Issues arising from use of multiple BBSIDs on wireless APs

Introduction

Almost all modern wireless Access Points (APs) can belong to multiple wireless networks (Extended Service Sets) simultaneously and advertise a number of a different Service Set Identifiers (SSIDs) within beacon frames. This is commonly used to provide various different networks in a particular area, so giving access to different resources and presenting services which may have differing management or security policies applied. This allows various categories of user, e.g. staff, students or visitors etc. to be provided with network services which are appropriate to them.

In the past, in order to present a multiple network palette to the Wi-Fi user, a number of separate APs would have been needed since each AP was only capable of managing a single Basic Service Set Identifier (BSSID) transmitted in the various wireless network frames in use within its Basic Service Set (the AP and its associated stations). Nowadays, APs can manage multiple BSSIDs, so support for multiple networks can be achieved through the use of different Basic Service Set Identifiers in the single Basic Service Set.

This document describes the implications of adopting this approach and the problems that may arise. An alternative to multiple SSID-based provision of networks is described that uses 802.1X and VLANs.

Benefits of Multiple BSSID Approach

The use of multiple BSSIDs in the same AP has its benefits. For instance, if separate APs are used at locations for every SSID, the APs will each try to find an unused channel. Where there are a significant number of APs in the same area, avoiding channel interference will be problematic. By deploying a single AP which is utilising multiple BBSIDs, the same channel can be used for all BSSIDs, thereby avoiding the channel interference problem.

Problems Arising

There are two ways of implementing multiple network environments built on multiple SSIDs. The basic method is to use a single BSSID and for a single beacon to advertise all the SSIDs available. This however is incompatible with many 802.11 clients and does not support different SSID capability sets.

The second and most common method, which is best-practice industry standard, is to use multiple BSSIDs. With this method only one SSID is advertised within each beacon frame and therefore multiple beacons are used to advertise all the SSIDs. This method has the highest client compatibility and allows each SSID to have different sets of capability. Several technical issues however arise from such configuration: the two main ones covered in this document are the loss of data throughput due to management traffic, and reduced battery lifetime of clients. This document also covers the interesting side-effect of client-speed and data throughput.

Reduced data throughput

With the multiple BSSIDs and beacons method, the AP behaves like a number of discrete physical APs at the L1/L2 level. Each BSSID will appear to the client as if it is associated with a separate AP. The effect of this is that the management traffic related to each BSSID, which is normally transmitted by individual APs, has now to be actually transmitted by the same AP. An AP that is advertising four SSIDs would be transmitting four streams of management traffic. The real physical layer (PHY) of such an AP stays the same, independent of the number of BSSIDs that are being used – i.e. an 802.11g AP has 54Mbit of bandwidth and this doesn’t change. This means that as you add more BSSIDs, the management traffic eats into the data bandwidth available.

This can be stated as an equation, where:

BW = bandwidth available (e.g. 54Mbit on 802.11g)
MGMT = Bandwidth required for management per BSSID
NOB = Number of BSSIDs being transmitted
UTB = User traffic bandwidth

UTB = BW - (MGMT * NOB)

From this simple equation it can be seen that the available bandwidth for the user decreases as the number of BSSIDs increases.

Measurements show that in a typical lecture theatre scenario, where 3 APs are supporting 100 clients (laptops and/or smartphones) and use 12 BSSIDs, 35% of traffic will be management frames. It should be remembered that beacons from APs and client probe requests/responses are all transmitted at 1Mbit/s as per the 802.11b/g standards. Reducing the number of BSSIDs in use has a dramatic effect - the same environment would have less than 10% management traffic if the number of BSSIDs were 3 [1].

These effects are even more noticeable when the client is in a real-world campus environment where there are APs on multiple floor levels. In such an environment, the client will pick up other APs on the same channel. Typically this could be between 4 and 6 APs resulting in 55% of bandwidth being lost to management frames.

There are ways of reducing this impact. For example, by increasing the minimum bandwidth to e.g. 12Mbit/s, the bandwidth usage of management traffic can be more than halved. If wireless network equipment cannot be configured to exclude 802.11b clients, this method is also the best practice way of preventing old legacy 802.11b clients from operating and degrading the performance of the Wi-Fi environment,.

Multiple BSSID and battery life

A Wi-Fi client uses power whenever it has to deal with a wireless frame that comes its way.

Power consumption is especially important in respect of mobile clients: smartphones, laptops in lecture theatres with no power provision and VoIP handsets as they all rely on batteries for operation. Most Wi-Fi vendors recognise this and utilise 802.11 standards such as WMM-PS or U-APSD to reduce battery drain of clients which are idle. According to the Wi-Fi Alliance these technologies can save between 15%–40% of battery power consumption.

Beacon frames are an important part of 802.11 – they let the client know that an SSID is available and a client using Wi-Fi will be looking out for such frames. Note that beacon and probe response frames not only notify clients about the presence of an AP but also carry important information such as the SSID, the BSSID, the mode (Infrastructure or Ad-Hoc), Protection security scheme (e.g. Open, WEP, WPA-PSK or 802.1X), support transmission rates, channel in operation and optional Information Elements. For example: variable length fields that mainly contain vendor or country specific information such as 802.11d or 802.11e.[2]

As was discussed above, if you employ multiple BSSIDs then multiple beacons are transmitted, one for each active BSSID, with the result that clients have to deal with beacon frames more frequently. This can be reduced by for example setting the beacon interval to be less frequent, but this may cause some clients not to detect the beacon when scanning, so leading the client to decide a particular SSID is not available.
Likewise, setting the DTIM (Delivery Traffic Indicator Message) period on the AP to a higher value will reduce how often clients are woken up to receive pending multicast/unicast packets but this will reduce throughput and, more importantly, since multicast packets are buffered, a large DTIM can cause a buffer overflow.

Note that some AP implementations may have client battery issues where an SSID is linked to multiple VLANs if the AP still sends the client traffic on that BSSID from VLANs onto which it is not bridged. Such traffic is invalid for the client and the client will see decryption errors. Having to handle such invalid traffic addressed to it will also waste battery power.[3] It should be ensured with the vendor that the single BSSID with VLAN override works in a client friendly way.

References

[1] https://airheads.arubanetworks.com/article/aruba-radio-corner-impact-mul... [1]

[2] http://chris.berger.cx/publis/2009-AICT-wifi-paris.pdf [2]

[3] http://www.patentstorm.us/patents/7339915/description.html [3]

[4] http://www.stanford.edu/~seethara/papers/wintech09.pdf [4]

Source URL: https://community-stg.jisc.ac.uk/library/janet-services-documentation/issues-arising-use-multiple-bbsids-wireless-aps

Links
[1] https://airheads.arubanetworks.com/article/aruba-radio-corner-impact-multiple-ssids
[2] http://chris.berger.cx/publis/2009-AICT-wifi-paris.pdf
[3] http://www.patentstorm.us/patents/7339915/description.html
[4] http://www.stanford.edu/~seethara/papers/wintech09.pdf