SCTE CABLE-TEC EXPO 23
CELEBRATING 40 YEARS

2023 Fall Technical Forum
SCTE • CABLELABS • NCTA

Virtualization in Wi-Fi to Fix Many Long-Standing Customer Experience Issues

Using Virtual BSS (VBSS) To Address Complex and Time-Consuming Client Roaming in Multi-Access Point Networks

A Technical Paper prepared for SCTE by

Ian Wheelock
CTO Europe
CommScope Inc
Cork, Ireland
Ian.Wheelock@CommScope.com

With additional support from CableLabs technical personnel

Steve Arendt, CableLabs Advanced Technology Group

Steve Glennon, CableLabs Advanced Technology Group

John Bahr, CableLabs Advanced Technology Group

Tucker Polomik, CableLabs Advanced Technology Group

Zackary Foreman, CableLabs Advanced Technology Group

Table of Contents

Title **Page Number**

List of Figures

List of Tables

1. Introduction

Wi-Fi® has become the primary way that people and their many devices connect to the internet at home and on the go. As homes have more devices and are getting bigger, people are adding more Wi-Fi access points to their networks to improve coverage and capacity. Devices often switch from one access point to another as they move around, whether within the homes or when moving between home, work, and elsewhere.

However, how devices move around the home has been a long-held issue within Wi-Fi, even with a variety of solutions to the problem. Devices like smartphones, tablets, and wearables sometimes stay connected to an access point even when it cannot provide a good enough connection. This can be extremely frustrating for users who expect Wi-Fi to be as reliable as their cellphones.

Mobile Wi-Fi solves this Wi-Fi roaming issue by creating a virtual basic service set (VBSS) for each device that is moving around. This technology, developed by CableLabs and shared with groups like the Wi-Fi Alliance, forms the basis of the solution. A reference implementation, which was used to produce the results in this paper, has been designed and contributed to the prpl Foundation prplMesh project. The decision of which access point handles the VBSS for a device is made by an intelligent Controller function (with interfaces to the multiple access points in the Wi-Fi network), and not by the device. This allows devices to roam between access points smoothly, with the Controller making sure the device connects to the best access point and radio. The system can also disconnect the device if the Wi-Fi network cannot handle its needs anymore, such as when a device departs from home. What is important is that this solution works with older devices too, without needing changes or newer Wi-Fi features on the device. Mobile Wi-Fi will improve the user experience in homes, apartment complexes, businesses, and, eventually, in a city-wide manner to ensure completely seamless Wi-Fi mobility.

2. Problem Space and Solution

2.1. Wi-FI Evolution And Roaming

Back when Wi-Fi was first introduced as a wireless alternative to Ethernet, no one really thought about the idea of Wi-Fi roaming. The idea of smoothly transitioning between different Wi-Fi access points was not a consideration at that time. The challenges of making Wi-Fi roaming work well did not pop up first in homes. Instead, they showed up in places like offices and similar places where there were several Wi-Fi access points on the same network.

Fast forward to the last six to seven years, many homes have adopted the use of multiple Wi-Fi access points too, mostly to improve the performance of their networks, dealing with range and throughput issues. In such an environment, with multiple access points and large numbers of connected devices, with many mobile devices moving around while running video calls, video streaming or gaming Wi-Fi roaming problems have become an issue.

In the past, these issues were mostly a concern for businesses. They had to figure out how to make sure devices stayed connected as people moved around with those devices. But now, regular homes are dealing with similar challenges as they set up multiple access points to cover larger areas or deal with lots of devices all without a dedicated IT (Information Technology) team to make it work. The various business or enterprise solutions can work in a residential setting, but they are far more costly than the typical solutions provided by service providers to their customer. A lot of the cost is in the more advanced APs capable of dealing with much larger numbers of connected devices, as well as alternative security requirements, network management requirements and overall complexity of operating such devices in the

home. A service provider solution can be based on a standalone in-home setup with an advanced Controller with several basic policies or a cloud-based solution, with a cloud Controller. Both are a lot less complex than an enterprise Wi-Fi solution.

To sum it up, the journey of Wi-Fi roaming, from being an overlooked detail when Wi-Fi was born to becoming a critical aspect of modern networks, shows how far technology has come. The shift from businesses to regular homes facing these challenges emphasizes its growing importance. With more home devices being connected to the Internet, more IoT (Internet of Things) devices in the home, then dealing with the complexities of Wi-Fi roaming will remain a big task, pushing the need to find new and better ways to make sure wireless connections stay strong and seamless.

Over the past ten years, there has been a significant increase in the number of devices that people carry around or use while moving around their homes or workplaces. It all started with adding Wi-Fi to smartphones and music players like the iPod Touch. This has now expanded to a whole plethora of devices like fitness gadgets, tablets such as the iPad or MS Surface, cheaper laptops like Chromebooks, pet trackers, robot vacuum cleaners, home security cameras, smart speakers, and even VR (Virtual Reality) headsets like the Meta Quest 2. Many of these devices are often used with demanding workloads while people are moving around their homes or offices. In the past, when the most demanding thing people did with Wi-Fi was checking emails on a Blackberry phone, there were few problems with switching between Wi-Fi points, and people hardly noticed any issues. But now, with things like streaming videos all around the house or using VR headsets in different rooms, these "smart" devices do not always work well with Wi-Fi, and it can cause problems.

2.2. Understanding The Problem

In the following paragraphs we describe the current situation relating to steering capability of existing networks and their connected clients and how it impacts on overall performance of the network and customer quality of experience.

2.3. Wi-Fi Multi-Access Point Networks

This paper assumes that the home Wi-Fi network already exists and is utilising some form of interconnectivity between multiple APs that allow for seamless connectivity between APs. Such a network could be based on an IEEE 802.11s mesh network or a Wi-Fi Alliance Certified Wi-Fi EasyMesh™ network [1], [2] or a proprietary meshing scheme. In any case, the network would already be established with APs connected (either via wireless or wired connections) and enable continuous connectivity throughout the home for clients. In this paper, the primary issue being tackled is when a client remains connected to an access point or frequency band that is not the optimal choice. For instance, when a device moves around a home with multiple access points, it should switch from one access point to another to maintain a connection with the strongest signal, the least crowded one, or the one offering the best throughput. Traditionally client devices decide on what AP to use, basing their decision on signal strength of available APs and some other historical data. The client device has no understanding of how the wireless network is connected, or how heavily loaded each potential AP might be (with other clients and/or network traffic). Connected Wi-Fi networks, based on a mesh approach, can propose to the client device that it switch to a specific AP (considering all the network conditions across the different APs in the network), however it is up to the client whether it will accept the suggestion and switch, or stay connected to the existing AP. In other words, the client has the final say whether it moves or not.

In real-life networks, this process varies among devices and does not always proceed smoothly for users. For example, a client device might persist in staying connected to a weaker access point even when a better one is available. Imagine being on a video call over Wi-Fi and moving from one room to another. If

the client device continues to stay connected to the original access point, the call's quality could suffer due to slower speeds. Ideally, the client device should switch to the closer access point, but this often does not occur. Clients might hold onto a specific access point even when it is not delivering the best performance (commonly referred to as a "sticky client" situation). To the user, this results in applications or experiences that do not function well due to terribly slow data speeds.

2.4. Client Roaming In The Home

To explain this further, a typical multi-AP network in a home with two APs and a Controller are shown below. The performance of client A connected to AP 1 degrades as the client moves away from AP 1 in the Wi-Fi network. Even though the client ends up being adjacent to AP 2, it persists with its connection to AP 1, leading to a degraded experience. This is known as the “sticky client” problem, where the client persists with the poorer connection. This not only causes mediocre performance for the client but can also impact all other clients connected to the same AP, as well as clients in overlapping APs that use the same radio band and frequency.

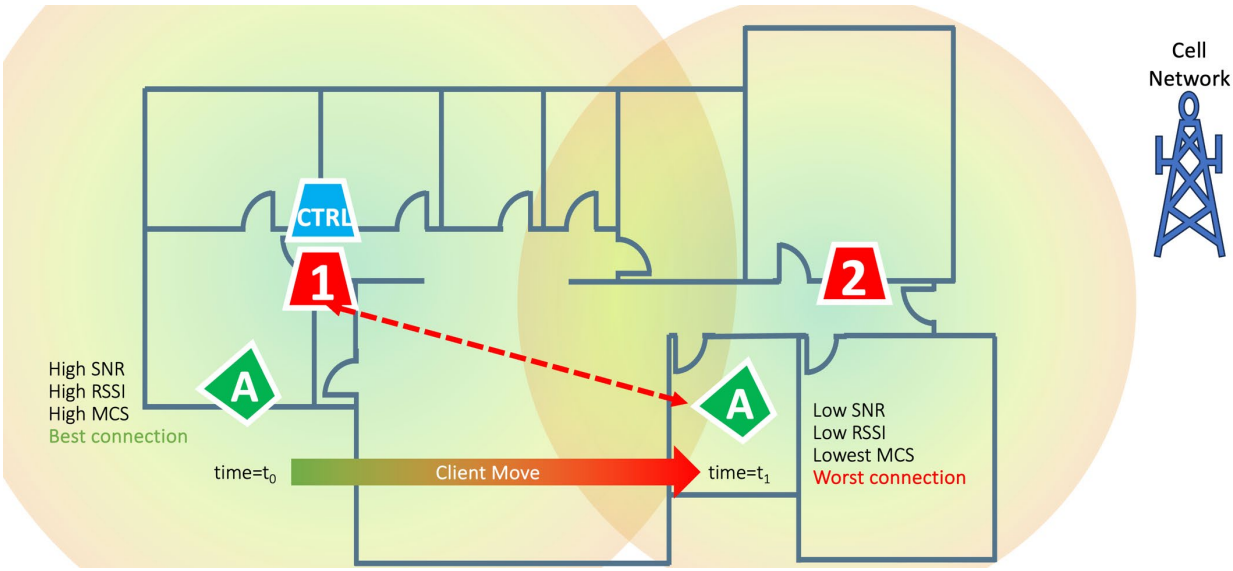


Figure 1, Multi-AP Home With Internal Client Wi-Fi Roaming Issues

2.5. Client Roaming At The Edge Of The Network

A similar problem occurs when there is no suitable AP to transition to when a client reaches the edge of coverage of the Wi-Fi network. In this case, the best course of action for the client would be to terminate the Wi-Fi connection altogether which would trigger the connection to switch over to a different interface such as cellular in the case of a mobile phone. However, clients often stubbornly cling to a Wi-Fi connection that no longer serves their needs. For example, a user gets in their car while still on the video or teleconference they start at home on their phone and starts to drive away. Instead of switching to the

cellular interface, the phone clings to the fading Wi-Fi signal, resulting in a frozen conferencing application.

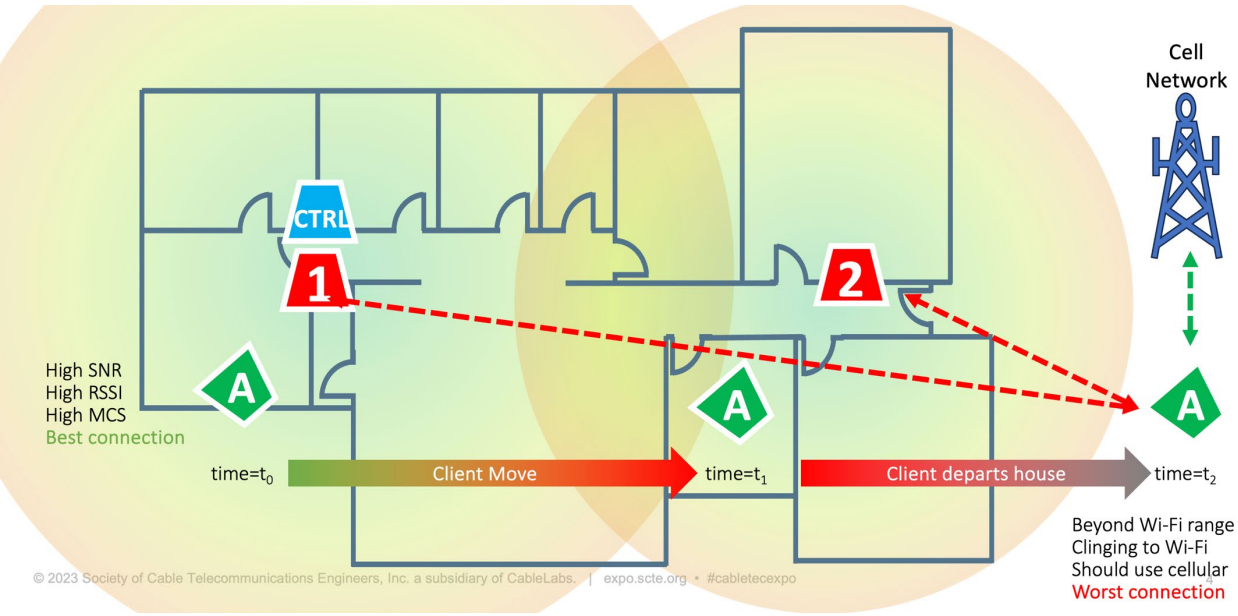


Figure 2, Multi-AP Home With External Client Wi-Fi Roaming Issues

2.6. RF Performance And Client Quality Of Experience (QoE)

The movement of the client throughout a home complicates Wi-Fi performance. RF signals used in the 2.4, 5 and 6 GHz frequency bands are subject to attenuation. This could be free space path loss, where there are no obstacles between an AP and a client, and the RF signal strength simply diminishes over distance due to physics. Another source of attenuation are obstacles such as walls (internal or external), insulation, windows, furniture, people, etc that all contribute to the attenuation of the RF signal – some obstacles are worse than others. The distance between the AP and client and any obstacles in between all impact the PHY rate that can be used – defined by a range of different Modulation and Coding Schemes (MCS). Depending on the version of Wi-Fi, the MCS options are numbered starting with MCS 0 that defines the lowest performance, ranging all the way up to the maximum performance available in Wi-Fi 7 using MCS 13. MCS0 offers a maximum PHY data rate of 72 Mbps for a 160 MHz wide Wi-Fi channel, while MCS11 gets up to a maximum of 1,200 Mbps. Higher Wi-Fi data rates are also possible when multiple spatial streams (SS) are used, which are enabled using Multi-Input/Multi-Output (MIMO) processing, with a typical AP supporting up to 4 SS per radio. In the case of a 160 MHz Wi-Fi 6 with 4 SS, the maximum PHY rate is 4,800 Mbps. These are maximum PHY rates for the Wi-Fi channel in use, and cover all communication, both uplink and downlink as Wi-Fi is half-duplex. This is different compared to 2.5 Gbps Ethernet which is full duplex and offers 2.5 Gbps for transmit and receive, for a total of 5 Gbps capacity.

2.7. Received Signal Strength Indicator (RSSI) & Signal to Noise Ratio (SNR)

The Received Signal Strength Indicator (RSSI) and the Signal to Noise Ratio (SNR) are used to determine what MCS can be used for data transmit/receive. While the RSSI value is a well-recognised metric that provides a simple measure of signal strength in Wi-Fi networks, most Wi-Fi mesh networks will use a more standardised metric, called the Received Channel Power Indicator (RCPI) instead. RCPI provides a method for measuring signal strength that also considers the noise and interference levels of

the Wi-Fi channel. RCPI is also especially useful in dynamic conditions (such as devices moving swiftly through a multi-AP residential network), helping to make better decisions about which channels to use or what access points to connect to. Throughout the rest of this document for the sake of simplicity RSSI is used as the measure of signal strength, but RCPI is the actual measure that a mesh Controller expects to receive to optimise client steering.

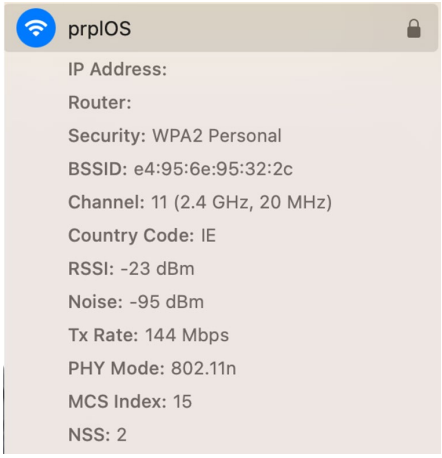


Figure 3, Typical Associated Wi-Fi Performance Readout (Including RSSI)

2.8. Varying RSSI Impact On Maximum Performance

The MCS defines what the maximum PHY rate is allowed. For static devices operating in a static environment, the RSSI/SNR will rarely change, allowing for the same MCS to be achieved; however, any Wi-Fi client that is moving around, or even held differently (e.g., landscape vs portrait viewing on a tablet), then the RSSI/SNR (and subsequently MCS) will change. The following diagram shows how the Received Signal Strength Indicator (RSSI) can change as a client moves away from an AP. This has a corresponding impact on the PHY rate (the diagram assumes that there is sufficient SNR for each MCS).

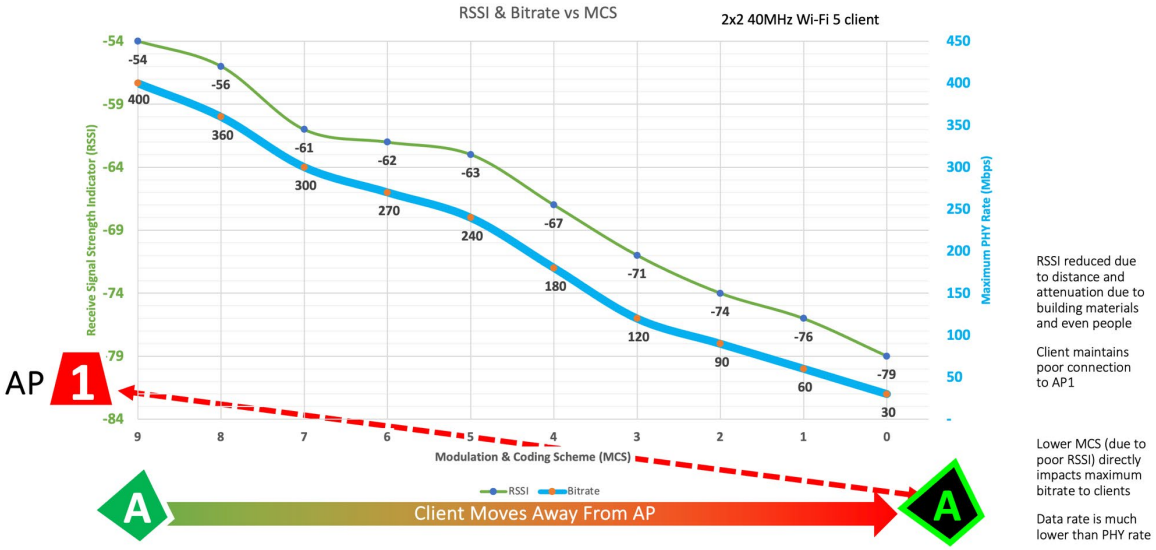


Figure 4, Impact of Wi-Fi Client Movement From AP On RSSI And PHY Rate

The lower the RSSI (assuming sufficient SNR), the lower the achievable PHY rate is. It must also be understood that Wi-Fi is half-duplex, meaning the PHY rate is the total capacity of the link (both uplink and downlink). In addition, Wi-Fi is a contention based MAC (Media Access Control) (for the most part) meaning that there are delays before clients or APs can transmit data due to how clients must check for quiet time on the RF/air interface before attempting to transmit, meaning that the suggested PHY rate does not translate 100% into usable data rate.

3. Client Roaming Between Access Points

As the client moves away from the AP it is associated with, its constantly examining network conditions to determine what action to take to ensure best performance. One action might be to switch from 5GHz to 2.4GHz (it has longer range), or another action might be to connect to an AP with better RF performance.

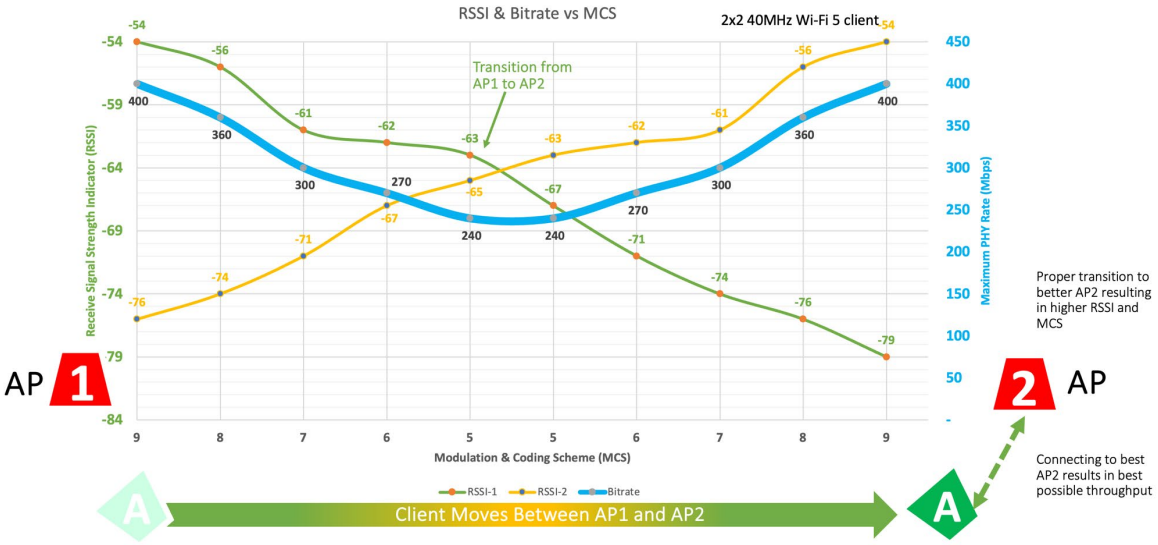


Figure 5, Wi-Fi Client Roaming To A New AP, Ensuring Performance

The above chart shows how an ideal client (maybe one that does not exist) can decide to roam to a different AP to maintain the highest performance levels. As the client moves, it identifies the available AP, and makes its own steering/roaming decision to disassociate from AP 1 and (re)associate with AP 2.

3.1. Controller-led Client Roaming Between APs

The Wi-Fi client has limited visibility into the organisation of the Wi-Fi network, what APs are connected where, if they use Wi-Fi backhaul or Ethernet backhaul, how loaded they are with other clients, etc. As a result, decisions it makes concerning roaming from one AP to another are primarily informed by the RSSI/SNR it can detect for different APs. In a lot of mesh networks, there are Controller entities that are used to help form the network of APs as well as deal with the operation of the network, with respect to optimising the performance of the connected APs and connected clients. The network provides detailed statistics from the APs and clients to the Controller to assist in forming a model of the network and clients. The Controller can use its model to identify opportunities for improving performance, particularly for clients that are mobile, or dealing with APs that have gone offline, or dealing with overlapping/ neighbouring Wi-Fi networks that use common RF frequencies.

In the case of clients that need attention (i.e., need to be moved to a new frequency band or a new AP), the Controller triggers a steering event that uses a variety of techniques to try to influence the client. Some of the primary methods that have been developed (there are others) include:

1. Allow-List/Deny-List
2. 802.11v BSS Transition Management (BTM)

3.2. Allow/Deny List Wi-Fi Client Steering

The Allow-List/Deny-List is one of the original approaches developed, relying on the ability of the Controller to tell certain APs in a network to not allow the nominated client from associating with them (as well as disassociating the client if it is associated to one of these APs). The Controller must also advise the target AP that it should allow the nominated client to associate. This brute force approach for steering does not require any extra Wi-Fi features with a client to work, and has a high chance of success, however some stubborn clients may refuse to re-associate, and drop from the network.

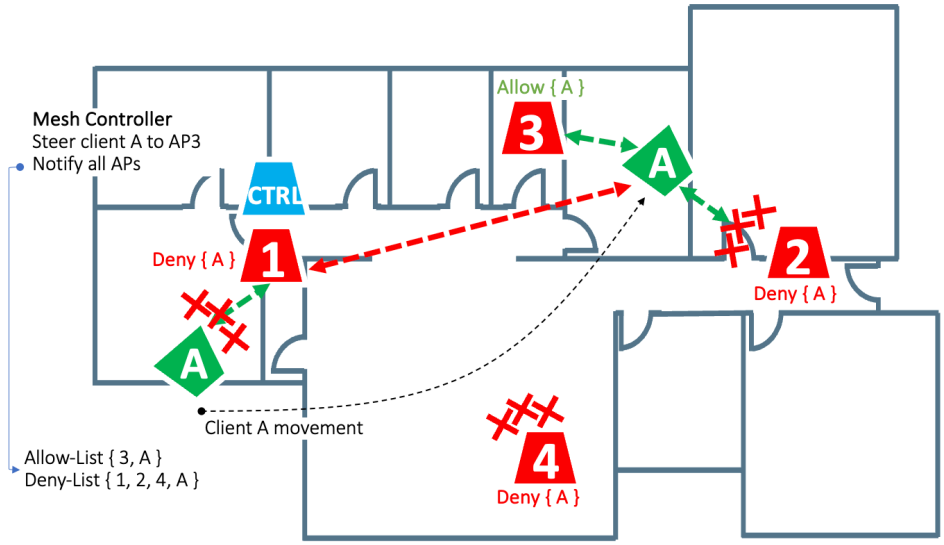


Figure 6, Mesh Controller Forcing Allow/Deny List For Client Steering (to AP 3)

3.3. BSS Transition Management Wi-Fi Client Steering

The BTM method takes a different approach, where the Controller requests the AP, the client is associated with, to send an 802.11 message with a list of other APs that it strongly suggests the client should consider associating with. This approach does require the client to support BTM, which is defined within the Wi-Fi Alliance Agile Multiband specification. There are two versions of BTM, 802.11v and 802.11r Fast Transition (FT). The main difference between these is the shortened time to complete the security establishment following client association. The overall transition time experienced using either of these approaches may be faster or slower depending on the combination of AP and clients involved.

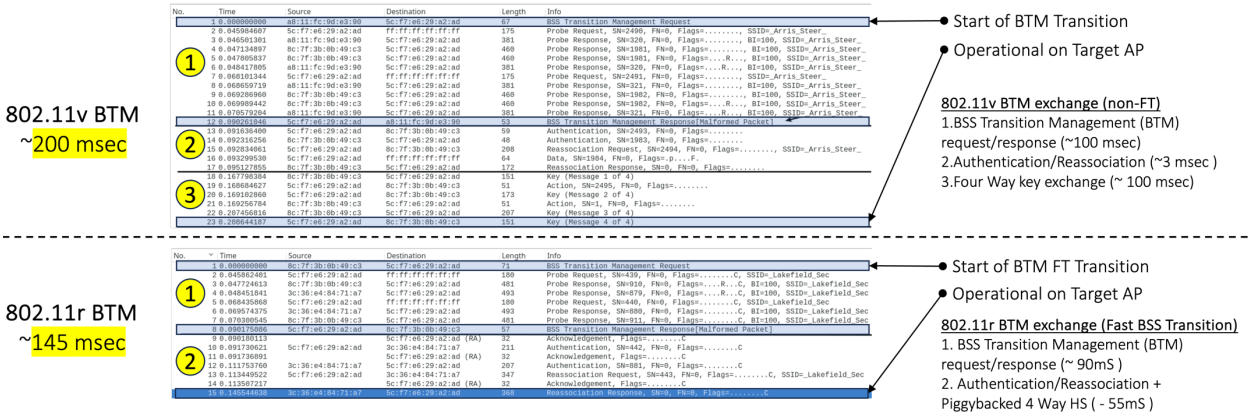


Figure 7, Comparison Of 802.11v And 802.11r FT Steering

3.4. Possible Consequences Of Steering Wi-Fi Clients

These approaches have some unintended consequences when moving clients. There is a tension between what the Controller and AP network request and what the client is willing to do. The client already has its own suite of roaming policies and approaches and receiving steering instructions from the network can often cause some conflict. This is compounded by having a variety of different Wi-Fi clients in the home that all have variations in what protocol support they have and how they react.

Common problems associated with this issue include:

Sticky Client – A client decides to stay associated with a particular AP even though a closer, much better performing AP is available. Due to operating at a very low MCS, this results in poorer performance for the individual client, but can also impact other clients in the same BSS due to the poor performing client consuming more "airtime" than is necessary (that is when a client continuously sends large amounts of data at a low MCS, is can take an unfair share of transmission time compared to other clients).

Ping-Pong Effect – a client may accept a steering instruction from the Controller/AP, stay on the new BSSID for a brief period, then switch back to the original BSSID. This has an obvious impact on client user experience, as the constant switching impacts on user traffic.

Interoperability issues – Some Wi-Fi Clients may have some or no support for BSS Transition Management mechanisms, as a result some may not handle steering requests as smoothly as others, leading to inconsistent results.

Unintended Disconnects – Sometimes clients get confused or give up on steering when they have been steered multiple consecutive times to different BSSIDs (Basic Service Set Identifier), partly because their steering algorithms believe their current connection is acceptable. This can result on clients becoming non-responsive, or worse, client disconnecting from the Wi-Fi network completely, requiring manual user intervention to reconnect.

Unfortunately, these problems are commonplace, and introduce considerable complexity for Controllers in terms of how they treat different clients differently, as well as having to maintain per-client information (device type, OS version, scorecard for different steering mechanisms, preferred steering method, etc). The possibility of the Controller negatively impacting a client (due to above problems) while trying to do good for the client presents a challenge as to how often devices should be steered.

In addition to challenges with compliance to the steering instructions, excessive transition/steering times also impact on the Quality of Experience (QoE) of the users. If the time is short (<30msec) then the steer is not noticeable. Transition times of less than 100 msec are sufficient for most real-time traffic streams (i.e., the user will not notice the communication gap) however longer transition times disrupt any activity on the mobile client. In addition, highly latency-sensitive traffic (e.g., mobile gaming) can be heavily impacted by even 50 msec of disruption.

As Wi-Fi availability and connectivity are fundamental to a clients Quality of Experience (QoE), risking such connectivity due to steering is a real concern. Having a steering technique that achieves close to 100% steering success, without these problems that might impact on QoE, is unbelievably valuable. This is where Mobile Wi-Fi and Virtual BSS comes in and will be discussed in section 4.

3.5. Wi-Fi Basics for Associating with an SSID

Wi-Fi clients connect to an AP, into what is known as a Basic Service Set (BSS). A BSS consists of a single AP and the client devices connected to that AP. The BSS is identified by a BSS Identifier (BSSID) which is a unique MAC address associated with a radio on the AP. When clients connect to that BSSID they become part of that BSS.

The Service Set Identifier (SSID) is a human readable name assigned to a wireless network. All devices within a BSS share the same SSID. It is common to have the SSID configured on different radios in the same AP (i.e., the same SSID on the 2.4, 5 and 6 GHz bands but each with a different BSSID), enabling all the AP radios to offer access to a specific SSID. The SSID will also be configured on radios of other APs within the network. Using this model means a client has complete choice between different APs in the network and different radio bands when trying to connect to a specific SSID. SSIDs (Service Set Identifiers) are advertised in Wi-Fi Beacon messages, allowing devices to scan available RF channels and collect the SSID/BSSID details to decide which SSID and BSSID they should associate on which AP that are within the range of the device. Note that this constant scanning for other SSIDs and BSSIDs by the client can impact on energy saving options within the client, as it is always checking for a better Wi-Fi connection.

An AP supporting multiple BSSIDs per radio can operate multiple concurrent SSIDs. An AP could support up to 16 BSSID per radio, and potentially have between 2 and 4 radios (Dual Band Concurrent (DBC), Tri-Band Concurrent (TBC) and Quad-Band Concurrent (QBC)), resulting in anywhere from 32 to 64 BSSIDs in a single AP. The following diagram shows the mapping of SSID, BSSID and BSS configured across two APs. Clients (with appropriate radios) can roam to any of the “in-range” BSSIDs configured for the “Home” SSID.

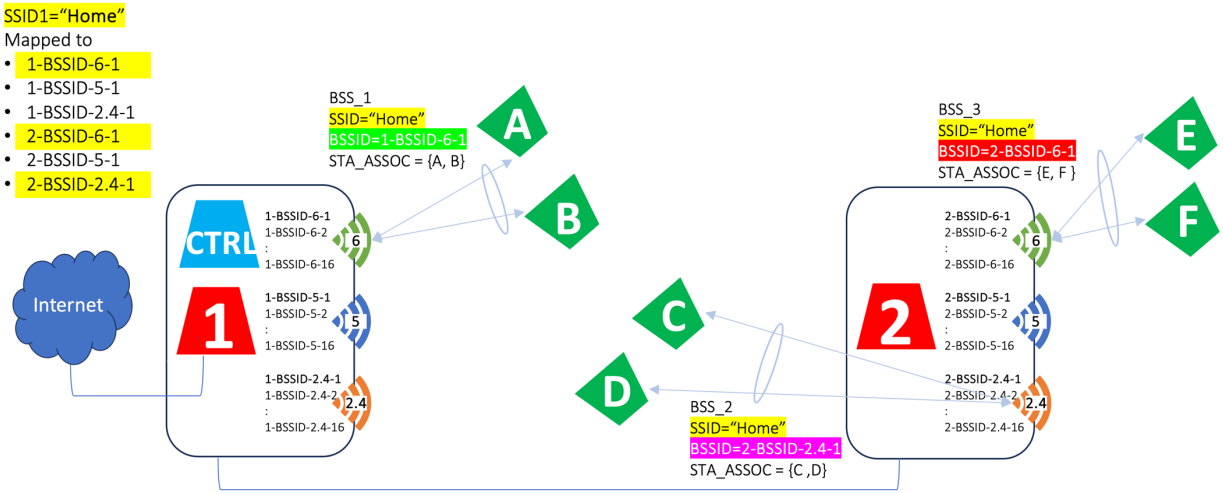


Figure 8, Example Of SSID="Home" Mapped Across All The Radios Of Two APs, With 3 different BSS Formed

When a client joins a BSS by connecting/associating to a specific BSSID, it conducts various MAC exchanges. A crucial exchange relates to establishing the security context for handling encrypted traffic sent between the client and the AP. This exchange results in a Pairwise Transient Key (PTK) for client<>AP transmissions and a Group Temporal Key (GTK) for multicast and broadcast traffic from the AP to clients. All encrypted traffic includes a sequence number, and each side (AP to client and client toAP) maintains separate packet numbers that are used in the creation of the security initialization vector (IV) when encrypting traffic (used to prevent replay attacks).

When Wi-Fi roaming is active, the client can pick any one of the available BSSIDs mapped to its current SSID and decide to roam to it (meaning it must complete Wi-Fi (re)association and repeat the 4-way security handshake for establishing security credentials before transmitting data traffic). Alternatively, a mesh Controller (maintaining details of every AP and the associated SSID/BSSID configuration) can direct a client to steer to an optimal BSSID to get maximum performance. Hopefully, the client complies with the direction. This whole roaming process, be it managed by the client or the Controller or both, continues the whole time the client is connected to the Wi-Fi network, constantly making efforts to ensure the best performance.

4. Virtualizing The BSSID, The Basis Of The Mobile Wi-Fi Solution

The details in the previous section show how standards and networks focus on ways to "request" a client to move from a BSSID on one AP to a BSSID on the same AP or a different AP, but never force the client to obey these directions. An alternative to this model is to move the actual "network" the client is connected to between APs. As mentioned already, when a client moves between BSSIDs, it must repeat the Wi-Fi association process. By focussing on moving the BSSID between APs, the client remains connected to the BSSID, never having to repeat the (re)association process. This is the basis of the "virtual BSS" concept – creating a per-client BSS with a unique virtual BSSID that is not tied to a particular AP, but rather a Virtual BSS that can be moved around a network with the client remaining connected the entire time.

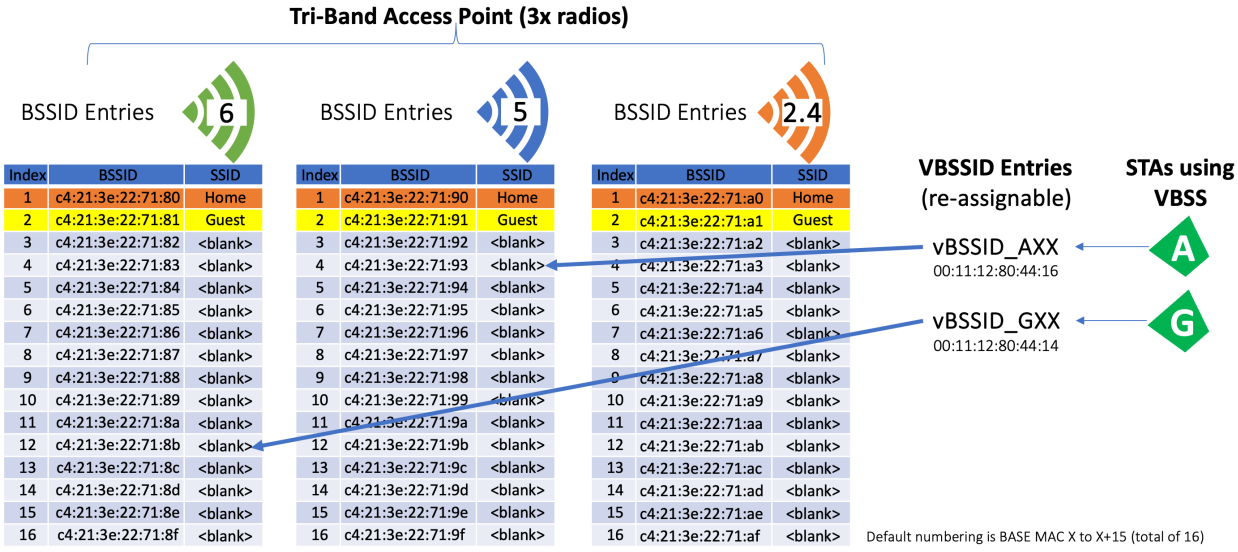
4.1. Previous Efforts for VBSS

The idea of a virtual BSS that follows a Wi-Fi client around actually has previously been explored. In 2016, the Wi-5 Project [3] worked on creating an open-source implementation for enterprise WLANs (Wireless LAN), but sources close to the project say that it suffered from extremely low throughput. In addition, there was a paper that focused on the personal virtual AP (PVAP) idea, [4], [5], [6] which presented the idea of moving a private BSS around in an enterprise WLAN (Wireless LAN) setup; however, CableLabs could not find any real-world implementations of it.

Both previous efforts focused on enterprise WLANs because (1) WLAN Controllers are present in enterprise networks to manage the movement of the BSSs (Basic Service Set), and (2) historically, enterprise networks were the only place where multiple APs on the same SSID were typically installed. However, in an enterprise environment, scalability becomes a problem because of the limited number of BSSs that current chipsets can support (e.g., currently 16 BSSs per radio) versus the number of active client devices moving around. Residential home networks are a more attractive target for virtual BSS implementations, given the lower number of BSSs required because of fewer mobile devices (out of all connected devices) in the home.

4.2. BSSID Capacity In APs For VBSS

For this paper, "Virtualising the BSS," the BSSID (and its related Wi-Fi MAC context) becomes "movable," and can be copied/transferred to a completely different radio on a different AP. This requires that the AP extract the entire operating context associated with the BSSID from the Origin AP Wi-Fi chipset/driver and the Controller communicate that information for installation in the Target AP when steering client devices. Obviously, there are limits to the number of these BSSIDs equipped per Wi-Fi radio. In most cases, a single BSS/BSSID is expected to manage 100's of connected devices dealing with all the per-client security and per client MAC context for each of these, while in the case of VBSS, the BSS/BSSID only deals with a single connected client. Referring to the following diagram, it is important to point out that in AP technology, most can operate between 8 and 16 different BSSID per radio – so in the example of a Tri-Band Concurrent (TBC) AP with three different radios, it would be expected to support up to 48 (3 x 16) BSSIDs.



Index	BSSID	SSID
1	c4:21:3e:22:71:80	Home
2	c4:21:3e:22:71:81	Guest
3	c4:21:3e:22:71:82	<blank>
4	c4:21:3e:22:71:83	<blank>
5	c4:21:3e:22:71:84	<blank>
6	c4:21:3e:22:71:85	<blank>
7	c4:21:3e:22:71:86	<blank>
8	c4:21:3e:22:71:87	<blank>
9	c4:21:3e:22:71:88	<blank>
10	c4:21:3e:22:71:89	<blank>
11	c4:21:3e:22:71:8a	<blank>
12	c4:21:3e:22:71:8b	<blank>
13	c4:21:3e:22:71:8c	<blank>
14	c4:21:3e:22:71:8d	<blank>
15	c4:21:3e:22:71:8e	<blank>
16	c4:21:3e:22:71:8f	<blank>

Index	BSSID	SSID
1	c4:21:3e:22:71:90	Home
2	c4:21:3e:22:71:91	Guest
3	c4:21:3e:22:71:92	<blank>
4	c4:21:3e:22:71:93	<blank>
5	c4:21:3e:22:71:94	<blank>
6	c4:21:3e:22:71:95	<blank>
7	c4:21:3e:22:71:96	<blank>
8	c4:21:3e:22:71:97	<blank>
9	c4:21:3e:22:71:98	<blank>
10	c4:21:3e:22:71:99	<blank>
11	c4:21:3e:22:71:9a	<blank>
12	c4:21:3e:22:71:9b	<blank>
13	c4:21:3e:22:71:9c	<blank>
14	c4:21:3e:22:71:9d	<blank>
15	c4:21:3e:22:71:9e	<blank>
16	c4:21:3e:22:71:9f	<blank>

Index	BSSID	SSID
1	c4:21:3e:22:71:a0	Home
2	c4:21:3e:22:71:a1	Guest
3	c4:21:3e:22:71:a2	<blank>
4	c4:21:3e:22:71:a3	<blank>
5	c4:21:3e:22:71:a4	<blank>
6	c4:21:3e:22:71:a5	<blank>
7	c4:21:3e:22:71:a6	<blank>
8	c4:21:3e:22:71:a7	<blank>
9	c4:21:3e:22:71:a8	<blank>
10	c4:21:3e:22:71:a9	<blank>
11	c4:21:3e:22:71:aa	<blank>
12	c4:21:3e:22:71:ab	<blank>
13	c4:21:3e:22:71:ac	<blank>
14	c4:21:3e:22:71:ad	<blank>
15	c4:21:3e:22:71:ae	<blank>
16	c4:21:3e:22:71:af	<blank>

Figure 9, Typical BSSID Mapping Per Radio, With SSID And VBSSID Assignments

Traditionally, before multi-APs were commonplace, the different radios in an AP would be configured with different SSID names for 2.4 and 5 GHz radios, for example “home” and “home5g”. While these different Wi-Fi networks are fully connected at an IP (Internet Protocol) level, a user must manually switch their device to pick either the “home” or “home5g” SSIDs, introducing unnecessary steps to jump between bands. With multi-AP networks, it is important that devices can automatically switch between different radio bands on the same AP as well as switch to other APs. As a result, the “home” SSID is often configured across each of the different radio bands in each AP, providing the same Wi-Fi network for connected devices (in other words the user does not have to manually switch).

In a typical Dual-Band Concurrent (DBC) AP operating with 2.4 and 5 GHz radios, with 16 BSSID per radio, the “home” SSID occupies 1x BSSID per radio. If there is a “guest” network, then that also occupies 1x BSSID per radio. This leaves 14 BSSID per radio. These 14 BSSID are available for the Virtual BSS (VBSS) operation that this paper outlines. Future Wi-Fi silicon that adopts VBSS and Mobile Wi-Fi Technology may be able to increase this arbitrary limit of 16 BSSID to a much higher number of BSSIDs, where such BSSIDs would only deal with a single client device, rather than the 100’s it is currently designed for.

4.3. Mobile Wi-Fi Technology

CableLabs Mobile Wi-Fi technology is a VBSS solution that has been developed over the past number of years and has reached a certain level of maturity. Mobile Wi-Fi was included in the fifth release of Wi-Fi EasyMesh (R5), and a reference implementation has been submitted to the prplMesh codebase [7]. However, it must be noted that the technology is not specific to Wi-Fi EasyMesh but rather can be used in any multi-AP management system. In other words, this technology is more of a steering technique that can be considered an alternative to the Deny-List or BTM steering approaches. The technology has been proven to work and is now ready for commercial adoption.

Like other VBSS solutions, Mobile Wi-Fi creates a special VBSS for each client and moves that VBSS across APs and radios as the client moves to ensure the best radio is serving the client. A central Controller manages the transitions between APs. The central Controller is likely to operate on one of the APs, normally the primary Gateway for the home, but can also be operated from a cloud platform (given the necessary remote configuration protocols are in place).

4.4. Mobile Wi-Fi Basic Operation

A key principle of Wi-Fi exploited by Mobile Wi-Fi is that a client's transmissions are not just directed at the AP its associated with; any AP also operating or able to monitor, on the same radio band and channel will receive these same transmissions, as shown in the following diagram. APs without the VBSS security context cannot decrypt any of those client data transmissions.

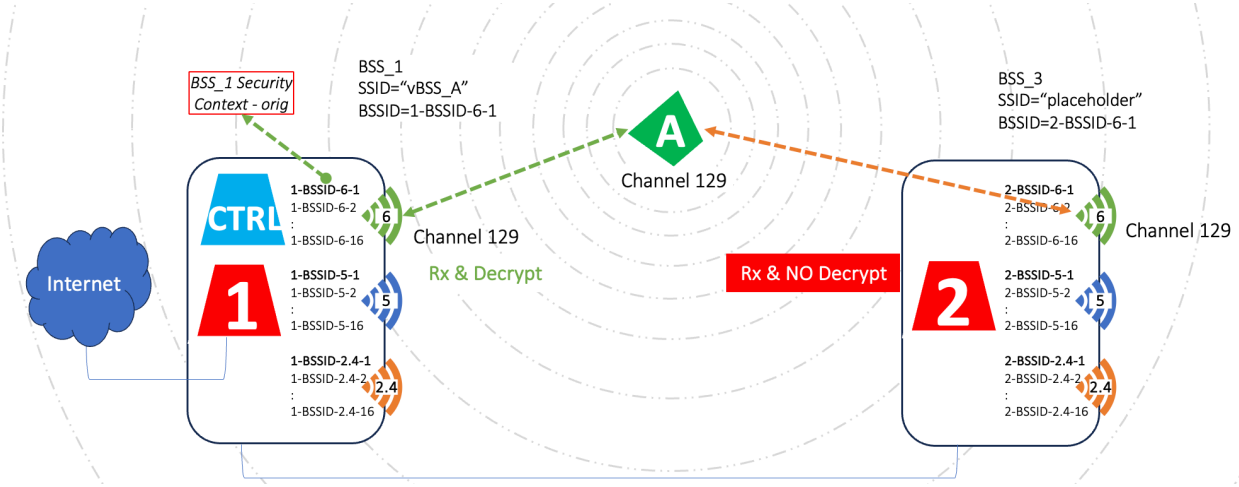


Figure 10, Client A Transmissions Received By Multiple APs, Only Decrypted By Associated BSS

This principle is taken advantage of when the VBSS is transitioned between AP 1 and AP 2, in that both APs will be able to receive the client's transmissions without having any interaction whatsoever with the client. In the case of a VBSS transition between two such APs, the client does not even know it is now talking to a completely different AP. The key here is to ensure the security context of the client BSS is copied to the target AP, enabling that AP to properly receive and decrypt the client data, as seen below. There is a brief period after the installation of the VBSS security context in the target AP (2) that traffic from the client (A) can be decrypted by both APs. This time must be minimised to prevent duplicate traffic entering the network from two different APs.

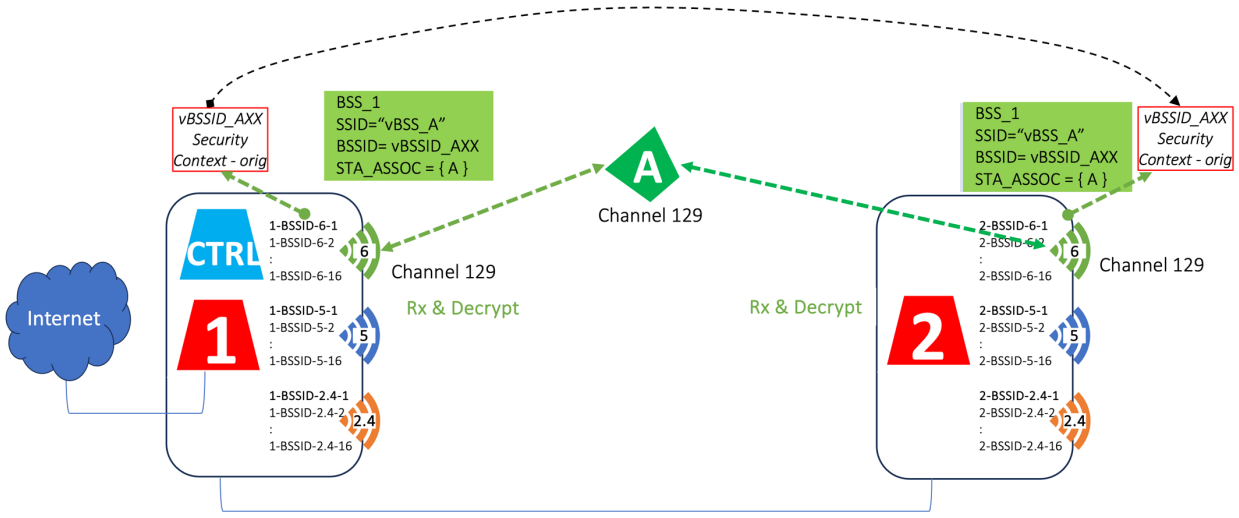


Figure 11, VBSS Transition Requires The BSS Security Context To Be Copied From The Origin AP To The Target AP

Once the VBSS has transitioned to the target AP and is confirmed to be operating, then the source AP (1) deletes the VBSS data, freeing up the AP resources for another VBSS client to use. The source AP can no longer decrypt data without the VBSS information so ceases forwarding data traffic received from the client.

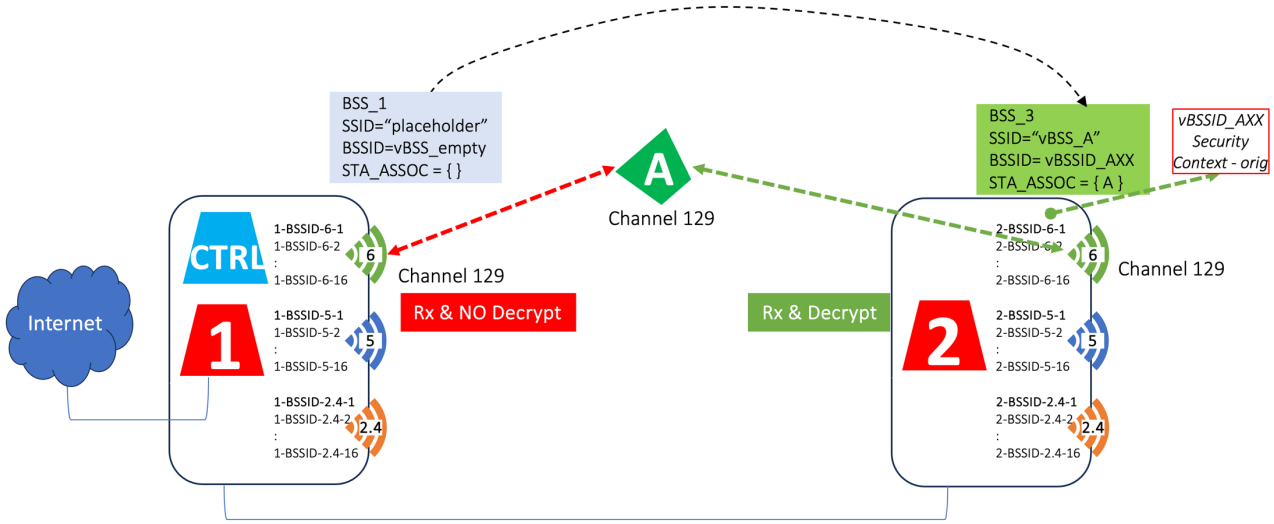


Figure 12, VBSS/Security Context Operational On The Target AP, Deleted from the Source AP

VBSS transitions related to moving a client to different channels in the same band do require some level of interaction between the current AP and the client, using a Channel Switch Announcement (CSA) message, where the Controller advises the Source AP to issue a CSA message to the client. The CSA message is normally used to advise a client that the AP is about to make a change of frequency – often in response to Dynamic Frequency Selection (DFS) when a radar event has triggered the evacuation of clients from a 5GHz channel. In the case of VBSS, because of having the same BSSID value being used on both Source and Target APs, it is possible to get the client to not only switch between different channels, but also to transparently switch between different channels on different APs. As there is a short delay in the handling of CSA messages, this has minor effect on the VBSS steering performance speed.

Unlike a standard Wi-Fi BSS that allows multiple clients to connect to an AP radio, a VBSS that moves between APs and radios based on client mobility demands can only serve a single connected client. To ensure this mode of operation a few steps are taken. Once a client is connected/associated with a VBSS, the solution stops responding to Wi-Fi probe requests from other clients. Additionally, to prevent other clients hearing about the VBSS, the solution adopts the use of unicast management and control frames (including beacons) that would typically be broadcast to all clients. By doing so, the VBSS can ensure only the intended (connected/associated) client hears the VBSS signalling.

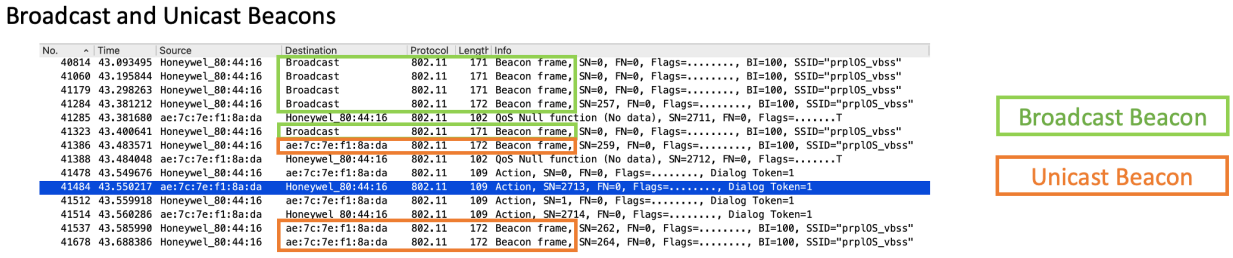


Figure 13, VBSS Transitioning From Broadcast Beacons to Unicast Beacons

4.5. VBSS Lifecycle

The life cycle of a VBSS is as follows:

1. A VBSS is created on an AP via a command from the Controller, with an assigned SSID name.
2. The VBSS initially operates using broadcast beacons and responds to all probe requests.
3. Any client can associate with the VBSS. Once associated to a client, the VBSS becomes dedicated to that client, meaning that beacons switch to being unicast and probe responses not from the connected client are suppressed.

4.6. VBSS Controller Management

As mentioned previously, to steer clients to the optimal AP/radio band, a Controller element must continually assess the quality of the Wi-Fi connectivity between the client and all other APs. This monitoring is no different to how other mesh networks work. Once the VBSS has a connected client, the Controller depends on continuous updates from all nearby AP, not just the connected AP, that are in range for the client. These updates include the RSSI value amongst other information about the client from the APs. The received data updates are evaluated by the Controller to determine the optimal AP, and if the client is not connected to it, the Controller initiates a transition not of the client, but of the VBSS/BSSID to the new/optimal AP. Care is taken to avoid repeatedly transitioning between APs with similar Wi-Fi performance, based on the use of hysteresis as well as evaluating other parameters such as latency, load, throughput, etc., of the candidate APs.

4.7. VBSS Transition Flow

Once a steering decision has been made by the Controller, then the VBSS transition is initiated via the following steps driven by the Controller:

1. Retrieves the security context from the source AP and sends it to the target AP,
2. Instructs the source AP to turn off Wi-Fi Block-ACKs on the connection,
3. Creates the VBSS on the target AP (with the client association already in place),
4. Instructs the source AP to send out a CSA pointing to the target channel/band (if the target channel/band is different than the source channel/band),
5. Deletes the VBSS on the source AP (without disconnecting the client),
6. Instructs the target AP to turn on Wi-Fi Block-ACK (if not already enabled) for the VBSS

At the end of these transition steps, the client is blissfully unaware that the VBSS is now being served from a different AP or radio, and any network activity that the client is engaged in is not interrupted. There is a small window of time between steps (3) and (5) where the VBSS is present on both APs, but in practice, that window of time is small enough to not cause any disruption. In experiments with a CableLabs VBSS implementation, this window of time was typically 5–10 msecs.

Occasionally, the source and target APs are on different channels or bands. In this case, a Channel Switch Announcement (CSA) is used to prompt the client to switch from the source channel or band to the target channel or band (this is step (4) above).

To complete the life cycle, when a client disassociates from a VBSS, the Controller instructs the AP to delete the VBSS and associated security context. Similarly, if the RSSI of the client on the connected AP goes below a useful minimum (indicating that the client cannot get usable throughput on the network), then the Controller instructs the AP to forcibly disconnect the client and delete the VBSS and associated security context. This covers the situation of devices leaving the home, where hard cutting the Wi-Fi

(again by deleting the VBSS and associated security context) means the device can cut over much quicker to the cellular network rather than persisting with an unusable Wi-Fi connecting that drives customer frustration. In normal mesh networks, where there are multiple client devices connected to the same network, having the ability to shut off the Wi-Fi network a poorly performing client is connected to is simply not possible, as ALL other clients would also be impacted, making the VBSS option more flexible.

Note that the above procedure does not need to associate a client using a fixed MAC address value; the sign-on process allows any client to sign on. In this way, Mobile Wi-Fi is robust in handling the challenge of random MAC implementations on clients. This is especially valuable because the clients using random MAC addresses (typically mobile phones, laptops, and tablets) are also those that will benefit the most from the mobility conferred by Mobile Wi-Fi.

Clients using Mobile Wi-Fi enjoy a seamless roaming experience—because the Controller controls the roaming, the user's experience is the same, regardless of which phone is being used, unlike previous efforts at Wi-Fi roaming. Furthermore, by keeping the mobile client on the best radio, the client rarely sees the need to go off channel and scan for a better AP, allowing the client to instead go into WMM (Wireless Multimedia) power save mode and save battery power. This requires no change to the client, as most clients only start scanning if their Wi-Fi experiences go bad in some way.

5. How Effective is Mobile Wi-Fi

5.1. Mobile Wi-Fi Testing Environment

The operation of Mobile Wi-Fi has been categorized by using the VBSS implementation contributed into the prpl Foundation prplMesh software component. This component implements the Wi-Fi Alliance Wi-Fi EasyMesh specifications, that includes the definition of VBSS operation. The software is integrated with prplOS and was run across several GL.inet B1300 dual band mesh routers [8] (used as a reference platform within the prpl Foundation development environment).

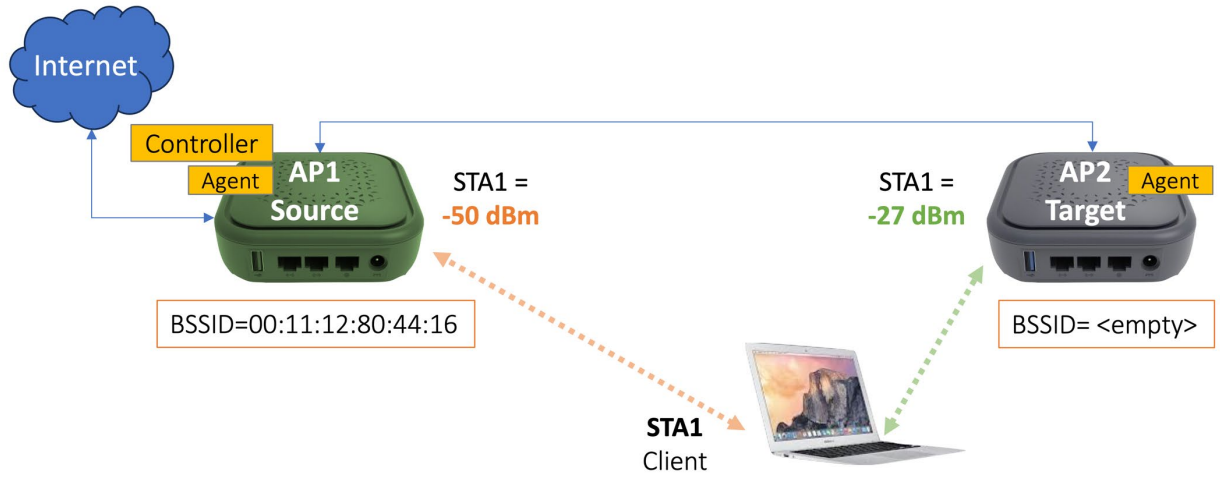


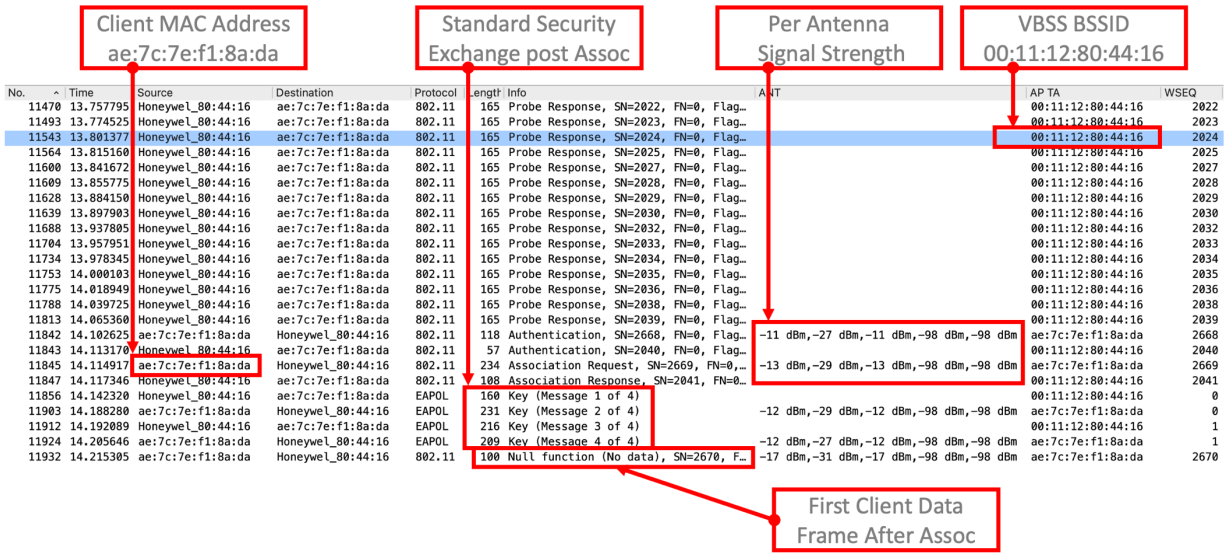
Figure 14, Main Test Network Description Using VBSS Running In prplMesh On GL.Inet B1300 Mesh Router

STA1, the client used in the testing is moved between the APs. A separate laptop in Wi-Fi monitor mode runs a continuous Wi-Fi capture that produces PCAP format files dissected over the following paragraphs. The two APs run prplOS with the prplMesh VBSS enabled software. AP1 includes the

Controller functionality (again based on Wi-Fi EasyMesh), and both APs include the prplMesh agent implementing the low level VBSS functionality as a steering mode.

5.2. Normal Wi-Fi Association

The client associates with the Source AP following normal Wi-Fi Association rules, connecting to the BSSID of the VBSS. The client notices no difference compared to connecting to any other BSS.



No.	Time	Source	Destination	Protocol	Length	Info	ANT	AP TA	WSEQ
11470	13.757795	Honeywel_80:44:16	ae:7c:7e:f1:8a:da	802.11	165	Probe Response, SN=2022, FN=0, Flag…		00:11:12:80:44:16	2022
11493	13.774525	Honeywel_80:44:16	ae:7c:7e:f1:8a:da	802.11	165	Probe Response, SN=2023, FN=0, Flag…		00:11:12:80:44:16	2023
11543	13.801377	Honeywel_80:44:16	ae:7c:7e:f1:8a:da	802.11	165	Probe Response, SN=2024, FN=0, Flag…		00:11:12:80:44:16	2024
11564	13.815160	Honeywel_80:44:16	ae:7c:7e:f1:8a:da	802.11	165	Probe Response, SN=2025, FN=0, Flag…		00:11:12:80:44:16	2025
11600	13.841672	Honeywel_80:44:16	ae:7c:7e:f1:8a:da	802.11	165	Probe Response, SN=2027, FN=0, Flag…		00:11:12:80:44:16	2027
11609	13.855775	Honeywel_80:44:16	ae:7c:7e:f1:8a:da	802.11	165	Probe Response, SN=2028, FN=0, Flag…		00:11:12:80:44:16	2028
11628	13.884150	Honeywel_80:44:16	ae:7c:7e:f1:8a:da	802.11	165	Probe Response, SN=2029, FN=0, Flag…		00:11:12:80:44:16	2029
11639	13.897903	Honeywel_80:44:16	ae:7c:7e:f1:8a:da	802.11	165	Probe Response, SN=2030, FN=0, Flag…		00:11:12:80:44:16	2030
11688	13.937805	Honeywel_80:44:16	ae:7c:7e:f1:8a:da	802.11	165	Probe Response, SN=2032, FN=0, Flag…		00:11:12:80:44:16	2032
11704	13.957951	Honeywel_80:44:16	ae:7c:7e:f1:8a:da	802.11	165	Probe Response, SN=2033, FN=0, Flag…		00:11:12:80:44:16	2033
11734	13.978345	Honeywel_80:44:16	ae:7c:7e:f1:8a:da	802.11	165	Probe Response, SN=2034, FN=0, Flag…		00:11:12:80:44:16	2034
11753	14.000103	Honeywel_80:44:16	ae:7c:7e:f1:8a:da	802.11	165	Probe Response, SN=2035, FN=0, Flag…		00:11:12:80:44:16	2035
11775	14.018949	Honeywel_80:44:16	ae:7c:7e:f1:8a:da	802.11	165	Probe Response, SN=2036, FN=0, Flag…		00:11:12:80:44:16	2036
11788	14.039725	Honeywel_80:44:16	ae:7c:7e:f1:8a:da	802.11	165	Probe Response, SN=2038, FN=0, Flag…		00:11:12:80:44:16	2038
11813	14.065360	Honeywel_80:44:16	ae:7c:7e:f1:8a:da	802.11	165	Probe Response, SN=2039, FN=0, Flag…		00:11:12:80:44:16	2039
11842	14.102625	ae:7c:7e:f1:8a:da	Honeywel_80:44:16	802.11	118	Authentication, SN=2668, FN=0, Flag…	-11 dBm,-27 dBm,-11 dBm,-98 dBm,-98 dBm	ae:7c:7e:f1:8a:da	2668
11843	14.113170	Honeywel_80:44:16	ae:7c:7e:f1:8a:da	802.11	57	Authentication, SN=2040, FN=0, Flag…		00:11:12:80:44:16	2040
11845	14.114917	ae:7c:7e:f1:8a:da	Honeywel_80:44:16	802.11	234	Association Request, SN=2669, FN=0,…	-13 dBm,-29 dBm,-13 dBm,-98 dBm,-98 dBm	ae:7c:7e:f1:8a:da	2669
11847	14.117346	Honeywel_80:44:16	ae:7c:7e:f1:8a:da	802.11	108	Association Response, SN=2041, FN=0…		00:11:12:80:44:16	2041
11856	14.142320	Honeywel_80:44:16	ae:7c:7e:f1:8a:da	EAPOL	160	Key (Message 1 of 4)		00:11:12:80:44:16	0
11903	14.188280	ae:7c:7e:f1:8a:da	Honeywel_80:44:16	EAPOL	231	Key (Message 2 of 4)	-12 dBm,-29 dBm,-12 dBm,-98 dBm,-98 dBm	ae:7c:7e:f1:8a:da	0
11912	14.192089	Honeywel_80:44:16	ae:7c:7e:f1:8a:da	EAPOL	216	Key (Message 3 of 4)		00:11:12:80:44:16	1
11924	14.205646	ae:7c:7e:f1:8a:da	Honeywel_80:44:16	EAPOL	209	Key (Message 4 of 4)	-12 dBm,-27 dBm,-12 dBm,-98 dBm,-98 dBm	ae:7c:7e:f1:8a:da	1
11932	14.215305	ae:7c:7e:f1:8a:da	Honeywel_80:44:16	802.11	100	Null function (No data), SN=2670, F…	-17 dBm,-31 dBm,-17 dBm,-98 dBm,-98 dBm	ae:7c:7e:f1:8a:da	2670

Figure 15, Standard Client Association To VBSS

The client once connected to the VBSS/BSSID will start to receive unicast rather than broadcast Beacon frames. This is done to A) prevent other clients attempting to associate with the VBSS, and B) ensure that the client continues to receive beacons for the VBSS it is associated with. The VBSS also refuses to respond to any Probe requests issued by other clients that may have received the initial broadcast beacons, making sure only one client remains associated with the VBSS.

5.3. VBSS Testing Approach

The main approach to testing involved moving a client between the different APs and having the Controller determine based on received RSSI (and other data) reports when to move the client from one AP to another AP. Thresholds can be configured for RSSI that are used to determine at what RSSI level an AP becomes a candidate for steering to, and at what RSSI level a client must experience before steering to the suitable AP. Given RSSI reports can have some variability, the use of ranges of RSSI is ideal to prevent constant steering between devices. Other controls can also be factored in to reduce the possibility of repeated/unnecessary steering.

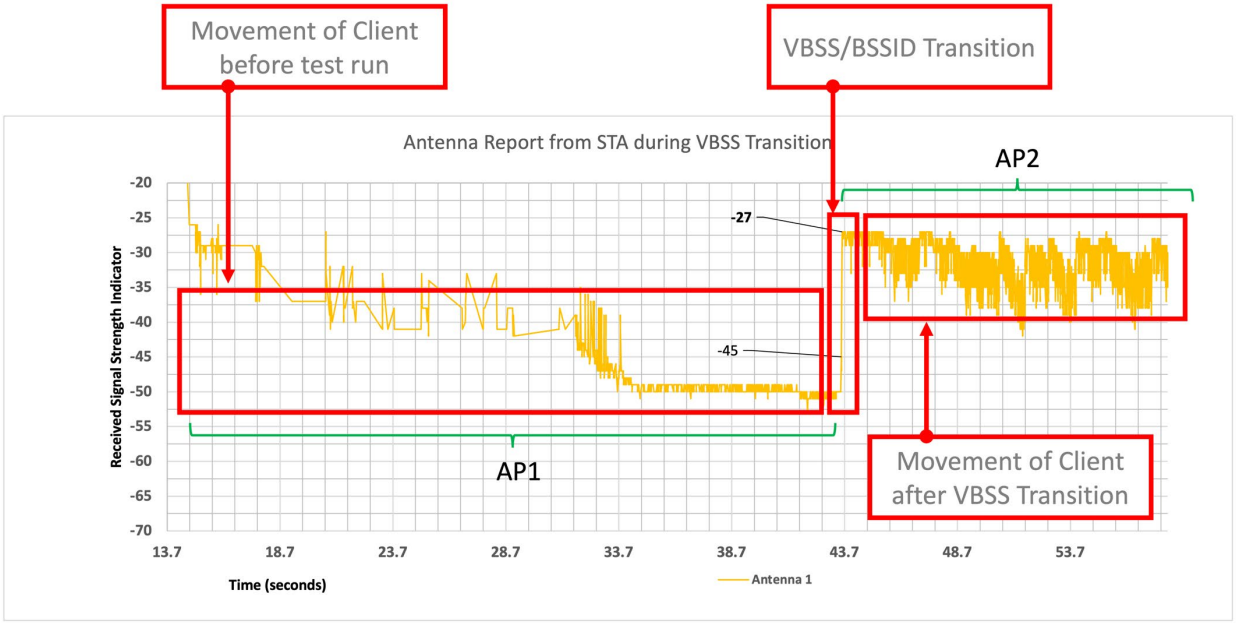


Figure 16, View Of RSSI During Test Run, Including RSSI At Time of AP Transition

5.4. Wi-Fi Alliance EasyMesh VBSS Steering Extensions

The testing relies on moving the client VBSS between the two APs, from AP1 to AP2, under the direction of the Controller, following the steering procedure defined in the EasyMesh Specification, outlined as follows. Each of these arrows represent protocol exchanges between the prplMesh Controller and the prplMesh agents that are used to coordinate the VBSS move between Source and Target APs. None of these messages interact with the client.

Please note the DELBA (Delete Block-ACK) optional step where the prplMesh agent requests the client to disable Block ACK (an optimization in Wi-Fi where multiple aggregated packets received by a client can be acknowledged back to the sender in one message rather than once for each packet). This reduces any packet acknowledgment issues during the brief interval when the VBSS can be active on both Source and Target APs.

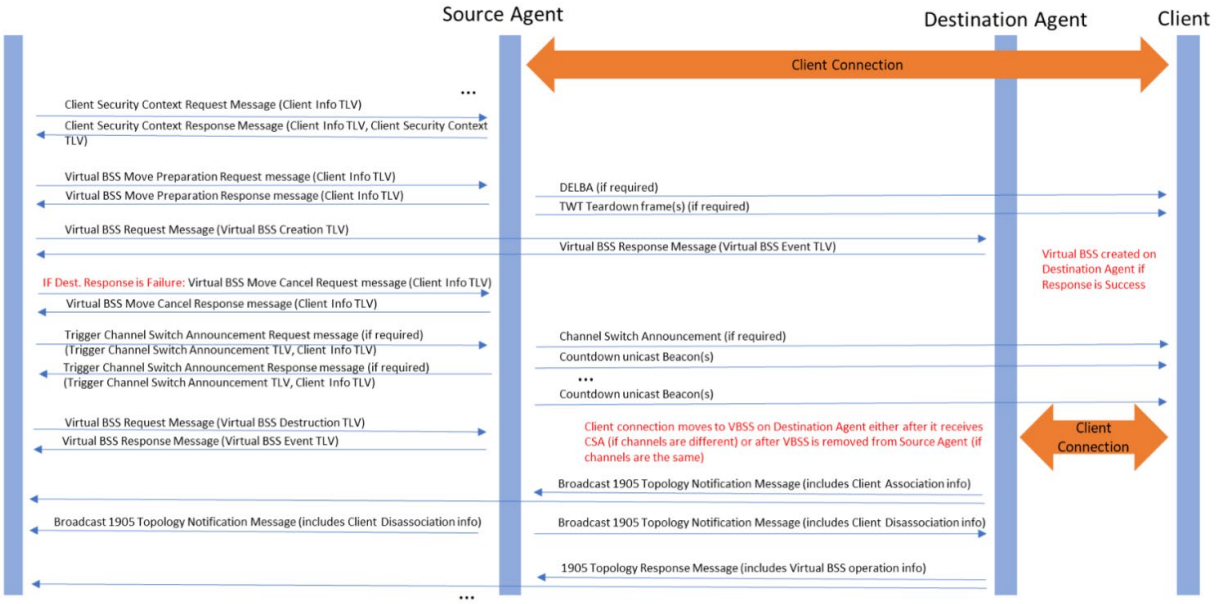


Figure 17, Wi-Fi EasyMesh VBSS Exchange To Support Steering Of VBSS between APs

5.5. Detailed VBSS Transition Analysis

The following capture taken during the VBSS transition between AP1 and AP2 shows no protocol interactions with the client, either before, during or after the transition. The BSSID that the client is connected to remains constant during the exchange. The only considerable evidence of the actual transition of the client to a new AP is the change in the reported antenna signal strength visible is the meta data collected by the wireless capture in the client. This should come as no surprise as the Controller is using RSSI to determine whether to steer a VBSS to a new AP.

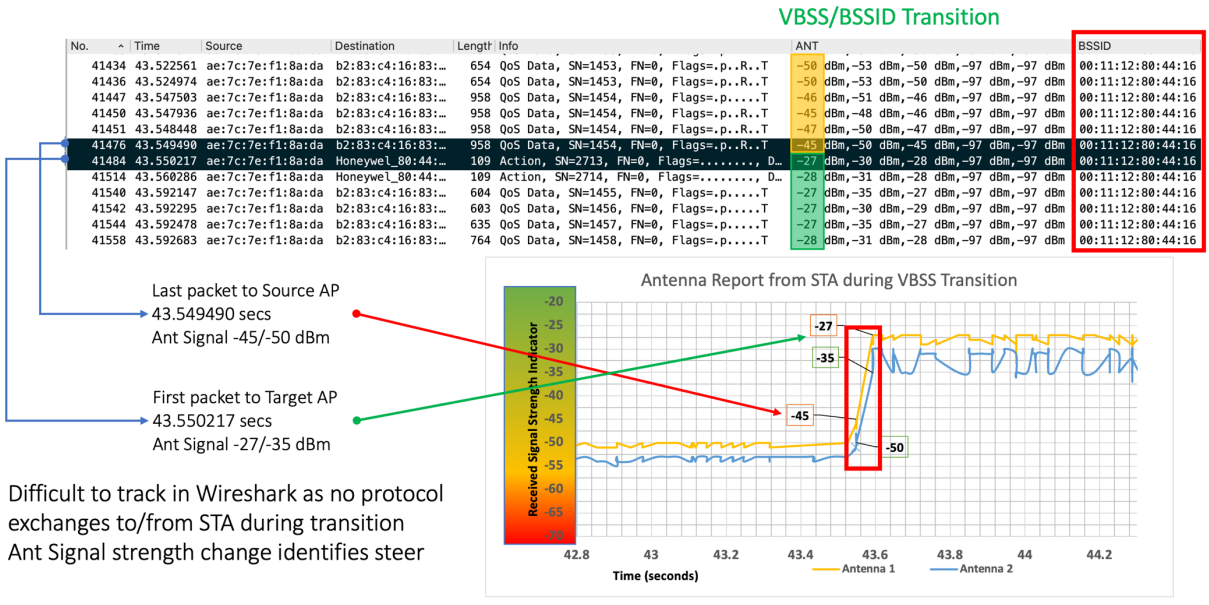


Figure 18, Transparent Move Of Client from AP1 to AP2, Including Antenna Signal Strength Detail And BSSID

Like all other meshing systems managed by a Controller, the solution continues to monitor and evaluate the connected clients and their performance with a view to ensuring optimum operation within the network.

5.6. ICMP Ping Testing Approach

In addition to detailed PCAP file analysis, a more user-friendly approach for testing the VBSS steering performance was developed by utilizing the ICMP ping utility. A device connected to the network is configured to ping the client device under test for the test. The ping rate is set at a 10msec interval, and the client continues to be pinged during the VBSS steering.

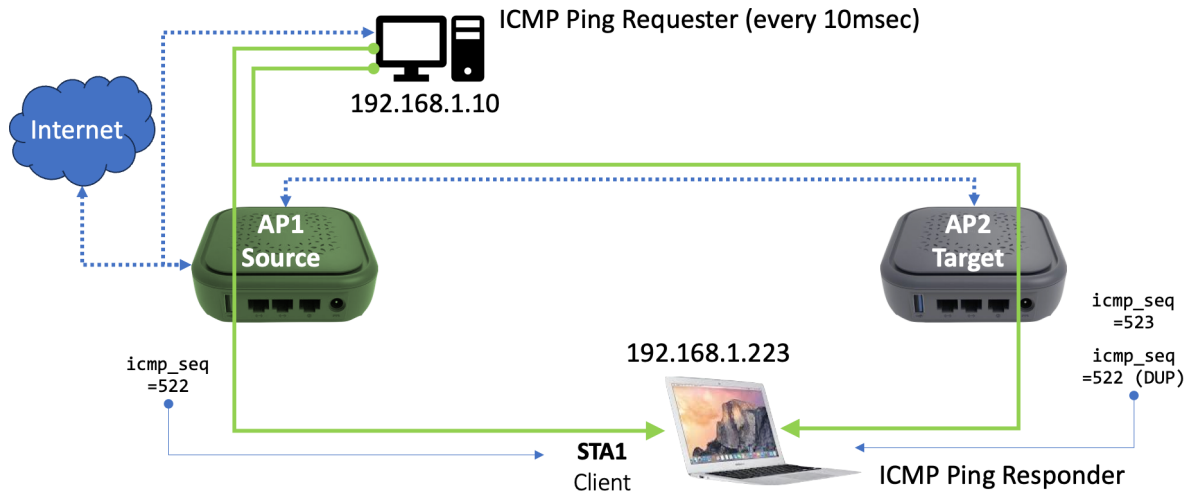


Figure 19, Simplified Test Environment To Deduce Performance Of VBSS Steering

The following is a snapshot of one test run during the VBSS transition.

Table 1 – ICMP Test Example, 192.168.1.233 Is Client Being Steered

```
64 bytes from 192.168.1.223: icmp_seq=522 ttl=64 time=6.949 ms

64 bytes from 192.168.1.223: icmp_seq=522 ttl=64 time=6.968 ms (DUP!)

64 bytes from 192.168.1.223: icmp_seq=523 ttl=64 time=6.224 ms
```

The first ICMP packet with a sequence #552 is received by the client from the source AP (AP1), while the second ICMP packet, shown as duplicate of sequence #552 is received by the client from the target AP (AP2). After the duplicate, all traffic is delivered by the Target AP to the client.

As the ping session was sending a packet every 10ms, and no packets were dropped, then it is possible to conclude a sub-10msec roaming time was achieved. Using this method makes testing VBSS a lot simpler and produces faster results for any device being submitted for testing.

6. Mobile Wi-Fi Results

6.1. Mobile Wi-Fi Steering Performance

The testing details above show the performance of the solution with a specific client being steered between two APs. The time taken between the last packet on the Source AP to the first packet on the Target AP is calculated as just under 1ms when examining the PCAP captures in fine detail. This is achieved by not involving the client in any client<>AP protocol exchanges for steering or having to have the client reassociate and run through new security context for the new Target AP (like most other steering techniques expect).

In addition to the above tests, many more tests have been conducted with a mixture of different devices. The following is a list of these devices and their steering times based on the use of the less granular ICMP ping approach:

- iPhone XS: 100% success rate, 10 msec transition times typically
- Samsung S10: 100% success rate, 10 msec transition times typically
- MacBook Pro: 100% success rate, 10 msec transition times typically
- iPad Pro 2nd gen: 100% success rate, 10 msec transition times typically
- Pad Pro 4th gen: 100% success rate, 10 msec transition times typically

These results are extremely encouraging, given they cover a range of different device types (laptops, phones, and tablets – most likely to be roaming around a home) as well as each device type having a different version of operating system. The fact that the steering transitioned within 10ms points to minimal impact on the QoE of services operating on the device. Additionally, the 100% success rate points to the possibility of using VBSS steering for trouble free steering in residential networks, as well as increasing the confidence of being able to steer many different, if not all, such roaming devices, regardless of their Wi-Fi protocol or driver and without requiring the Controller to decipher each and every client to identify what will and will not work where steering is concerned.

6.2. What has been done and what is next

CableLabs built a complete proof of concept, which shows that the technology works, that has been integrated into the prplMesh (Wi-Fi Alliance EasyMesh compatible) software component that can run on prplOS (and potential to run on RDK-B). Mobile Wi-Fi shows how it removes the need for complex interactions between a mesh network/Controller and clients, which points to a future with far simpler Controller logic to steer heterogeneous Wi-Fi clients. This is available at the GitLab site listed in the references.

These are the various accomplishments achieved by the CableLabs team during the development of the Mobile Wi-Fi/VBSS software implementation. The results of the VBSS software are very impressive given that there was no work or expectation of the client devices, and they "just worked." The ability for the Controller to continuously make handover decisions, without losing the client devices is another testament to the robustness of the solution compared to other more fragile approaches for client steering.

- Seamless handoff of unmodified Apple and Samsung phones
  - iPhone 4 and beyond, Galaxy S6/S10, iPad Pro, MacBook Pro, and beyond
  - Both major silicon variants of each generation
- Implemented on Qualcomm 802.11ac Wave 2 AP silicon
  - Minor CableLabs modifications to firmware/driver

- Have proven seamless handoffs of WPA2 (Wi Fi Protected Access 2) secure connections
    - Without handset involvement
- Handoff decisions made every second
    - With no battery impact to phone

6.3. Challenges

The current support for Mobile Wi-Fi depends on the ability to extract certain security context information from the configured BSSID entries within a Wi-Fi Access Point, and deploy these in other APs. The current implementation work has been done with Qualcomm chipsets – where it was relatively easy to extract this information to enable the solution. To extend the solution to other Wi-Fi chipsets, more work is required with Wi-Fi SoC (System on Chip) companies to ensure the same types of interfaces are available and operate similarly where extracting security details are concerned. Work is happening in this space.

The current setup of most Wi-Fi chipsets is that they support up to 16 BSSIDs per radio. Since many devices in the home are NOT constantly moving around, this limitation of 16 is not a dealbreaker. These BSSIDs are created to scale to 100+ devices, each with their own independent set of security contexts. A VBSS BSSID is scaled to 1x device. There exists the potential in some Wi-Fi SoC to modify their internal architecture/organization of BSSIDs to accommodate more lightweight (e.g.,1x device) options, with a view to increasing to many more than 16x BSSIDs per radio.

One perceived challenge to the VBSS solution is the concern about an explosion in beacon related traffic if there are multiple BSSIDs in operation. The main drawback with beacon traffic is that it is normally broadcast at the lowest common PHY rate between connected devices, as well as requiring in most cases beacons being broadcast every 100ms. Additionally, clients tend to probe any broadcasted SSIDs they have a profile for, driving up more traffic. Under normal conditions, this would drive up the % of bandwidth capacity consumed to send beacons, however given that VBSS operation results in the use of unicast beacons to the single device connected to the BSS, then this broadcast overhead disappears, and without the beacon being sent to all devices, then only the connected device will probe the BSS.

6.4. Mobile Wi-Fi Opportunities Beyond Residential

As has been outlined, steering Wi-Fi devices around a Wi-Fi network is a major challenge, whether this is in a residential setting or beyond. A big challenge with pushing Wi-Fi into larger deployments has always been steering of clients, and the reliability and complexity of ensuring this happens flawlessly. Using Mobile Wi-Fi/VBSS enables many different applications previously thought too difficult to operate, including deployment in the MDU (multi dwelling units) or Enterprise space and consideration for Metropolitan Wi-Fi.

With devices constantly moving, be they within a building or outside in the open where they may travel at different speeds, the typical issue with Wi-Fi steering was the time to complete the steer. This paper points to some examples of 145/200ms for distinct types of BTM steering. Other steering options also exist. Such lengthy delays simply rule Wi-Fi out of the running for many different use-cases that are filled by cellular devices. Mobile Wi-Fi/VBSS, with its much shorter steering times, presents the opportunity to re-engage with Wi-Fi for several use-cases previously ruled out.

Beyond the residential setting described in this paper, Mobile Wi-Fi may also have utility in enterprise, MDU and Metropolitan Wi-Fi. Having a solution that is client device agnostic really helps when dealing

with such a large mix of device types encountered in these settings. There is the potential for Mobile Wi-Fi to provide truly seamless mobility in the case of Wi-Fi mobility.

In addition to enabling better roaming of clients in a residential setting, efforts are underway, driven by CableLabs to seek adoption of the Mobile Wi-Fi approach within the IEEE 802.11 standard. Several other companies are also interested in the concept of a VBSS within the next version of Wi-Fi [9] [10] [11].

The following is a timeline of the key milestones of the Mobile Wi-Fi project.

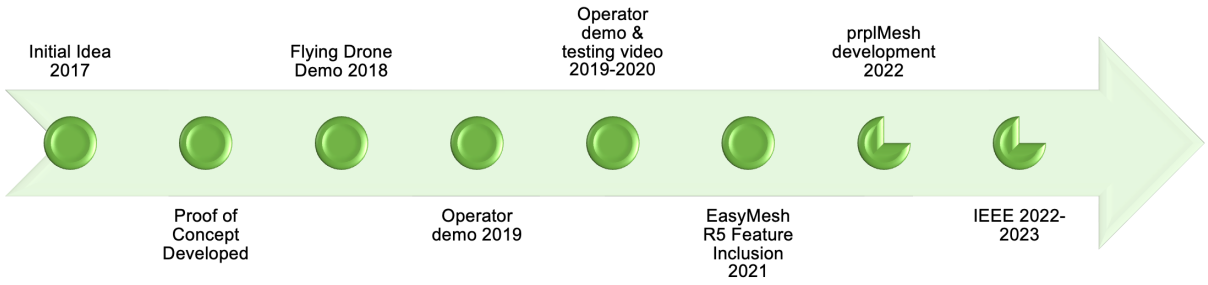


Figure 20, Mobile Wi-Fi Key Milestones

7. Conclusion

Mobile Wi-Fi/VBSS steering technology significantly enhances the reliability of Wi-Fi steering in mesh networks, while also delivering incredibly fast steering of clients between different APs ensuring maximum performance within the limit of available APs to the client. The solution is extremely robust, requiring no specific protocols, or software running on the client, making it transferrable to any Wi-Fi client. Mobile Wi-Fi has a positive impact on QoE, ensuring that the most mobile devices within a home network remain connected and deliver their services with minimal degradation The ability to deal with handover at the edge of Wi-Fi performance is also a key feature of Mobile Wi-Fi that enhances overall QoE.

Mobile Wi-Fi is in its infancy, and while it has achieved a lot in terms of a portable reference software implementation, a standalone reference demo (using a B1300 device) and impressive test results, more work is required to get Mobile Wi-Fi in front of operators, equipment manufacturers, and standards bodies for it to really get the momentum needed for it to become the de-facto approach for Wi-Fi device steering in all sorts of different applications.

Abbreviations

AP	Access Point
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
BTM	BSS Transition Management
CSA	Channel Switch Announcement
CTRL	Controller
DBC	Dual Band Concurrent
FT	Fast Transition
GHz	Gigahertz
GTK	Group Temporal Key
ICMP	Internet Control Message Protocol
IEEE	Institute Of Electrical and Electronic Engineers
IoT	Internet of Things
IT	Information Technology
LAN	Local Area Network
MCS	Modulation and Coding Scheme
MAC	Media Access Control
MDU	Multi Dwelling Unit
MHz	Megahertz
MIMO	Multi-Input, Multi-Output
OS	Operating System
PCAP	Packet Capture
PHY	Physical layer
PTK	Pairwise Transient Key
QBC	Quad Band Concurrent
QoE	Quality of Experience
QoS	Quality of Service
RCPI	Received Channel Power Indicator
RF	Radio Frequency
RSSI	Received Signal Strength Indicator
SCTE	Society of Cable Telecommunications Engineers
SNR	Signal To Noise Ratio
SS	Spatial Streams
SSID	Service Set Identifier
STA	Wi-Fi station
TBC	Tri Band Concurrent
VBSS	Virtual Basic Service Set
VR	Virtual Reality

WFA	Wi-Fi Alliance
WLAN	Wi-Fi LAN
WPA	Wi-Fi Protected Access
SCTE	Society of Cable Telecommunications Engineers

Bibliography & References

[1] Wi-Fi Alliance EasyMesh Release 5 Specification - https://www.wi-fi.org/system/files/Wi-Fi_EasyMesh_Specification_v5.0.pdf
[2] Download location for future Wi-Fi Alliance EasyMesh Specifications - https://www.wi-fi.org/file/wi-fi-easymesh-specification
[3] Wi-5 Project - https://github.com/Wi5/odin-wi5/wiki
[4] Programming the Enterprise WLAN: An SDN Approach - https://lalithsuresh.files.wordpress.com/2011/04/lalith-thesis.pdf
[5] Programmatic Orchestration of Wi-Fi Networks Video Overview - https://youtu.be/m8CEGuQSKQk
[6] Programmatic Orchestration of Wi-Fi Networks paper - https://www.usenix.org/system/files/conference/atc14/atc14-paper-schulz_zander.pdf
[7] Current release of VBSS incorporated into prplMesh - https://gitlab.com/prpl-foundation/prplmesh/prplMesh/-/tree/dev/vbss-integration-demo-staging?ref_type=heads
[8] GL.inet B1300 target hardware used for VBSS implementation - https://www.gl-inet.com/products/gl-b1300/
[9] Nokia Nov-2020 IEEE contribution on VBSS (https://mentor.ieee.org/802.11/dcn/20/11-20-1247-01-00be-virtual-bss-for-multi-ap-coordination.pptx)
[10] Samsung July-2019 IEEE contribution on VBSS (https://mentor.ieee.org/802.11/dcn/19/11-19-1019-00-00be-virtual-bss-for-multi-ap-coordination.pptx)
[11] Huawei Nov-2019 IEEE contribution on VBSS (https://mentor.ieee.org/802.11/dcn/19/11-19-1972-00-00be-operation-of-virtual-bss-architecture-for-multi-ap-coordination.pptx)

