ARUBA™
The Mobile Edge Company

Virtual Access Points

Performance Impacts in an 802.11 environment and Alternative Solutions to overcome the problems

By

Thenu Kittappa
Engineer

Abstract

This paper primarily discusses the effects of Virtual Access Points (VAPs) on 802.11 networks. Deployment scenarios that best benefit from the use of virtual APs and design recommendations for such deployments are also discussed in the document.

WiFi devices like laptops, PDAs, WiFi-phones differ in their ability to support different encryption and authentication methods. Based on the capabilities and functionality of a device, the WLAN system should be capable granting network access rights to the device.

When multiple encryption types have to be supported, an AP can be configured to support all required WiFi encryption methods. This however is not recommended. A network deployment using a single AP for weak and strong encryption methods is liable to security attacks and can compromise the integrity of the wired network.

The alternative is to use VAPs to address the problem. VAPs are logical AP instances on the same physical access point that cater to the unique requirements of various user groups and encryption types. Based on how the VAPs are used to solve the problem, the resulting solution could be secure and stable or one that requires high bandwidth for the 802.11 management traffic alone.

This document discusses the effects of multiple VAPs on the bandwidth of a WLAN network and makes recommendations for optimal deployments.

Virtual Access Points

Introduction

A Virtual AP is a logical entity that resides within a physical Access Point (AP). To a client, the VAP appears as an independent access point with its own unique SSID.

There are multiple approaches to implementing virtual APs.
One of the implementation uses a single BSSID and advertises all the SSIDs supported by the system on the same beacon. Some of the issues with this approach are

- Incompatible with most 802.11 clients deployed.
- Does not support different capability sets for each SSID

The de-facto industry standard is to use multiple BSSIDs. Only one SSID is advertised per beacon and multiple beacons are used to advertise the SSIDs corresponding to the virtual APs configured. This solution is compatible with most 802.11 clients and also allows the SSIDs to support different capability sets. This solution however results in an increase in management traffic. The remainder of this document discusses the later solution. The term Virtual AP is used synonymously with BSSID throughout this document.

Effects of Virtual Access Points on the available throughput

Every VAP appears as an independent AP to the client. The VAPs emulate the operations of a physical AP at the MAC level. All wireless management traffic that would be transmitted by one physical AP would also be transmitted by the VAP. For example, a physical AP can broadcast 3 SSIDs (using virtual APs). This AP would also transmit the management traffic of 3 independent APs, one for each VAP it supports.
The actual bandwidth supported by an 802.11 AP is constant (11 Mbps for 802.11b, 54 Mbps for 802.11g and 54 Mbps for 802.11a) independent of the number of the VAPs. Since the bandwidth available per 802.11 channel is fixed and the bandwidth required for management traffic requirement is on a per Virtual AP basis, definition of multiple VAPs results in a proportional decrease in the data bandwidth. This is further explained using the example below

```
Net = Net bandwidth available on an AP (11 Mbps for a 802.11b AP and 54
Mbps for a 802.11a AP)
Mgmt = Net bandwidth required per AP per SSID (per virtual AP)
VAP = Number of virtual APs configured
Data = Net data throughput available for data traffic
Data = Net – (Mgmt * VAP)
```

As can be seen, the data bandwidth decreases as the number of VAPs configured increases. Large number of VAP definitions can result is very low data throughputs especially in an 80.211b/g environment and in extreme cases can result in on the air traffic congestion.

NOTE: The throughput of an 802.11 cell is not only affected by the traffic to and from the APs and stations in the WLAN but also neighboring APs and stations whose transmit coverage area includes the 802.11 cell in question.

The effects of virtual APs on the WLAN network largely depends on the 802.11 band used. This is attributed to the coverage area and the channels supported by the 802.11 b/g versus the 802.11 a band. 802.11 a has a large number of channels to choose form and the coverage area is smaller (100 feet as compared to 250-300 feet for b/g). Smaller cell sizes and larger number of channels results in lower chances of having neighboring cells of the same channel whose traffic can result in interference in any given area. As a result with the 802.11 a band, the effect of management traffic on the overall throughput is minimal when multiple VAPs are defined as compared to the b/g band.

1. Effects of virtual APs on 802.11 b/g deployments

Consider the following 802.11b/g deployment scenario. The maximum number of non-overlapping channels available are 3 - channels 1, 6, 11. An ideal deployment for data capacity recommends placing APs at a distance of 30 - 45 feet from each other. In such a deployment, any 802.11 b/g client can hear at least 3 APs on the same channel

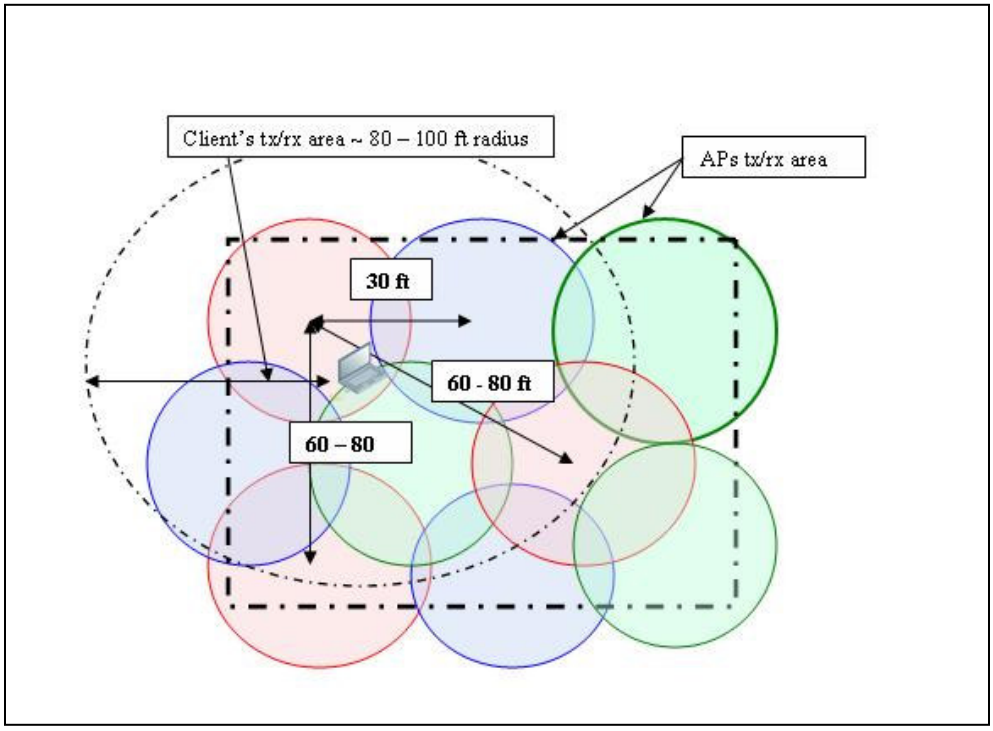

Figure 1.1: 802.11b/g AP deployment in a given coverage area. Channels used are 1,6,11 (color coded).

This is because the coverage area for an 802.11b/g environment is about 300 feet at maximum power, the 802.11b/g client's or AP's packets can be heard over 300 feet at lower traffic rates. In addition most clients also transmit at the highest tx-power levels resulting in large coverage areas.

In deployments of this size, there could be anywhere from 10 to 100 802.11b clients. The following graph is based on the bandwidth calculations for the 802.11 management traffic for different number of stations and different numbers of virtual APs (per physical AP) when there are at least 3 APs in the receive range of each client. These calculations are based on beacon, probe request and probe response traffic alone. (Refer to the calculations in Appendix A).

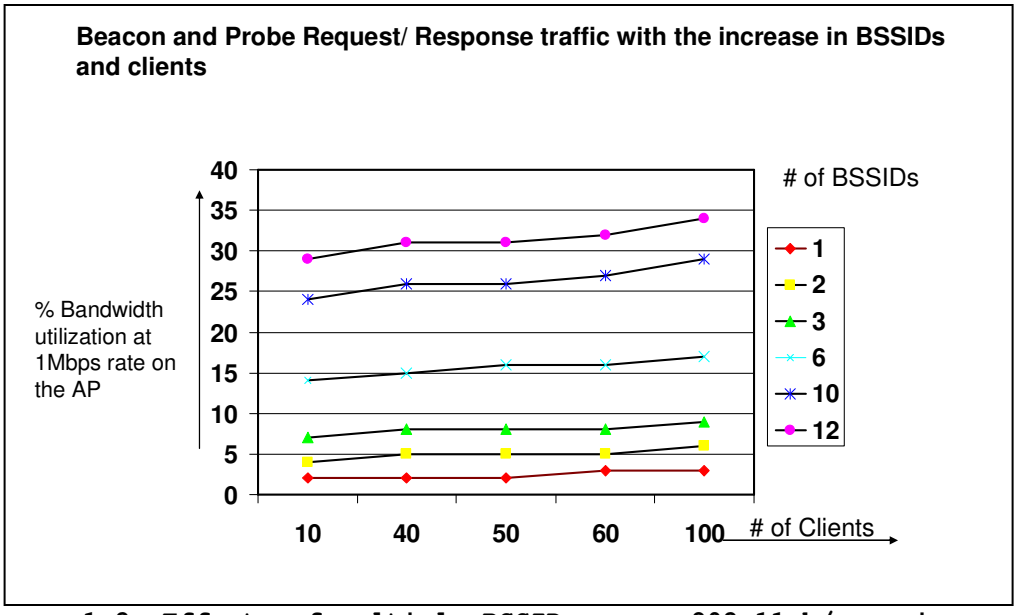

Figure 1.2: Effects of multiple BSSIDs on an 802.11 b/g environment

From the graph, with 12 virtual APs (BSSIDs), 100 clients in a given coverage area and with 3 APs on the same channel, the management traffic is almost 35% of the overall traffic at a data rate a 1 Mbps. This is because beacons, probe requests and probe responses are transmitted at 1Mbps data rate as per the 802.11b/g standards.
The bandwidth utilization for management traffic however is still well below 10% when the number of SSIDs is less than or equal to 3.

The effects are more pronounced in real world deployments with multiple floors and signals from neighboring offices bleeding into the coverage area. A client would now hear other APs on the same channel from neighboring WLAN deployments apart from the APs on its own valid WLAN network. As a result the client would hear 4 – 6 APs at any time. The bandwidth utilization for control traffic shoots up to 55% for 12 SSIDs at a data rate of 1Mbps assuming that there are at least 6 APs in the RF vicinity of each client.

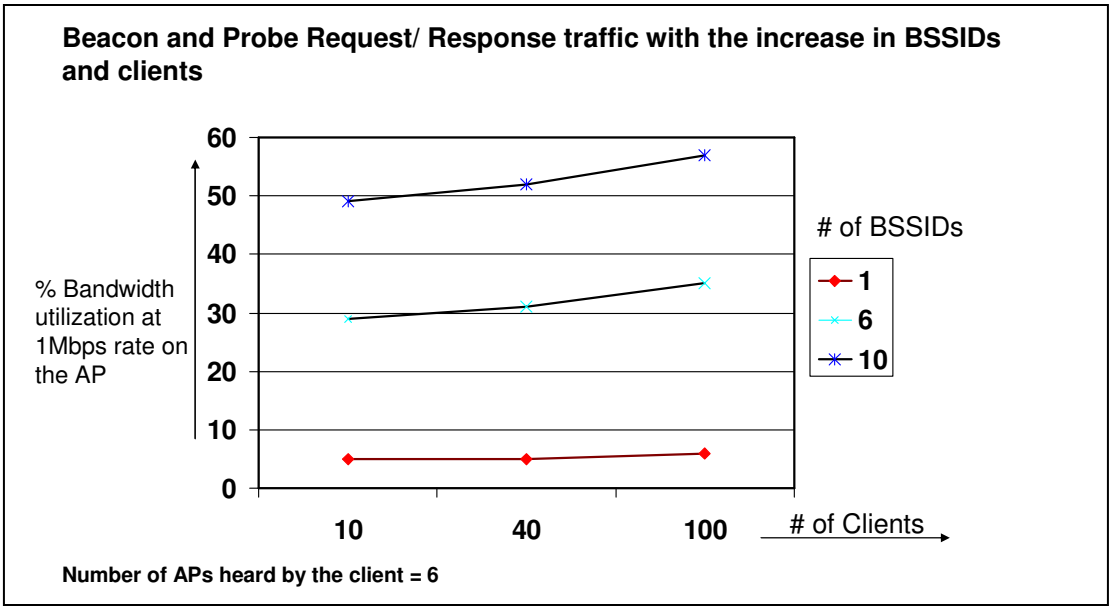

Figure 1.3: The graph shows the effects of multiple virtual AP declarations (1,6,10) on 802.11 b/g channel throughput with the

2. Effects of virtual APs on an 802.11a network

From the previous section it can be seen that multiple BSSIDs have a pronounced effect on an 802.11b/g network. This is largely attributed to the facts that the 802.11b/g band offers limited non-overlapping RF and channel coverage area for an 802.11b/g band is large (around 300 feet). The same problems also affect the 802.11a network but the effects are less pronounced because the

- 802.11a band offers a larger number of overlapping channels to choose from allowing the neighboring APs to be on distinct channels. This greatly reduces the number of APs that can be heard by a client.
- Coverage area for the 802.11a band is smaller which also helps alleviate the pains of a multi-ssid deployment. Since the client's RF range is smaller, the client will not be able to listen to the APs that are further away which it would have otherwise heard if the band used was the 802.11 b/g band. Example:

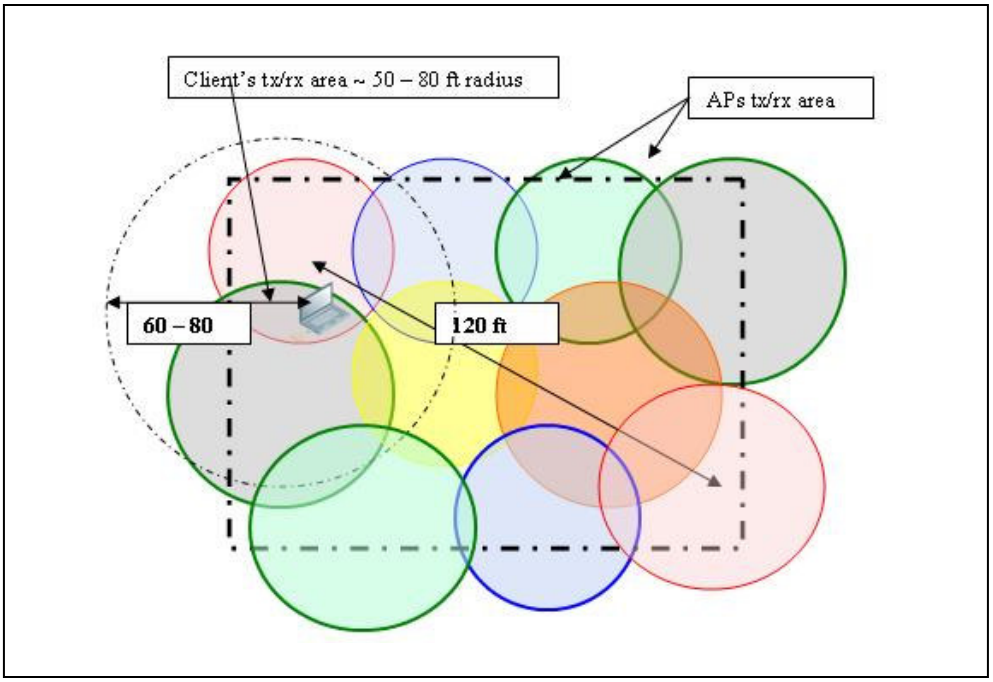

Figure 2.1: 802.11a AP deployment. Note that for the same coverage area (shown in Figure 1) an 802.11a deployment can accommodate more APs on different channels than 802.11b/g greatly reducing the possibilities of the traffic from cells on the same channel bleeding over.

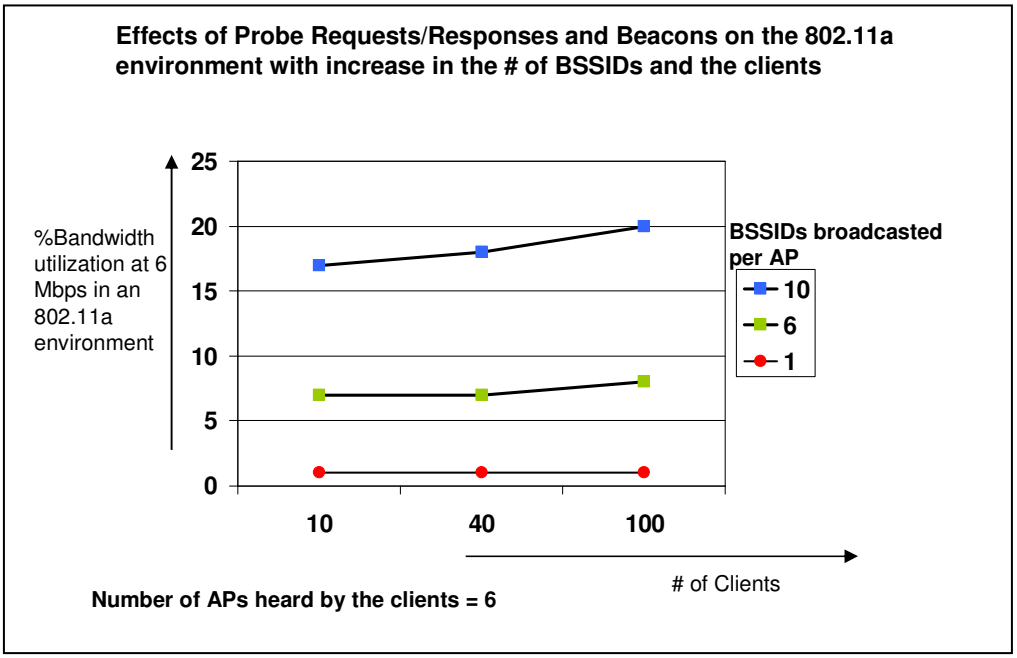

Figure 2.1: Effects of multiple virtual AP declarations on the 802.11a throughput for different number of clients in the APs range.

When to use Virtual Access Points (VAPs)

A single SSID is sufficient to provide basic connectivity. A WLAN deployment however is seldom basic and simple. The WLAN deployments are required to support different types of devices from multiple vendors.

- The devices support different authentication and encryption methods. Depending on the level of encryption supported the devices have to be access-restricted to protect the integrity of the network and other wireless users.
- Different devices have different network access requirements. A WiFi phone needs limited access to the call servers and other phones whereas for a data device like a laptop the access required depends on the access privileges of the host using the system. The network access needs to be restricted to prevent excess access privileges.

Solutions

Two possible solutions that address these requirements are discussed below. While both solutions use VAPs to address the requirements of a heterogeneous network, the methodology used largely influences the security aspect of the solution and the number of VAPs defined.

Solution 1. Solution 1: Using a unique VAP for each device class and user class. In this case a unique VAP and SSID are defined for each encryption method and for each user class based on access privileges. Each of these SSIDs could optionally map to a unique VLAN on the wired network to restrict network access based on VLANs. The inherent problems with this solution is that

- It requires the definition of too many VAPs and VLANs
- Each VAP definition increases the management traffic eventually choking the WLAN with management traffic
- Security is now enforced based on the VAP association and not the identity of the user accessing the network.

Solution 2. Using VAPs for basic service separation and using firewalls to further segregate the users based on their access-privileges.
The advantage of this solution is two fold. It restricts the number of VAPs defined to a bare minimum. Since the access privileges are now based on the user/device identity and is firewall based, the network is secured from malicious attacks. This solution however requires the firewall capabilities to be integrated with the WLAN system.

Example:

Network Requirements:

- Support for visitors with no encryption enforced. These users would have no access to the intranet and will be able to access the internet alone.
- Voice handsets that support only WEP encryption and require specific RF settings
- Employee access with dynamic key exchange (WPA, WPA-2), advanced authentication like 802.1x, VPN and access based on their department – Sales, Marketing, Engineering, Administration

Solution 1

SSID	Encryption	Description
Guest	Open (No encryption)	Guest users can access the internet and have no access to the intranet. This SSID is required

		since it is not recommended to use the same SSID for encrypted and non-encrypted users
Voice	WEP shared keys	Voice needs limited access to the network (access to call servers only). They need to be on a different SSID since they have different DTIM requirements
Sales Marketing Engineering Administration	WPA, WPA2 dynamic keys and using advanced auth methods like 802.11i, 802.1x, VPN	Access to the network limited based on the SSID the user associates to.

Solution 2

SSID	Encryption	Description
Guest	Open (No encryption)	Guest users can access the internet and have no access to the intranet. This SSID is required since it is not recommended to use the same SSID for encrypted and non-encrypted users
Voice	WEP shared keys	Voice needs limited access to the network (access to call servers only). They need to be on a different SSID since they have different DTIM requirements
Employee	WPA, WPA2 dynamic keys and using advanced auth methods like 802.11i, 802.1x, VPN	Access to the network is limited by the authentication profile and not by the SSID

Analysis of the Solutions

The difference between the two solutions might seem minimal but from the previous analysis Solution 1 can consume significantly higher bandwidth than Solution 2. Solution 1 requires the definition of multiple additional SSIDs on the network which results in an increase in the wireless management traffic and a decrease in the actual data throughput on the network. Additionally SSIDs are used for user classification and access rights policing. Thus users are assigned access rights not by their identities but by their SSID association which could give a malicious spoofer privileged access into the network. The solution requires Employee A in the sales department to associate with the “Sales” SSID for the right network access privileges. Associating with the “Employee” SSID could result in Employee A gaining access to a privileged set of servers not accessible to the Sales user group. This is because the rights are assigned by the SSID and not Employee A’s identity or authentication profile.

Solution 2 is the Aruba recommended solution. In this case the virtual APs are defined for basic service separation based on the radio configuration. User differentiation and access privileges are

granted based on the individual user's identity and authentication profile. Limiting the number of SSIDs has a direct bearing on the APs bandwidth as the wireless management traffic is kept in check. Also this solution improves security as privileges are granted based on the user's identity. Employee A from the Engineering department and Employee B from the Sales department would both associate with the *Employee* SSID but the Aruba system would assign different the access privileges based on the user's identity and authentication profile. This ensures that the user will always be assigned the right access permissions depending on the user's identity.
When users associate with an SSID supported a weak encryption, the rights of the users could be further limited to a subset of their actual rights to protect the integrity of the network.

Conclusion

Virtual APs address some of the basic wireless design requirements successfully only when used judiciously. The Virtual APs should be defined for basic service separation based on the radio configuration and not for user classification and access policing. Advanced and more secure methods like firewalls definitions should be used to ensure that user groups are assigned the right access policies depending on their encryptions and/or authentication methods. Employee / student access based on department or categories should be differentiated using firewall policies, which is more scalable and secure. Virtual APs should not be used to enforce security.

In scenarios where multiple virtual APs have to be define like hosted services, hot spots, air ports, hospitality services where the same WLAN network is used by multiple vendors, the 802.11a band should be used as the effects VAP definitions and the effects of AP management traffic on the data throughput is less when compared to a 802.11b/g network.

Judicious use of virtual APs helps improve and secure the connection on the wireless side by the encryption method with acceptable bandwidth loss. In conclusion, Virtual Access Points should not be used as the means to secure the network or classify users by their access rights but should be used to group users by their basic service sets and RF requirements.

Appendix A: Calculations

This section explains the process for computing the data used in this document.

Management Traffic Type

All calculations are based on the traffic generated by the clients and the APs in terms of probe requests, probe responses and beacons.

Client behavior model

On an average a normal WLAN client sends 2 probe requests per minute per channel. One of these is a broadcast with SSID set to the broadcast EESID and the other packet is sent with the ESSID set to the required SSID. The later is a broadcast but only the APs/Virtual APs with the corresponding SSID would respond.
The assumption made is that the client is pre-configured SSID as would be the case in an enterprise network.

AP behavior

The assumption made here is that the APs are configured to respond to broadcast probe requests.

Calculations

Num_{AP} = Number of APs that can hear the client or which the client hears.
Num_{VAP} = Number of virtual APs configured per AP. The APs will have a unique BSSID for each of these virtual APs.
Num_{C} = The number of clients in a given coverage area that hear Num_{AP} APs.

Every AP sends a beacon once every 100 milliseconds.
Number of beacons per AP per SSID = $10 * Num_{AP}$
Number of beacons per AP = $10 * Num_{AP} * Num_{VAP}$
Number of beacons per AP per minute = $60 * 10 * Num_{AP} * Num_{VAP}$

PBReq = Number of broadcast probe requests for Num_{C} clients per minute = Num_{C} PBRes = Total Number of broadcast probe responses from Num_{AP}
Number of probe responses per client = $Num_{AP} * Num_{VAP}$
PBRes = $Num_{AP} * Num_{VAP} * Num_{C}$

PUReq = Total Number of probe requests from Num_{C}
PURes = Total number of probe responses for the PUReq from the client
= $Num_{AP} * Num_{C}$

Total number of packets from the client = PBReq + PUReq
Total number of packets from AP = Probe response + Beacons
= Beacons + PBRes + PURes
$= (60 * 10 * Num_{AP} * Num_{VAP}) + (Num_{AP} * Num_{VAP} * Num_{C}) + (Num_{AP} * Num_{C})$
$= (600 * Num_{AP} * Num_{VAP}) + (Num_{AP} * Num_{C}) (Num_{VAP} + 1)$

Total packets per minute = Packets from client + Packets from AP
$= (2 * Num_{C}) + (600 * Num_{AP} * Num_{VAP}) + (Num_{AP} * Num_{C}) (Num_{VAP} + 1)$

Packets per sec = PpS

$$\frac{(2 * Num_C) + (600 * Num_{AP} * Num_{VAP}) + (Num_{AP} * Num_C)(Num_{VAP} + 1)}{60}$$

$$PpS = \frac{(2 * Num_C) + (600 * Num_{AP} * Num_{VAP}) + (Num_{AP} * Num_C)(Num_{VAP} + 1)}{60}$$

Time to transmit

Considerations

- Beacons and probe requests / responses are transmitted at the lowest supported rates which would be 1 Mbps for 802.11b/g and 6 Mbps for an 802.11a network
- Assumption made is that probe requests, responses and beacons are of approximately 100 byte (since these calculations are used to provide a rough estimate of the bandwidth consumptions)
- Long preambles overheads and ACKs for unicast packets are not considered

Rate = The minimal rate at which these packets are transmitted (1 Mbps for 802.11 b/g and 6 Mbps for 802.11a)
Time to transmit 1 bit = $(1 / 2^{20})$
Time to transmit 100 bytes = $100 * 8 * 1 / 2^{20}$
Adding DIFs (inter packet interval)

$T_{pkt} = (100 * 8 * 1/ 2^{20}) + 50$ [50 microseconds is the DIFs time]

Time to transmit PpS number of packets =

$T = PpS * T_{pkt}$ microseconds
% bandwidth utilization when the AP is transmitting at rate R
$\%B = (T / 10^6) * 100$

$$T = PpS * T_{pkt} \text{ microseconds}$$
$$\%B = (T / 10^6) * 100$$