. The initial test was a difference between 100ms vs. 125ms for the beacon interval. The beacon interval value was incremented from 125ms, 150ms, 200ms, and 300ms. Unfortunately, the results were inconclusive as the AP kept crashing during a majority of the sampling runs.

Figure 8: Chambered Experiment Setup

IV. Chambered Experiment with Network Preference Defined

The chambered analysis was further conducted on the Windows 7 laptop with the order of wireless networks prioritized; the results were unanimously favored the lower beacon interval AP for all runs, (Table 4 and Figure 9).

When Beacon Rate Increases to: /Devices	Windows 7 Laptop (% tendency to associate to 100ms radio)
125ms	100%
150ms	100%
200ms	100%
300ms	100%

Table 4: Chambered with Network Preference Experiment Results

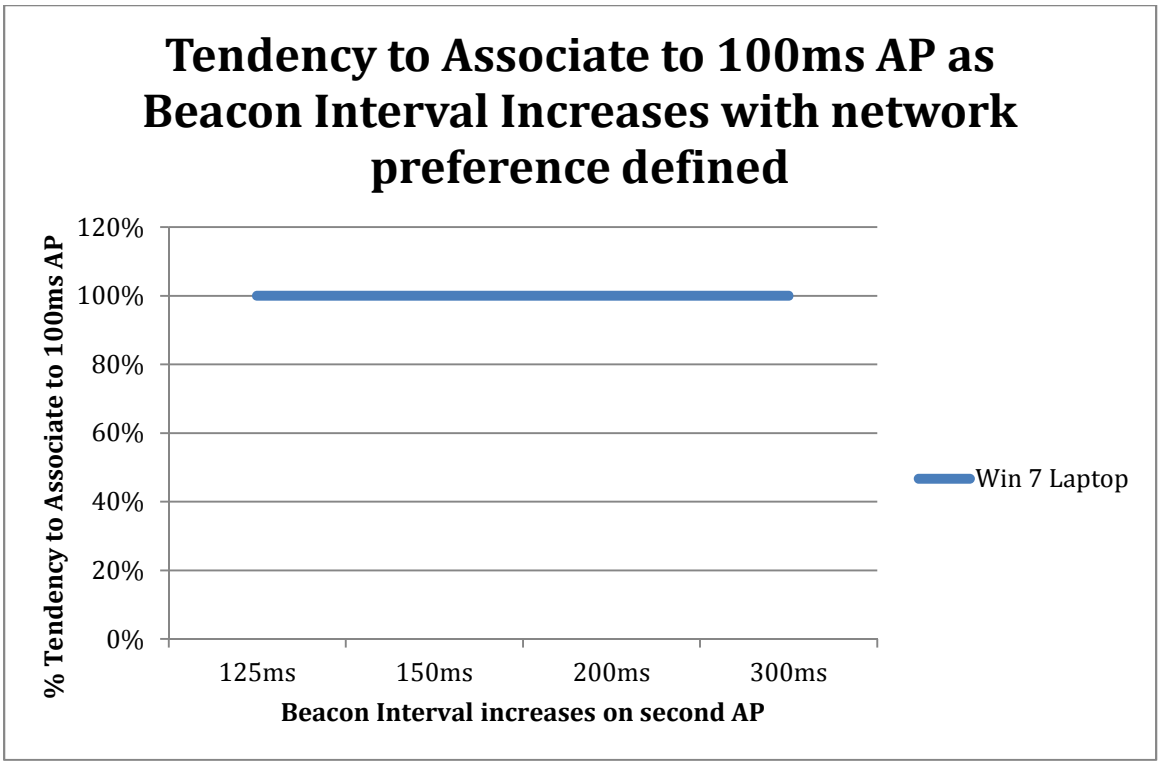

Figure 9: Chart inferred from Table 3

The pertinent observation in this experiment was the network SSID preference was defined on the Windows 7 laptop, the private SSID was set as the 1st SSID to seek then the public SSID as 2nd. As the beacon interval increased on the simulated public SSID, the test client still retained the tendency to associate to the 100ms private SSID. The experiment switched configuration to ensure there was no BSSID or hardware affinity between AP. To expand on the likelihood of the test client associating due to network preference, the same simulated private SSID AP was then configured with a higher beacon interval than the private SSID AP. The results in the next few sampling runs were a little more random as the test client attempted to seek the private SSID AP but due to the higher beacon interval, couldn't do so, and associated occasionally to the public SSID instead.

Proposed MAC Layer Frame Manipulation to Enhance SSID Prioritization of Private over Public SSID

Based on the observations of the experiments, the three proposed resolutions were inferred as a means of ensuring SSID prioritization.

I. Approach 1: Scheduling Implementation

Given that each beacon frame sent from the AP to STA will contain a beacon interval block defined within the frame body, the proposed implementation employs a change in beacon intervals between SSID or even suppression of all other SSID other than the home SSID through cognitive scheduling. A client device will associate to the home AP and the client MAC will typically be cached in the list of connected devices even after disassociation. The daily schedule of client association can be learned and a schedule developed based on defined sampling rates. This fingerprint will then enable application of a cognitive algorithm that either increases beacon interval or suppress all other SSIDs other than the home one in the Beacon

Interval block of the beacon frame during specified times of the day.

A use case to better describe this implementation is a client that returns home anytime between the hours of 5-7pm after work or between certain time blocks on weekends and 'sees' more of the home SSID than other SSID broadcasted by the AP.

Between the predefined hours of return, the AP will broadcast beacon frames with home SSID interval set to 100ms (default value) and increase the value for other SSIDs, thus increasing the frequency that the home beacon may be seen over others. Figure 10 provides the data flow diagram of the proposed implementation:

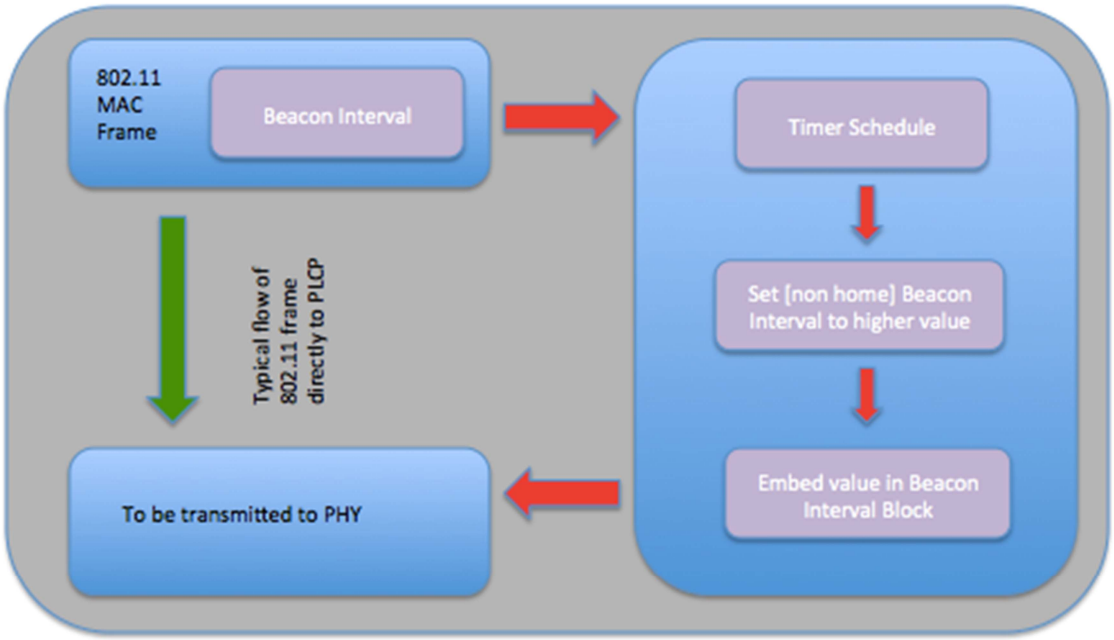

Figure 10: Approach 1: Cognitive Scheduling for SSID Prioritization within MAC layer

The green arrow line in Figure 10 represents the normal flow where an 802.11 frame embeds the necessary beacon values and sends it to the PLCP sub layer for transmission via the PHY layer. The implementation proposes an alternate step in terms of embedding a beacon value to insert higher frequency values for non-home SSIDs to increase the probability of the home SSID being detected by the client's passive scan or probe request when the client returns home within the specified timeframe. The following pseudo code describes the logic within the MAC layer:

While timestamp (i) is between 5pm-7pm, implement scheduling algorithm

{

i=0

Write a higher frequency beacon interval (>100ms) to non-home SSID;

Replace the more significant bits with higher defined B (Beacon Interval) values

i= i+B

}

II. Approach 2: Reject Initial Probe Requests per Unique Client MAC

A client's innate connection manager priority is simple for iOS, the order is as listed:

1. The private SSID is most recently associated

2. A private SSID
3. A Hotspot SSID

In contemporary deployments, the hotspot and home SSID have no differentiating trait at the MAC layer level other than the SSID name. Passpoint 2.0 has the ability to address some of this issue but has not been deployed nor supported widely yet. A mobile client will associate to the public SSID throughout the day and upon return to its residence will attempt to re-associate to the same public SSID. This behavior was observed in the 'non-chambered with network preference' defined scenario. The variations in beacon interval did not deter the iOS device from associating to its last known network. Even though more analysis is warranted, this methodology was conceived as a result.

The proposed implementation is to reject all initial probe request to the public SSID [within the residence], this will force the innate connection manager to select the next best private SSID which will be the home SSID.

The sequence diagram in Figure 11 describes the rejection of the initial probe request of the client upon entering the proximity of the residential Wireless Gateway. The probe response will contain [optionally] values forcing the client to proceed to the next valid SSID. These values may include a null SSID along with a reason code indicated within the Frame block of the 802.11 MAC management

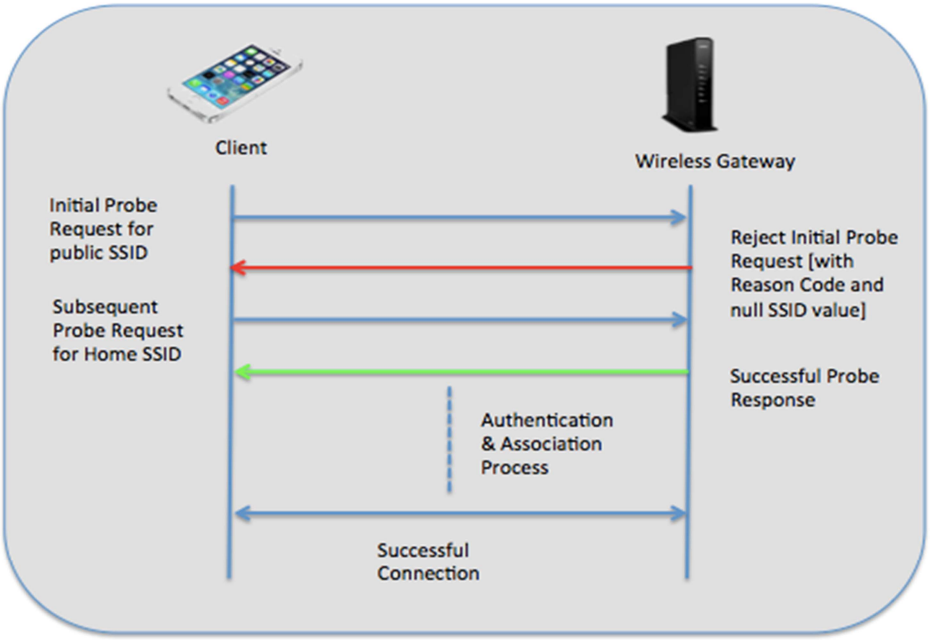

Figure 11: Approach 2: Rejection of initial Probe Request

Note that this algorithm is not a blacklist but merely a lack of response to the initial probe request of each unique MAC and if user desires to associate to the public SSID, the process can be manually triggered to force an association. This process is no different than what is available today by entering the connection manager User Interface and selecting the public SSID.

III. Approach 3: Smart Association to Home SSID

There are mechanisms within a service provider's core network today to indicate a user is sending and receiving traffic behind their home network. When this use case applies, and the client attempts to join a non-home SSID, the initial

association request will be validated the client is behind the home DOCSIS network based on billing account information. The Association response from the AP to the STA will in fact be a disassociation and deauthentication frame used to end the initial association to the non-home SSID. A slight delay timer will begin after this frame is sent to allow time for the client to receive and process the disassociation. A Beacon frame will then be issue after the delay timer expires containing the Receiver Address (client) and the home SSID to connect to within the Probe Request frame.

Subsequently, the client's next action is to perform an [active/passive] scan and potentially may attempt to re-associate with the public or home SSID. The behavior observed all experiments lead to this methodology as evident by how both iOS and Android client behaves. In the event that the client does associate to a non-home SSID, there is reliance on the AP to intelligently switch the client back to the home SSID.

This algorithm will ensure the client in fact will respond to the probe request frame directed from the Source AP (home) with the proper home SSID. Figure 12 describes the process flow of the proposed approach.

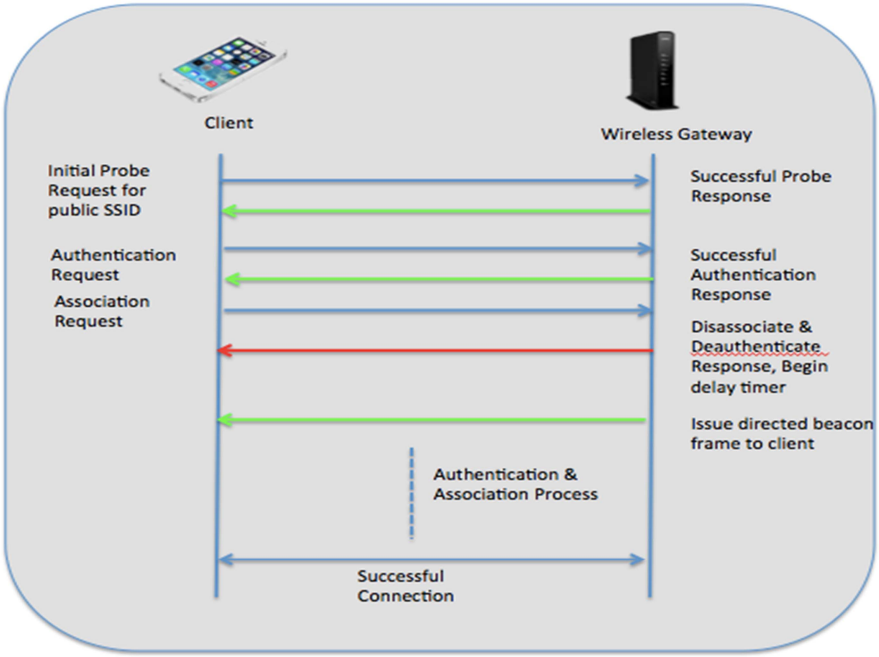

Figure 12: Approach 3: Smart Association to Home SSID

The following pseudo code describes the logic within the MAC layer:

```
When client associates to public SSID behind home cable modem
{
        Validate client traffic is sourced from home cable modem;
        Respond with Disassociation and Deauthentication frame;
        Begin delay timer i=0;
        When i=3ms
        {
                Send Beacon Frame directed to client with Home SSID value embedded;
        }
}
```

Further Analysis

The proposed methods described in this paper has been submitted and accepted for patent filing as potential implementation on wireless gateway routers used in the service provider industry. There are additional analyses required to optimize the design and adapt to the evolving changes in 802.11. For example, manipulating the beacon interval may affect the client behavior; increasing beacon interval to a larger value may cause delays for clients attempting to connect to the AP as the clients scans through every channel seeking for the beacon frame, potentially leading to a longer association time. Conversely, if the beacon interval were to decrease, more bandwidth is consumed but the client will rapidly associate to the AP; as a fallout, power consumption of the client may be affected due to more frequent scanning that occurs.

References

[1] http://www.huffingtonpost.com/vala-afshar/50-incredible-wifi-tech-s_b_4775837.html

[2] http://marketingland.com/nielsen-time-accessing-internet-smartphones-pcs-73683

[3] http://www.ideaconnection.com/blog/2014/02/the-internet-of-things-predictions-for-home-automation-in-2014/

[4] https://manuals.info.apple.com/MANUALS/1000/MA1685/en_US/ios_deployment_reference.pdf

[5] http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/CMX/CMX_802Fund.pdf

[6] Figure 5 Beacon Interval frame : http://flylib.com/books/en/2.519.1.35/1/

[7] Figure 1 Active Scan: http://www.ciscopress.com/articles/article.asp?p=360065&seqNum=3

[8] Figure 2 Passive Scan: http://www.h3c.com/portal/Technical_Support___Documents/Technical_Documents/Security_Products/H3C_SecPath_U200-A_U200-M_U200-S/Configuration/User_Manual/01-Firewall_Web_Configuration_Manual-5PW100/201205/746164_1285_0.htm

[9] Figure 3 802.11 Client State Machine : http://cecs.wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks.htm

[10] iOS Deployment Reference, 2015, Apple.