Extreme Wireless WiNG

High Density Design

Abstract: The deployment architecture of WiFi networks is shifting from providing large cell coverage areas to application specific coverage areas. With WiFi being a half-duplex shared medium and RF propagation characteristics, network administrators are finding it challenging to plan, deploy and maintain high density WLANs in university auditoriums, theme parks, airports etc This guide outlines the key challenges and addresses design dilemmas network administrators are faced with when designing high density design.

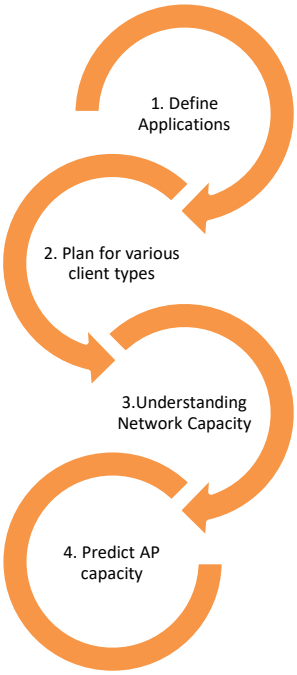
Published: November 2017

Extreme Networks, Inc.
6480 Via Del Oro
San Jose, California 95136
Phone / +1 408.579.2800
Toll-free / +1 888.257.3000
www.extremenetworks.com

Contents

Design Considerations

A high density design can quickly get complex due to varying factors that need to be addressed. These key considerations can be summarized as shown in the figure below.



Applications - The successful design of a high density network starts with defining the requirements. The first step is to define the applications that need to be supported on a WLAN. For example, Service Level Agreements (SLA's) for watching YouTube style videos for educational purposes is very different from supporting voice calls. The application partly affects the Access Point (AP) capacity and placement. High throughput intensive applications like video will reduce the amount of clients supported on a single radio leading to higher number of AP's. Thus figuring out a how applications affect capacity is a challenging issue which needs to be identified.

Client Devices - There has been an explosion in the various kinds of client device from Smartphones to tablets to Laptops. Most devices shipped today are 11ac compliant however; they don't support the maximum data rates of >1Gpbs. To conserve battery life of portable devices manufactures limit the devices to lower data rates like 72.2Mbps. This has an impact on the overall system throughput and needs to be accounted for when designing a high density network.

Network Capacity – The total network capacity is a function of technologies (a/b/g/n/ac) and applications. 802.11ac devices support varying speeds and generate overhead in presence of legacy clients and can lead to throughput degradation. Understanding these complexities will aid in a better design

AP Count and Capacity – Figuring out the number of AP's is not a trivial task. Based on the type of client devices in the network and the applications, AP capacity can be estimated. AP Capacity can also be affected by co-channel and adjacent channel interference. Placing AP's close to each other or at high power can generate enough interference to drag the throughput down. It is thus important to understand various AP placement options along with the associated pros and cons. Moreover, the amount of available channels can hamper the design by limiting the number of deployed AP's

Define the Applications that will be used over WLAN

Applications play a critical role in the design since user expectations are based on how well their applications work. For example, in a classroom/auditorium scenario, streaming video is a critical application. Understanding the application and the associated SLA's is very important. Video based applications are time-sensitive and throughput intensive. A jittery video will not be acceptable to the end user.

Applications dictate the amount of throughput that is required per client which affects the total number of clients that can associate to a single radio. It is thus important to know the bandwidth requirements of all applications. The following table lists some common bandwidth requirements and associated packet sizes:

Application	Bandwidth
Netflix Ultra HD Quality*	25Mbps
Netflix HD Quality*	5Mbps
FaceTime**	1Mbps
YouTube***	500Kbps – 1Mbps
Web Browsing	500Kbps – 1Mbps
Skype (HD)#	1.5Mbps
Google Hangout##	3.2Mbps

*https://support.netflix.com/en/node/306

**http://support.apple.com/kb/HT4534

***https://suppor.google.com/youtube/answer/78358?hl=en

#https://support.skype.com/en/faq/FA1417/how-much-bandwidth-does-skype-need

##https://support.google.com/a/answer/1279090?hl=en

Identify Client Types that will be used on the Network

Client type will dictate the efficiency of the network. Hence it's important to know what client types will be accessing the network. With 802.11a/g networks all clients supported identical data rates. However, 802.11n/ac introduces varying modes of operation: Single stream to multiple streams, 20Mhz / 40 MHz to 80Mhz operation, multiple radio chains etc. Two 802.11ac certified clients will interoperate but may not necessarily have the same speeds and feeds.

For example, with a 1.3Gbps capable AP (a 3x3:3 MIMO like AP7532) the effective TCP throughput can be close to 975Mbps (1500 byte frames). This assumes that the client is also capable of 1.3Gbps speed. With the same AP if you associate a 1x1:1 Smartphone or tablet that is only capable of 72.2Mbps data rates, the effective TCP throughput will be around 30-40Mbps (1500 byte frames).

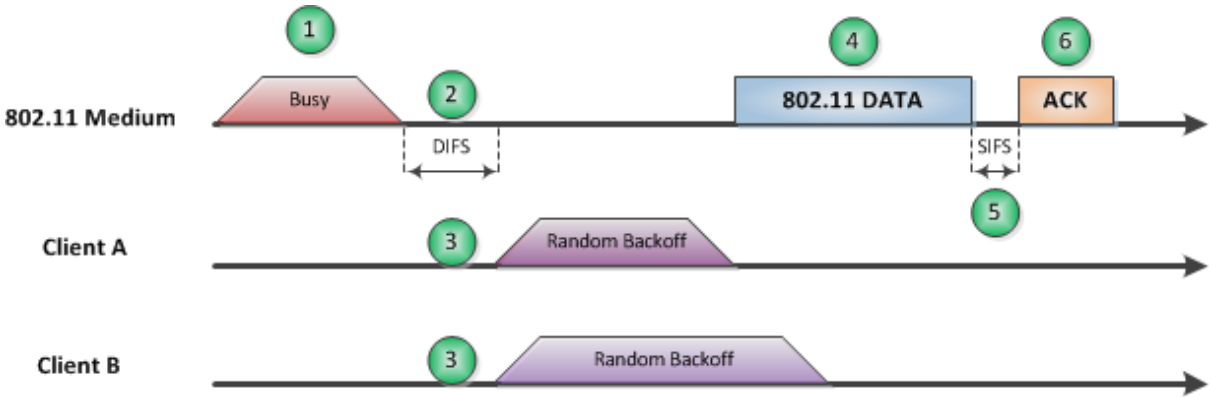
Why is there a difference? This is analogous to having a highway capable of supporting cars speeding at 300 mph. Now if a car goes at 65mph, the efficiency of the highway is significantly reduced.

What happens when packets go at varying speeds?

Let's consider the highway example again. There are cars going at 300mph. If we add cars that can traverse at 65mph, things will start to slow down. Adding more and more 65mph cars will lead to a traffic jam. The same is true for wireless networks. As the number of lower data rate client's increases, the overall available bandwidth shrinks since these devices spend more time on air.

Throughput over 802.11a/b/g

Unlike Ethernet (802.3), 802.11 is a half-duplex medium and cannot detect collisions over the air. 802.11 mandates a random back off mechanism that enables each client to avoid collisions over the air. Following figure depicts the mechanism in detail.



The figure above illustrates how the random back off mechanism works. Let's assume Client A and Client B want to transmit a packet. Following the sequence of events:

1. Both Clients sense the medium to the busy and refrain from transmitting
2. After the medium becomes idle, both clients wait for a specific amount of time called DCP Inter Frame Spacing (DIFS)
3. After the DIFS expires and the medium is still idle, both clients start a random back off timer
4. In the above scenario Client A's random back off timer expires and he gets control of the medium to transmit his Data packet. Client B sense the medium is busy and refrains from transmission until the medium is idle again
5. After the data packet is transmitted, the receiving station needs to acknowledge the successful reception by sending an ACK packet. To give this packet priority

over other clients like Client B that are waiting to transmit, a Short Inter Frame Space (SIFS) is used. SIFS is shorter than DIFS

6. After the SIFS expires, the receiver sends the ACK back to Client A. The medium now becomes idle and the entire process repeats

To ensure reliable packet delivery over wireless, the standard specifies and mandates a built in reliability mechanism. Every unicast data packet transmitted by an 802.11 transmitter needs to be acknowledged by the receiver as seen above. Due to this overhead associated with every packet the effective throughput is much less than the advertised data rate. For example, on an 802.11a/g network the maximum data rate supported is 54Mbps. However, the maximum achievable TCP throughput is about 25Mbps. The reason for this loss is the overhead due to 802.11 control packets like Acknowledgements.

Throughput over 802.11n/802.11ac

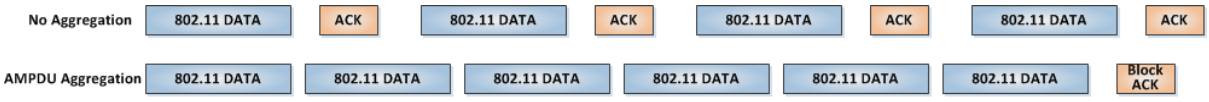
802.11n significantly enhanced the throughput of the network using the following amongst others:

- Increased the data rate from 54Mbps to 450Mbps (3x3:3 MIMO with 40MHz wide channel)
- Introduced Aggregation (AMSDU and AMPDU)
- Reduced the guard interval
- Introduced MIMO
- Optional 40Mhz channel

Furthermore 802.11ac expanded on 802.11n enhancements and added the following:

- Increased the data rate from 450Mbps (3x3:3 MIMO with 40MHz channel up to 2.17Gbps (4x4:4 MIMO with 80MHz wide channel)
- Increased bit density that provided 33% increase in throughput
- Increase the number of spatial streams
- Introduced Downlink MU-MIMO to support concurrent transmission to multiple clients (in practice showed mixed results across different environments, realistically only works in controlled static environment providing up to 2x increase in aggregate throughput)
- 20 MHz / 40MHz / 80MHz / 160MHz channel width

One key enhancement was aggregation. Rather than acknowledging each packet, 802.11n specifies a new Block ACK packet. The transmitter can send multiple data packets back to back and the receiver then responds back with one single Block ACK packet that acknowledges every packet received as seen in the figure below



As seen above the Block ACK acknowledges all packets it has received as opposed to No Aggregation where each packet is acknowledged. The overhead in ACK's leads to throughput degradation.

Mixed Mode Throughput

So far we have seen how 802.11a/b/g and 802.11n/802.11ac function independently. However, in a real world deployment these two technologies are deployed together. There are a lot of legacy devices that are supported by 802.11n/802.11ac infrastructure. 802.11n was designed to be backwards compatible with 802.11a/b/g. 802.11ac while being backward compatible with 802.11a/n is 5GHz only, therefore it is not applicable for 2.4GHz

band and interoperability with 802.11b/g standards. Higher 802.11n/802.11ac data rates are achieved with different modulation techniques that are not supported by the legacy clients.

802.11n mixed mode with 802.11b/g

When an 802.11n packet is transmitted, the legacy clients will not be able to de-modulate the frame and hence will not back-off the medium. In order to prevent this situation 802.11n clients use protection mechanisms. Before transmitting frames at 802.11n rates, the clients transmit a protection packet that can be demodulated by legacy clients. This packet reserves the medium and forces all clients to back-off for a duration defined in the protection packets. The protection packets are transmitted legacy rates to ensure all clients can decode them. This same concept was used by 802.11g clients when transmitting in presence of 802.11b clients.

As above the CTS-to-self (protection packet) is transmitted prior to any 802.11n Data transmissions. This reserves the medium for a specific duration and causes all clients to backoff. Using protection packets can drastically affect the throughput of the network

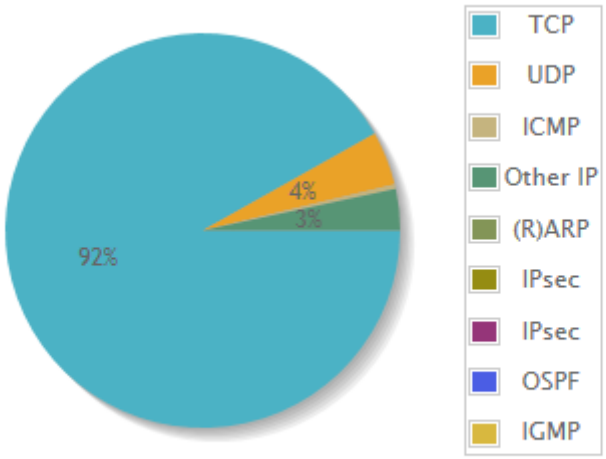
802.11ac mixed mode with 802.11a/n

802.11ac clients use the same protection mechanisms for 802.11a clients. As for mixed environments between 802.11ac and 802.11n clients, 802.11ac clients will use a compatible preamble allowing 802.11n devices to read the medium as busy and avoid collisions.

Estimate Network Throughput

Protocol Type

The type of protocol (UDP or TCP) an application uses affects the network performance. UDP being a stateless protocol has less overhead and hence better throughput. It is strongly recommended to check what protocols are dominant in the network using Network Management / Network Analytics tools, such as ExtremeNSight or ExtremeAnalytics. The following snapshot was taken from a live network and shows 92% of the traffic is TCP, which is typical for any public WiFi environment, as most of the modern apps are TCP based.



UDP Aggregate Network Throughput (ANT)				
	20 MHz	*20MHz*	*40MHz*	*40MHz*
Packet Size	*54Mbps (11a)*	*65Mbps (11ac 1x1)*	*150Mbps (11n 1x1)*	*300 Mbps (802.11n 2x2)*
88	*3.59*	*33.41*	*37.37*	*57.917*
128	*5.12*	*48.33*	*54.23*	*57.917*
256	*9.3*	*82.128*	*102.47*	*162.18*
512	*16.02*	*89.13*	*122.323*	*210.62*
1024	*24.69*	*93.01*	*133.88*	*246.09*
1280	*27.57*	*93.43*	*135.66*	*251.75*
1518	*30.13*	*93.58*	*136.16*	*254.288*

Table above lists the UDP Downstream Throughput obtained using 1 client. The tests were conducted for various types of clients and packet sizes. As seen based on the client type (for example 65Mbps vs. 300 Mbps) and packet size the throughput varies. These tests were conducted using IxVeriWave.

Collision Factor (CF) and Mixed Mode Factor (MMF)

The Collision Factor or CF is used to determine the effects of collision on AP capacity. This factor was calculated based on various tests conducted by Extreme Networks and depends on the aggregate throughput drop as client count increases.

Collision Factor* (CF) = 0.8

The Mixed Mode Factor or MMF is calculated based on the throughput drop as the mix of client's changes from 11n/ac to legacy a/b/g clients and from 802.11ac to 802.11n as well. This factor affects the overall AP capacity.

Mixed Mode Factor* (MMF) = 0.6

*These factors are rough estimates and may not give accurate results

Estimate AP Count and Capacity

In the previous section we demonstrated the capacity of a single AP when using a mix of legacy and 802.11ac clients. However, the overall AP count and capacity will depend on many other factors that need to be taken into consideration. The following sections outline these considerations.

A rough estimate of AP Count can be made based on the various variables defined in the previous section. Following are some definitions:

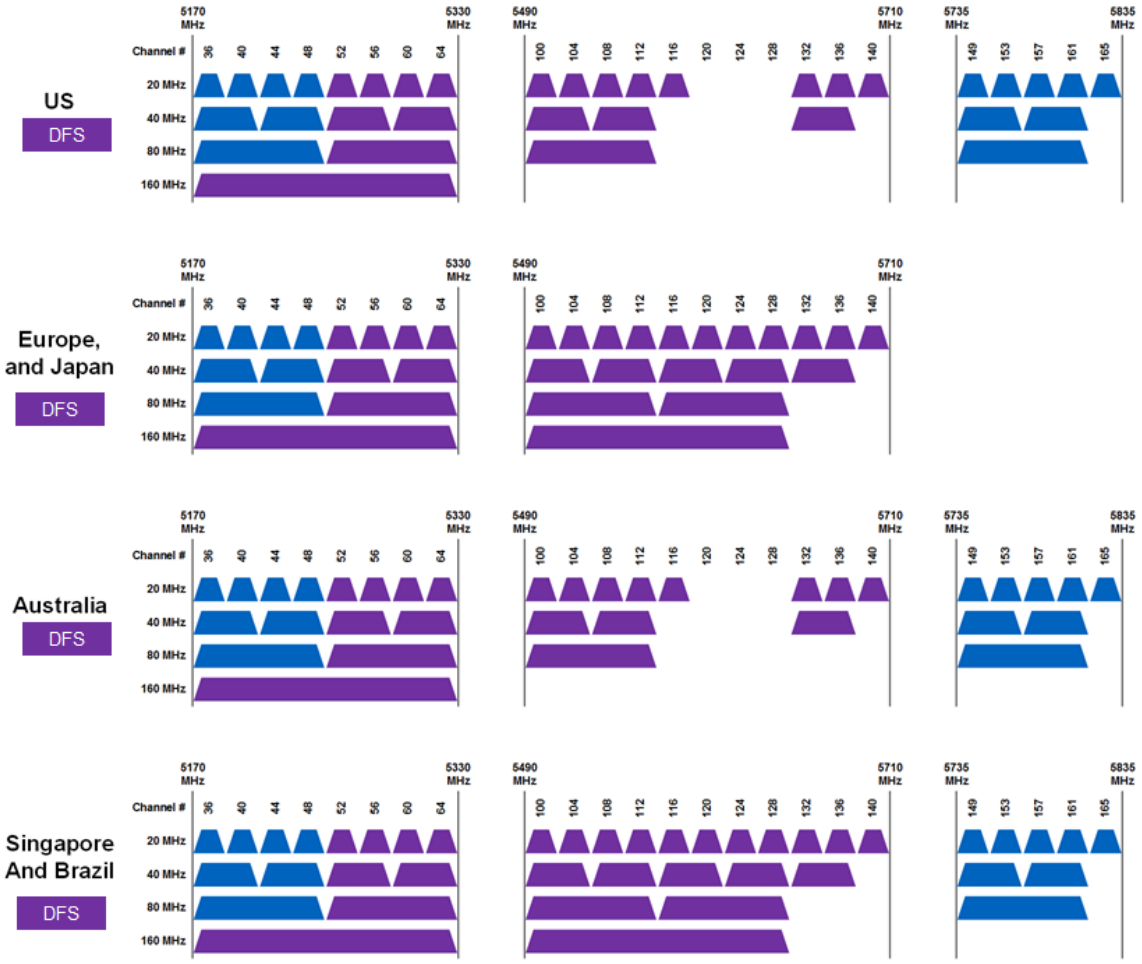
Variable Name	Description
Application Throughput (AT)	The amount of throughput application needs
Aggregate Network Throughput (ANT)	Total aggregate throughput of the radio based on the type(s) of clients
Base Client Count (BCC)	Client Count in an Ideal RF environment. *BCC = ANT / AT*
Collision Factor (CF)	Degradation of throughput based on collisions
Mixed Mode Factor (MMF)	Degradation with mixed mode clients
Client Count (CC)	Client count based on collisions *CC = BCC * CF*
Final Client Count (FCC)	Client count based on Mixed Mode and Collisions *FCC = (CC1 + CC2 + … CCn) * MMF/n* CC1 – 1st type of client (i.e. 802.11ac 1x1 72.2Mbps) CC2 – 2nd type of client (e.g. 802.11n 300Mbps) CCn – nth type of client (e.g. 802.11a 54Mbps)
Access Point Capacity (APC)	Final Number of Radios required: *APC = Total Number of Expected Clients / FCC*

The overall AP count and capacity will depend on many other factors that need to be taken into consideration. The following sections outline these considerations.

Channel Planning

The availability of a channel depends on the regulatory domain where the AP will be deployed. The first step in channel planning is to get the list of allowed channels.

The 5 GHz band has more non-overlapping channels. The 7532 for example has 20 channels that it can operate on. This provides more room to collate AP's without the need for channel re-use. The list of available channels varies based on the model number of the AP and country of operation. Please refer to the technical documentation to verify the available channel list. One thing to note when deploying in 5 GHz is the Dynamic Frequency Selection (DFS) requirement on certain channels. DFS requires AP's to detect radar signals and change channels. Out of the 24 channels in the US only 9 channels are Non-DFS (36-48 and 149-165), while in EU there are only 19 channels with only 4 Non-DFS (36-48). Following is a list of allowed channels



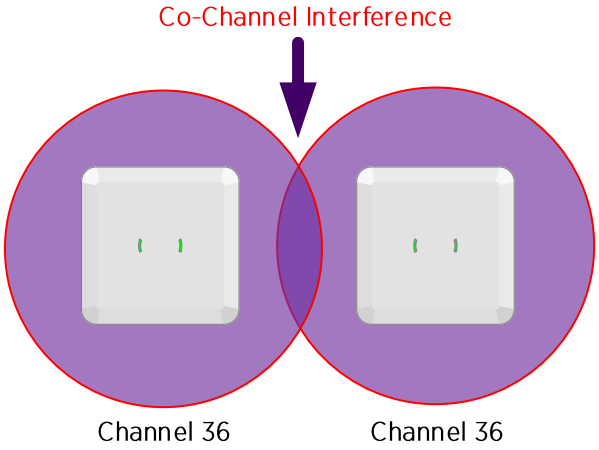
The AP will change channels on radar detection or false positive events which can be very disruptive to the network. Moreover, a lot of client chipsets do not support DFS channels. Hence it is important to be aware of these issues while deploying AP's on DFS channels. Based on the capacity there may be a need to use DFS channels or re-use non-DFS channels. The effects of the latter are discussed below

Co-Channel Interference (CCI), Adjacent Channel Interference (ACI) and AP Placement

- What is Co-Channel Interference (CCI)?

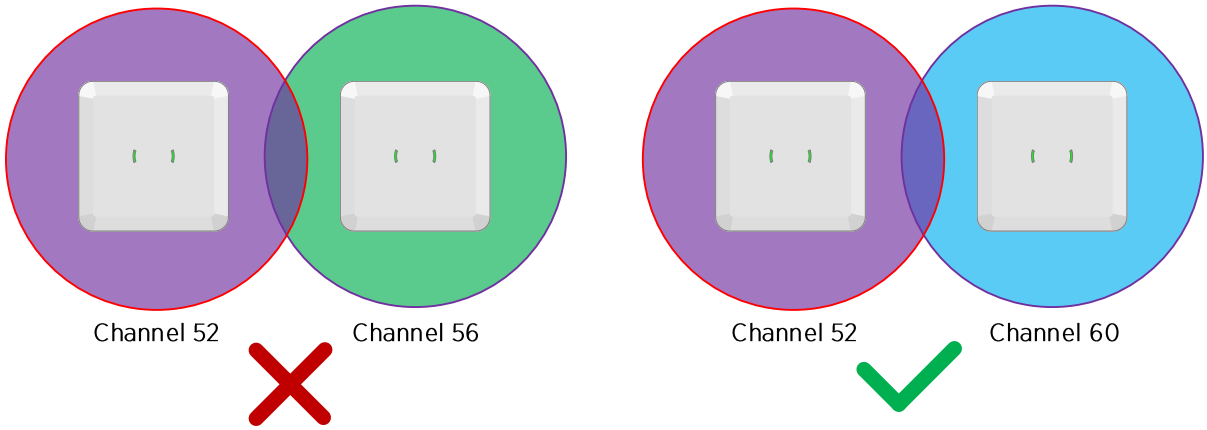
When the two Wi-Fi operating devices transmit the data on same channel (for instance channel 36), in such a manner that they both interfere in each other's range, co-channel interference occurs. This results in degradation of network performance and if a client

device wants to transmit data, it would see the channel occupied. Hence, CCI is an important factor that should be taken care of. The impact of CCI can be limited by using different channels in the surrounding AP cells or having attenuators – wall partitions, pillars, thick metal plates, that absorb the signal.



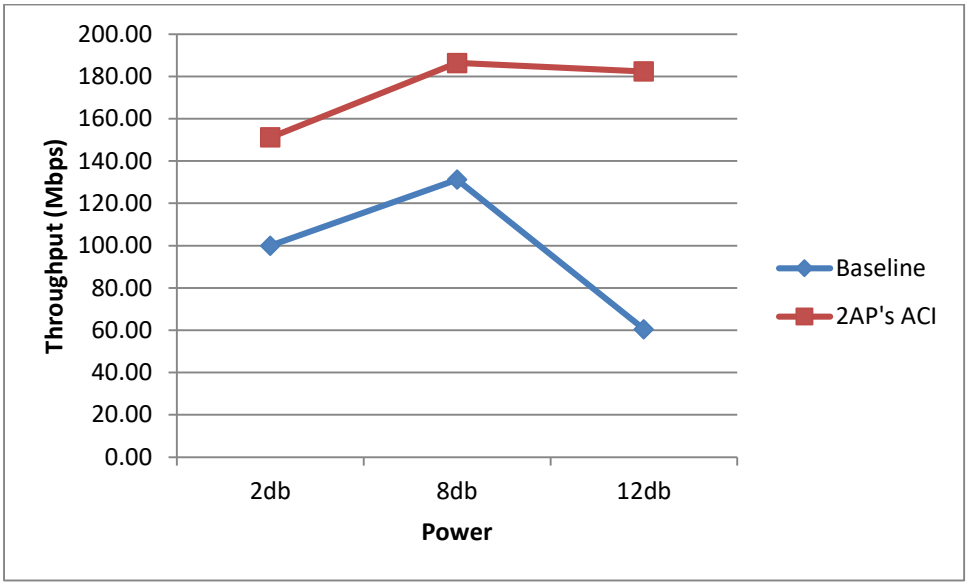
- What is Adjacent Channel Interference (ACI)?

It should be noted that the APs' should not be operating on same channel or adjacent channels. These APs' should not be placed in line of sight or adjacent locations to each other in order to limit the impact of CCI and ACI respectively. The AP operating on channel 52 should not be placed near an AP that operates on adjacent channel 56 as the signal would overlap and cause interference; thereby reducing the throughput and performance of the network.



The figure below demonstrates how ACI affects performance. Two AP's were spaced at 25' from each other. The baseline test was done on each AP individually using 1 client. The throughput was measured at various power settings. At 2dBm there is not enough signal at the ground level causing lower throughput. At 8dBm and 12dBm the throughput remained almost the same.

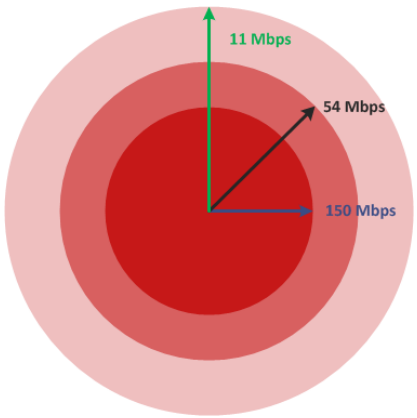
The test was repeated with both AP's transmitting simultaneously on channel 36 and 40. One client was connected to each AP. At 2 dBm the throughput degradation was not a whole a lot. However, at power 12dBm the throughput dropped over 50%. Based on these results it evident that the transmit power of the AP should be set to optimal values or else there can be significant interference



It is also important to note the client power can cause ACI. For example, Intel Client Software gives the user the ability to tweak client transmit power settings. Also 802.11h specifies transmit power control (TPC) that can be used set power levels on supported clients

Understanding Coverage Patterns

When designing a wireless network, it is important to understand how coverage varies at different data rates. In a high density deployment, the AP coverage area can be large when lower data rates are enabled. Data rates are determined by different signal modulation techniques.



As seen in the figure above an 11Mbps signal will have a much larger range than a 150Mbps signal. In a high density deployment, it is strongly recommended to disable lower data rates to increase available airtime by forcing clients to use higher data rates.

Note that trimming lower data rates does not reduce the RF cell size at the PHY level. CCA (Clear Channel Assessment) algorithm still works by looking at the PLCP preamble and header of every frame received by wireless clients or APs, which is always sent at a hardcoded data rate, either 1, 2 or 6 Mbps depending on the preamble length (short / long) and band (2.4GHz is 1 or 2Mbps; 5GHz is 6 Mbps).

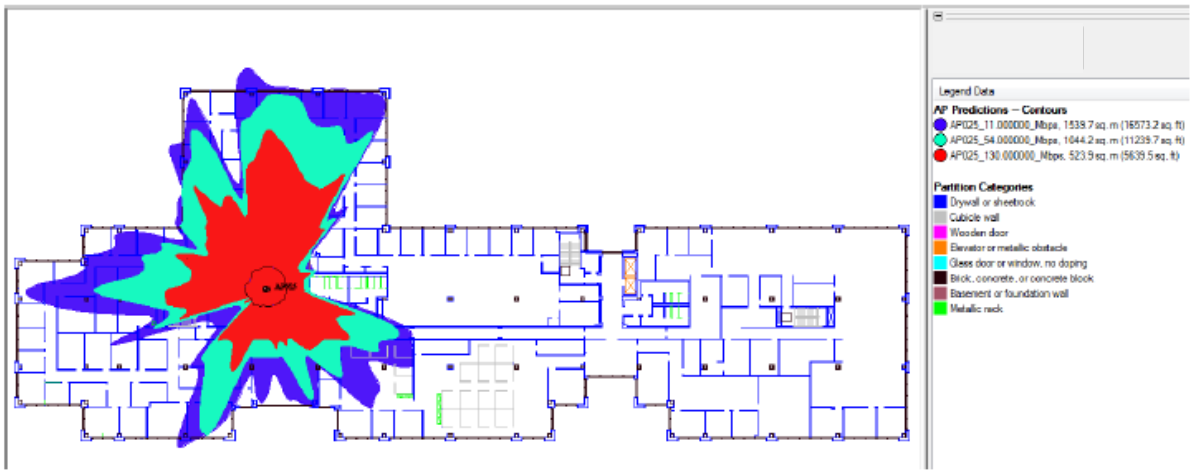


Figure 18 - LanPLanner Heat Map

As seen in the figure 18 the coverage patterns for AP's varies with technology. A 11n AP at 150 Mbps has a much smaller footprint compared to an AP at 54Mbps data rates. 802.11ac 256QAM data-rates will reduce the effective coverage even more. Since 11n is backwards compatible with 11a/b/g networks and 802.11ac is backward compatible with 11a/n it can cover a large area at lower data rates. Thus while designing a network it is important to decide what data rates should be supported. All lower data rates should be avoided if possible.

Choosing the right Antennas

Antennas are an integral component of any wireless network deployment. They enable communication between two wireless devices by converting guided waves on wires into free-space radio waves and vice versa. Hence, at the physical layer of a wireless network antennas play a key role similar to that of an Ethernet cable in a wired network. However, communication process between an access point and associated client devices becomes more complex as transmission and reception of data takes place through air as the medium of communication. Therefore, use of antennas requires more attention during planning phase of a deployment to design and deploy an optimal wireless network.

Extreme Networks provides variety of antennas that operate in the 2.4GHz, 4.9GHz, and 5.0GHz bands as part of its Wireless LAN portfolio. While antennas can work in any given environment, some are likely to be a better fit for network access based on the location and coverage needs. Hence, use of right antennas in right location can help maximize both the performance and coverage of the network.

In following sections, we will discuss certain characteristics of antennas and deployment options for which the antennas can help provide an optimal coverage solution.

Antenna Patterns

Antenna patterns are used to understand how an antenna radiates its energy in space. A pattern defines change in energy radiated by an antenna over distance. That is, the pattern identifies how radiation of power changes as you move away from the antenna. Given that an antenna radiates in all directions, the radiation of an antenna can be described in a 3-dimensional radiation pattern. However, as normal industry practice, 2-dimensional radiation patterns are provided as cuts of a 3-dimensional radiation pattern.

To understand this, we can consider the radiating pattern provided in Figure of an "isotropic"[1] antenna. The antenna patterns can be represented in 3-dimensions (as seen in Figure) or in 2-dimensions using the polar coordinates system shown in Figure

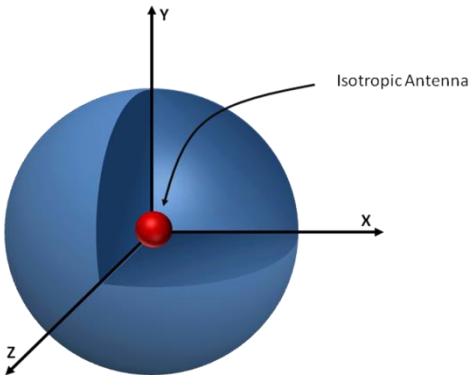


Figure: Isotropic Antenna Radiation Pattern

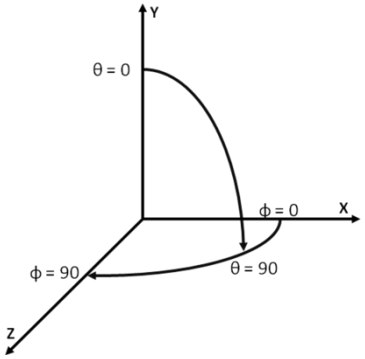


Figure: Polar Coordinate System

The Azimuth pattern, also referred to as horizontal pattern, is a cut of the 3-dimensional pattern at measured maximum value on the x-z plane when θ is at 90°. Similarly, the Elevation pattern is a cut of the 3-dimensional pattern at measured maximum value on the x-z plane when φ is at 90°.

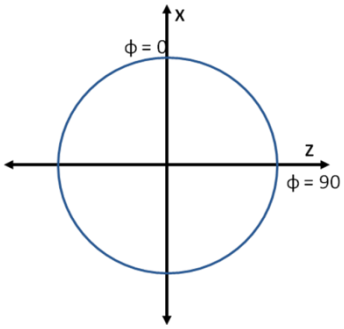


Figure: Isotropic Azimuth Pattern

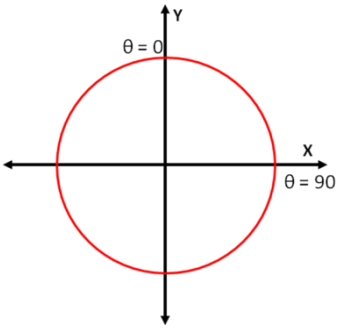


Figure: Isotropic Elevation Pattern

It has always been an acceptable practice in the industry to provide the Azimuth and Elevation patterns of an antenna because they are easy to produce and are able to provide sufficient information in determining the overall coverage of an antenna.

[1] Isotropic antenna is an ideal antenna that radiates equally in all directions around the antenna. They do not exist in practice, but they are used to understand antenna phenomenon and for comparison of characteristics with real antenna.

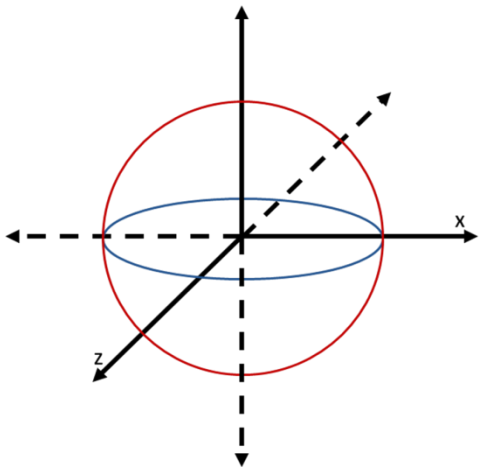


Figure: Isotropic Azimuth and Elevation Pattern

RF patterns are generated in form of a polar plot as shown in Figures. They are defined either as Omni-directional or directional patterns. Omni-directional pattern indicates that the signal from an antenna radiates in all directions in the azimuth plane. Whereas, directional pattern indicates that the signal from an antenna radiates in a specific direction, typically described as a beam of given width, expressed in degrees in the azimuth and elevation plane.

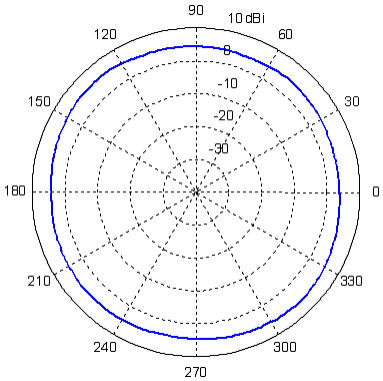


Figure: Omni-directional Azimuth Pattern

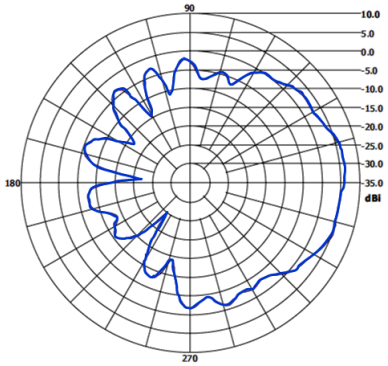
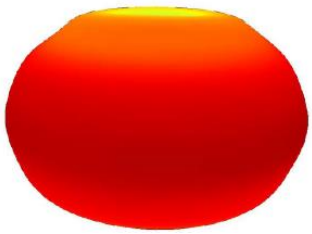


Figure: Directional Azimuth Pattern

As part of this document we will focus on dipole, patch, sector and panel types of antennas. We will also identify how these antennas can help optimize RF coverage based on install location.

- Dipole Antennas

When positioned vertically, the antenna emits power in all directions in the azimuth plane. Whereas, an elevation cut of the coverage in the elevation plane the power is emitted with 2 main lobes, each in the opposite direction. A 3-dimensional coverage pattern of the antenna takes form of a toroidal coil.



The radiation from the antenna occurs mainly around the antenna with radiation nulls (places where an antenna radiation is the weakest as compared to other areas surrounding the antenna) above and below the antenna.

As seen in the figure below, Extreme Networks ML-2452-APAG2A1-01 antenna is a perfect example of a dipole antenna. It emits Omni directional radiation in azimuth plane and directional radiation in the elevation plane.

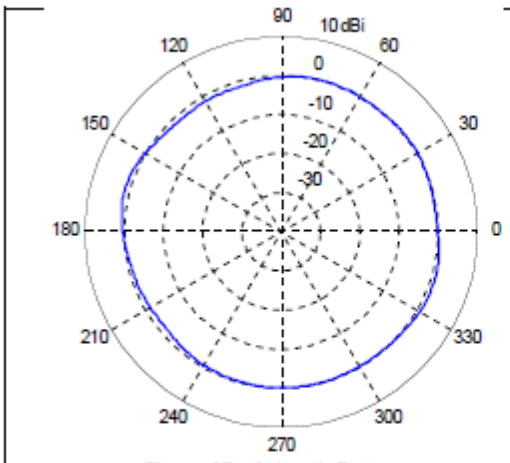


Figure 27 - Azimuth Pattern

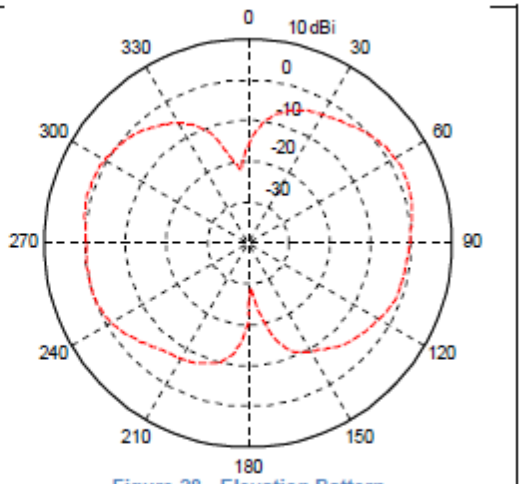


Figure 28 - Elevation Pattern

- Patch Antennas

Patch antennas can be considered as Omni antennas because they provide Omni coverage in horizontal plane. In vertical plane, they radiate energy away from the antenna in a given direction.

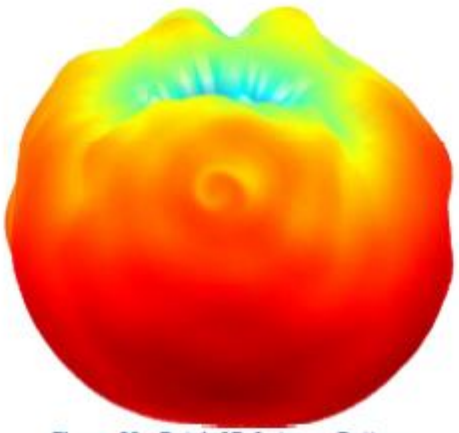


Figure 29 - Patch 3D Antenna Pattern

To better visualize the radiation, consider the 3D pattern provided in figure 29. By taking a horizontal cross-section of the pattern with respect to the antenna produces shows how the antenna distributes the RF energy in the azimuth direction, as seen in figure 30. Likewise, a vertical cross section of the pattern produces the elevation pattern provided in figure 31.

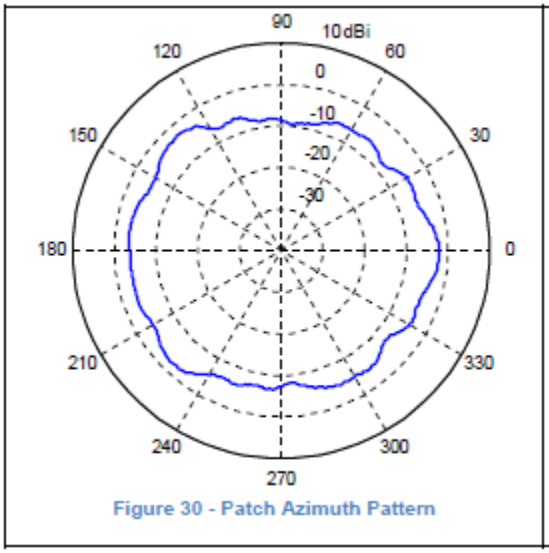


Figure 30 - Patch Azimuth Pattern

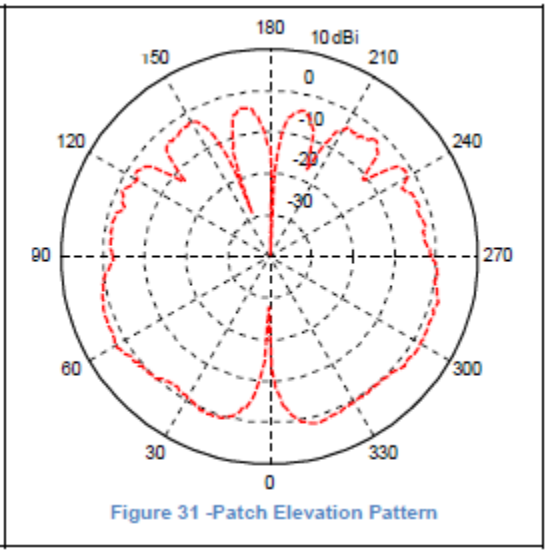


Figure 31 -Patch Elevation Pattern

Patch antennas thus produce an Omni coverage like that of a flashlight. Consider shining a flashlight on a wall while standing 2 feet away from the wall. If the light produced from the flashlight is observed from the flashlight's point of view, a circle will be observed on the wall. While, viewed from a side a directional radiation is observed. As you move the flashlight further away from the wall, the coverage of the light on the wall continues to increase. Since patch antenna behaves identical to a flashlight, they are the preferred antennas to install on ceilings to cover large areas on the floor. However, it is important to note that just as the intensity of the light continues to decrease as the flashlight is moved further away from the wall, the patch antennas radiation also continues to lose intensity as the distance between the antenna and clients increases. Therefore, as part of RF planning it is critical to ensure that the ideal gain of antenna is selected to get an optimal coverage.

- Sector and Panel Antennas

Sector and Panel antennas are directional antennas. Both types of antennas radiate energy directionally in azimuth and elevation plane. The 3dB beamwidth of azimuth pattern helps distinguish the two types of antennas. 3dB beamwidth is the width of the main beam represented in degrees between the two half power points (also known as 3dB points) on the antenna pattern. As shown in figures 32 and 33, the 3dB beamwidth of the panel antenna is 68◦ and beamwidth of a sector antenna is 120◦.

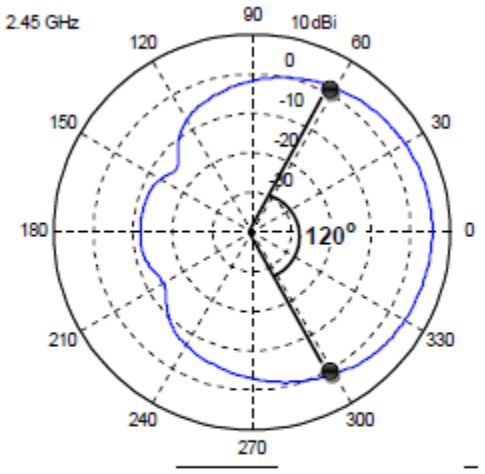


Figure 32 - Sector antenna with 120o of azimuth beamwidth

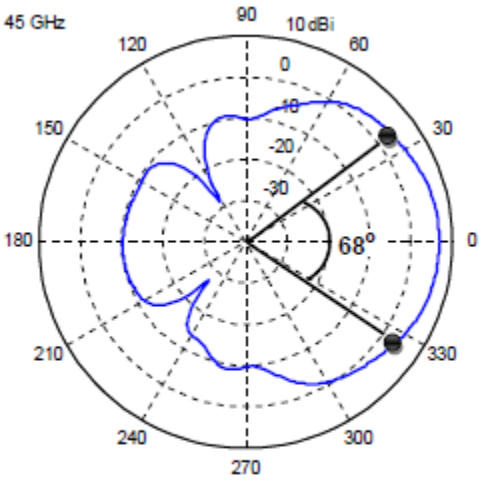


Figure 33 - Panel antenna with 68o of elevation beamwitdh

The 3-D pattern below of the same antenna shows how the radiation from a sector antenna provides wider coverage.

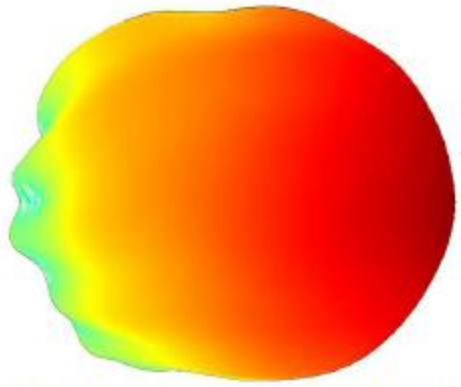


Figure 34 - 3-d antenna coverage view of the sector antenna

Between panel and sector antenna with same gain, the sector antenna is designed to provide wider area of coverage whereas the panel antenna is designed to provide a narrower area of coverage. Hence, panel antennas are mainly used to provide long-range narrow coverage while sector antennas are used to provide wide area coverage near the antenna.

AP Placement Strategies

The challenging task in improving the network performance in a HD environment is placement of AP. An accurate and précised survey of the site is required. Depending on site construction, for instance large auditorium, conference hall, APs' can be generally placed in following ways.

In legacy deployments, coverage based on low data rates to support wireless clients was an acceptable trend. Such deployments mainly consisted of an access point and an antenna combination that offered coverage cell size defined by applications running on lower legacy rates supported by 802.11a/b/g. However, such a deployment cannot scale to meet demands of deployments where people gather in groups to participate in a common event. Advances in mobile applications and proliferation of 802.11n and 802.11ac client devices have led consumers to expect network based services at social venues. Hence, the deployments of today and of future will require wireless network that can provide robust network access per client and be able to serve more clients within an RF coverage cell.

Dense deployment of 802.11ac access points is an ideal way to address this challenge. This deployment practice is essential for indoor and outdoor auditoriums where people gather in groups to participate in a common event. Conference halls, college classrooms, concert/performance halls, and sports arenas are all examples of venues where people expect to have access to high bandwidth content and social applications. For each of the venues and based on available mounting options, following use cases of antenna installation should be considered.

- Ceiling mounted:

For areas where access points and/or antennas can be deployed on a ceiling, consider use of low gain patch or low gain dipole antenna for low ceiling areas and high gain patch antennas in areas with high ceiling.

As seen in figure 35, the coverage can be offered in various sets of cells distributed across 2.4 and 5.0GHz frequencies or across a single frequency.

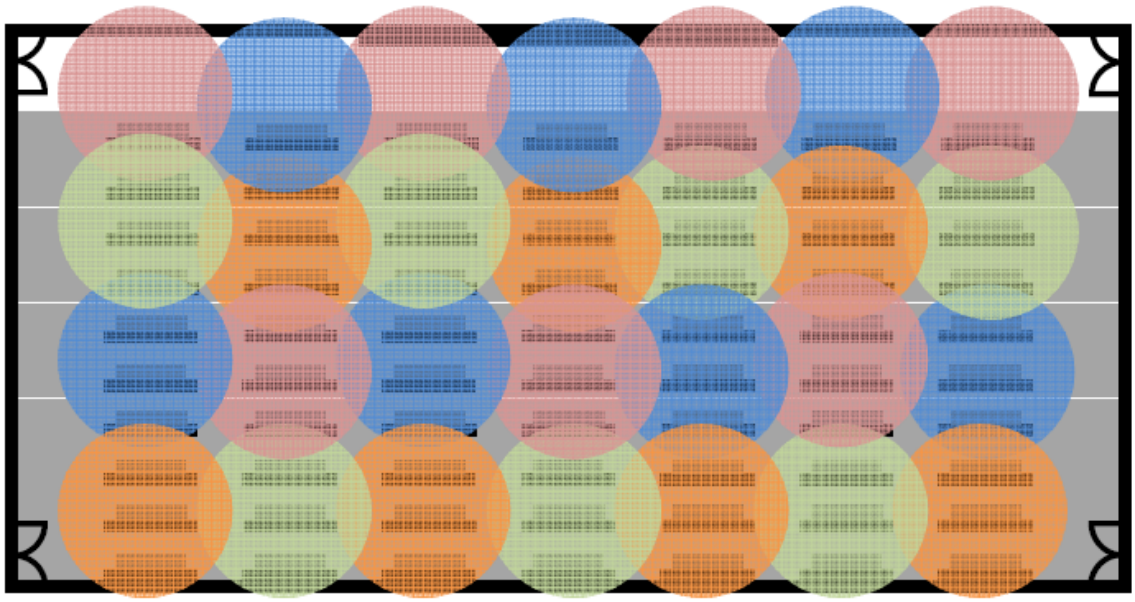


Figure 35 - Top view of RF cell-coverage by patch and dipole antennas

Between Patch and dipole antenna, however, Patch antenna should be considered as a preferred type of antenna for small cell network deployments. RF coverage of a patch antenna is directed more towards the ground, whereas, coverage from a dipole antenna is more directed around the access point.

Installation of dipole antennas in high ceiling environment leads to inefficiency in RF energy distribution. As illustrated in the figure 36 below, the RF coverage of dipole antenna provides more coverage in area near the antenna, but the coverage below the antenna remains very limited. This is the most general technique of placing the APs' at equidistance from each other. With such an equidistant AP placement, ACI and CCI effects are reduced. The AP's coverage is uniform with the ceiling mounted approach. With this strategy, the channels cannot be re-used as the signal coverage expands horizontally. This is shown in following figure. This inefficiency in RF coverage can result in loss of throughput for clients on the floor.

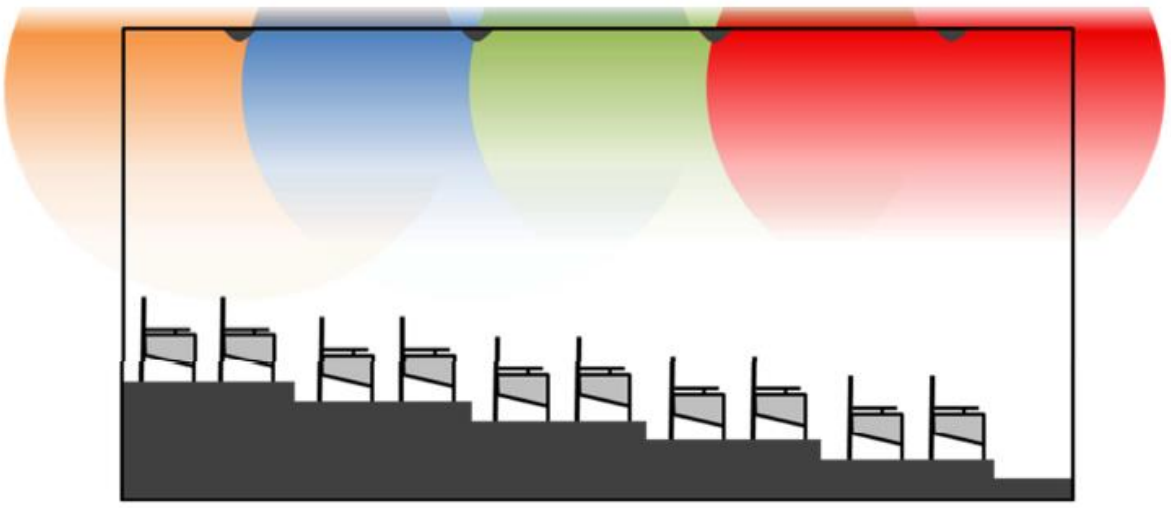


Figure 36 - Side-view illustration of dipole antenna cell-coverage

Hence, to avoid this inefficiency for small cell deployments, it is ideal to deploy patch antennas that can direct coverage underneath the antenna as illustrated in the figure 37 below.

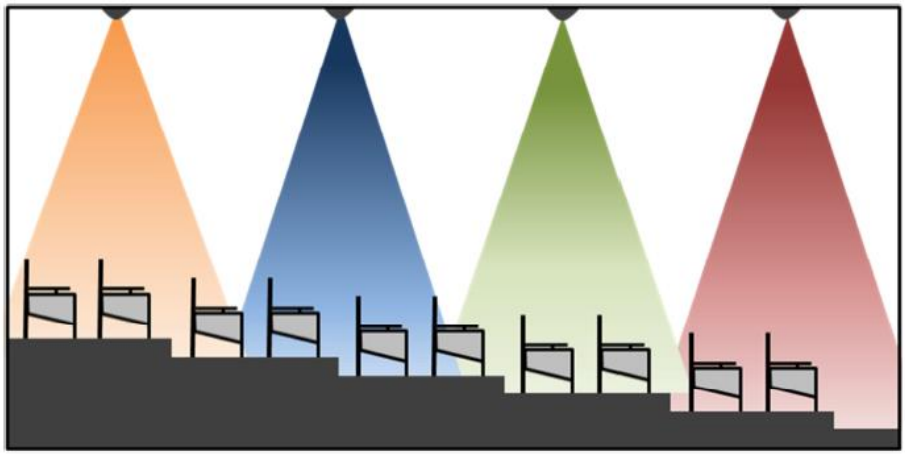


Figure 37 - Side-view illustration of patch antenna cell-coverage

The fact that is required to be taken into consideration with this mounting is the AP antenna used; Omni-directional or a directional antenna. The above scenario uses a directional antenna AP mounted overhead.

- The Omni-directional antenna is useful if no channel is required to be re-used. The signal energy is wasted using Omni-directional antenna as the energy penetrates through the ceiling and hence the energy cannot be used effectively. In addition, the signal energy penetrating through the wall may cause interference with the AP operating around adjacent channel on higher floor. If the site is average-sized, the low gain Omni-directional antennae can cover the entire site, thereby increasing the network performance. A low gain Omni-directional antenna covers lesser floor area i.e. horizontal beamwidth decreases and the vertical beamwidth increases. Hence, an average-sized site with ceiling height of approximately 20 feet, a low gain omni-directional antenna with AP ceiling mounted placement serves as a better option.
- Directional antennas are useful when the site has high ceiling heights and channel re-use is required. Good floor coverage with directional antenna is obtained, with signal energy focused in downward direction, towards the floor. This can be observed from the figure 37. As the maximum signal energy is focused towards the floor, unlike omni-directional antenna, less energy propagates through the ceiling, leading to minimal interference with the AP's operating at above floor. This also offers noise discrimination, both from APs on adjacent channels and other noise sources.

- Side Walls mounting:

Sector or panel directional antennas can be considered for installations on walls. Mid-gain panel antennas with narrow beamwidth and sector antennas with low gain and wide beamwidth can help deploy small cell deployment. One such deployment option is illustrated in figure 38.

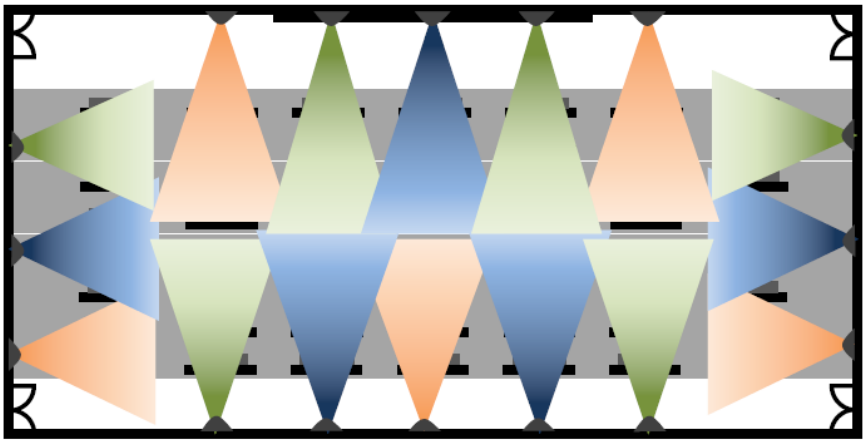


Figure 38 - Panel and Sector Antennas coverage mapping

With articulating mounting configuration, directional antennas from Extreme Networks can be adjusted to allow optimal RF coverage in a given area.

For medium and large auditoriums, one of the biggest challenges remains is the need to cover large areas with very restricted and limited mounting options for access points or antennas. In many dome like structures, ceiling height presents an installation and coverage challenge that cannot guarantee high bandwidth access per user. For outdoor open ceiling stadiums, installation options are even further limited. In both situations, the standard practice remains to install antennas on the walls around the dome and direct the signal in the seating area. Hence, careful deployment planning and antenna selection is essential to achieve optimal coverage using low gain sector and panel antennas.

Any AP placement strategy depends on construction of site. If the site is wider as compared to its length, this strategy may serve as good option for covering the site. This strategy is useful when the site has no ceilings. For instance, hotels with large garden area, outdoor stadiums, where overhead AP mounting is not feasible, side wall AP mounting is one of the option. Like the ceiling mounting strategy, channel re-use is not possible with side wall mounting too. In order to limit ACI and improve the network performance, it should be kept in mind that no two access point operating on adjacent channels should be placed in LOS while mounting the APs' or near to each other. The side wall mounting strategy is shown in below figure, with internal directional antenna used.

- Pillar mounting:

It may be possible that a site may consist of pillars, wall partitions constructed. These constructions create a "shadow" area on opposite side of AP placed on the pillar/partition.

In order to cover the users lying under shadow area, it is necessary to place the APs' using the discussed approaches with the assurance of maximum users being served/covered. The antenna patterns should cover the intended area with less ACI interference. The signal energy is wasted when omni-directional antennae are used because they spread the signal energy outwards, crossing the walls of auditorium. This signal bleed may even lead to interference with the AP operating in adjacent site, causing interference.

- Underneath the seat mounting:

This is one of the good AP placement approach as the access point with external or internal antenna remains hidden from end user view. In addition, the users and seats themselves attenuate the signal and consequently the AP coverage range reduces that leads to usage of more quantity of access points and channel re-use functionality. Intensive

survey is required for this mounting due to the fact that as APs' are placed under the seats, the site having metal seats would attenuate the signal. Hence, the AP coverage area reduces. So, the estimation of number of access points for covering the site is required to be determined carefully. It should be noted that if there are any obstruction/shadows, the shadowed area should be covered by the neighboring access points.

- Floor mounting:

Although it is not a widely recommended deployment practice, customers should also consider installing access points underneath the seating infrastructure. This practice relies heavily on the level of loss the signals the client antennas and the access point antennas will experience through the seating infrastructure. If the seating infrastructure is accessible and applicable for deployment, access points or patch antennas can be mounted facing towards the seating area.

In this deployment, the coverage can degrade tremendously as signals travel through the seating area, resulting into formation of a small coverage cell. As illustrated in the figure 39 below, the RF coverage remains stronger near the antenna and the coverage becomes weaker as the signal traverses through the seating structure.

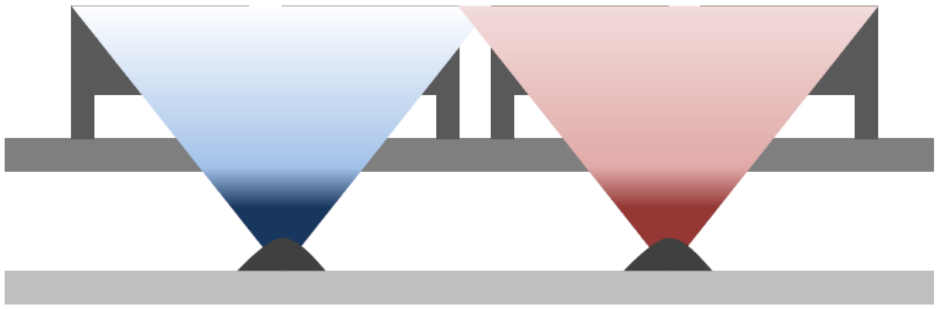


Figure 39 - Floor Install

Distance between the antenna and the seating area needs to also be evaluated before installation. Coverage area is directly proportional to the distance between the antenna and the seating area. If the antenna is placed far away from the seating area, the coverage cell size will grow with reduced signal strength. The ideal placement of the antenna should be determined based on the antenna parameters and the infrastructure environment.

Floor mounting is one of the preferred approach for placing an AP for two reasons. Firstly, it is easy to install AP as compared to ceiling mounting and secondly, the attenuation is provided by human body, seats and floor (if underneath floor AP placement strategy is used). Hence, the possible impact of AP-AP interference reduces and channel can be re-used. In floor mounting approach the access point now points towards the ceiling and the signal energy is directed in upward direction. Floor AP placement can be accomplished in two ways, either placing the AP just above the floor or underneath the floor. These placements depend on site survey and the type of AP and antenna used. It should be noted that while placing the AP underneath the floor, the signal energy should be able to radiate through the floor and provide good coverage so as to improve the network performance, thereby serving the clients satisfactorily. In addition, the distance of AP placed under the floor directly impacts on cell size. In other words, the AP placed under very near to the floor will have lesser cell area as the signal would highly get absorbed. In contrast, the AP placed at a distance from the underneath of the floor, will have greater cell area.

AP Placement dictates the adjacent channel interference between AP's. Factors affecting AP placement are:

1. Radio Transmit power – as a best practice it is strongly recommended to lower the transmit power of the radio. Though if the power is reduced below 9dBm, it will cause a power mismatch with the mobile devices which will then transmit at higher levels, potentially reducing downlink data-rate and increasing overall noise.
2. Antenna type and gain – Choosing the right antenna can significantly increase performance and reduce interference

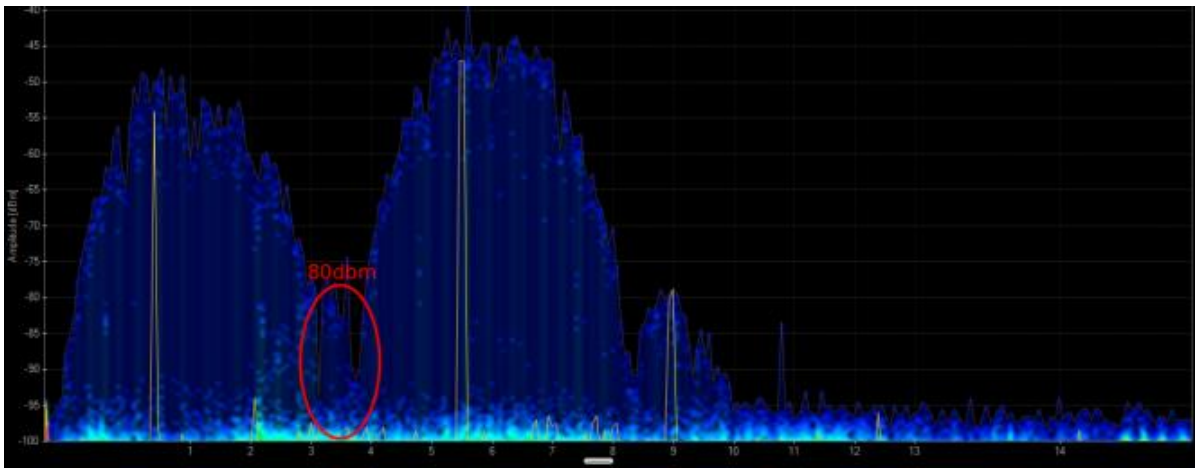
- If AP's are mounted on ceilings or walls or under seats, it is recommended to use integrate antenna AP's with patch antennas as shown in the figure 39

3. User Density – Based on applications and client type a fixed number of clients can be supported per radio. If the number of users is high, more AP's may be needed to installed which will lead to reduced spacing between them

Adjacent channel interference can drastically reduce performance of the network and it should be avoided by:

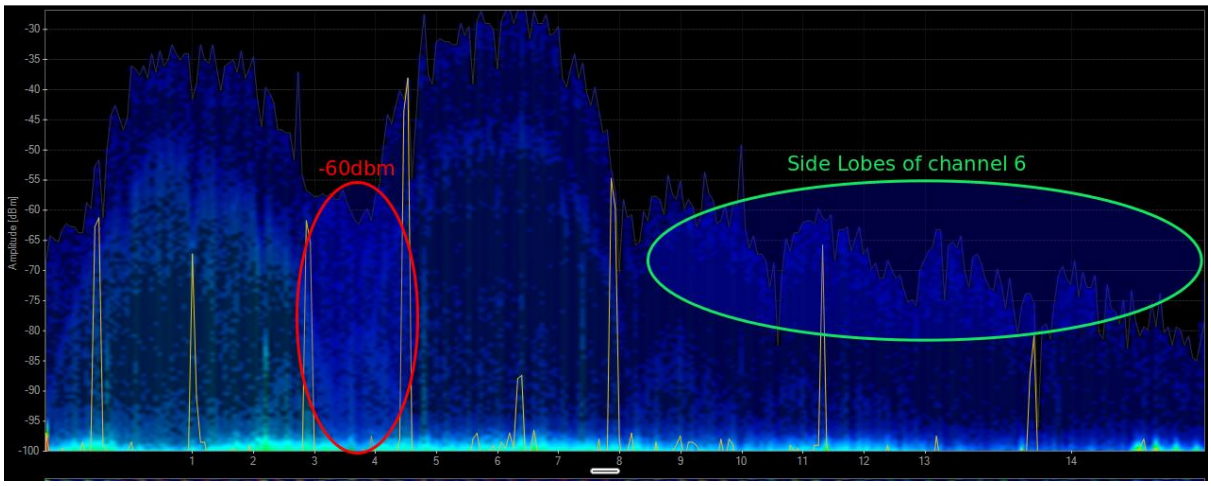
- Spacing AP's far enough
- Reducing AP transmit power
- Choosing the right antenna

The following figure demonstrates how AP's on neighboring AP's can interfere with each other



In this scenario a spectrum analyzer was placed equidistant from two AP's 10 feet apart. The power on both AP7532's (integrated antennas) was set to 4dbm. The interference between the side lobes should ideally be below -90. In this case it is -80dbm

In the following figure the setup was the same except the AP's power was increased to 19dbm. As seen below the interference level is significantly higher (-60dbm). A network with such high ACI will have very poor performance. Also notice the side lobes of channel 6



If the AP spacing is increased from 10' to 50' the interference level will drop. Based on this analysis, it is strongly recommended to reduce the power when placing AP's close to each other. Using a spectrum analyzer the interference can be determined and AP's can power or placement can be changed to compensate accordingly.

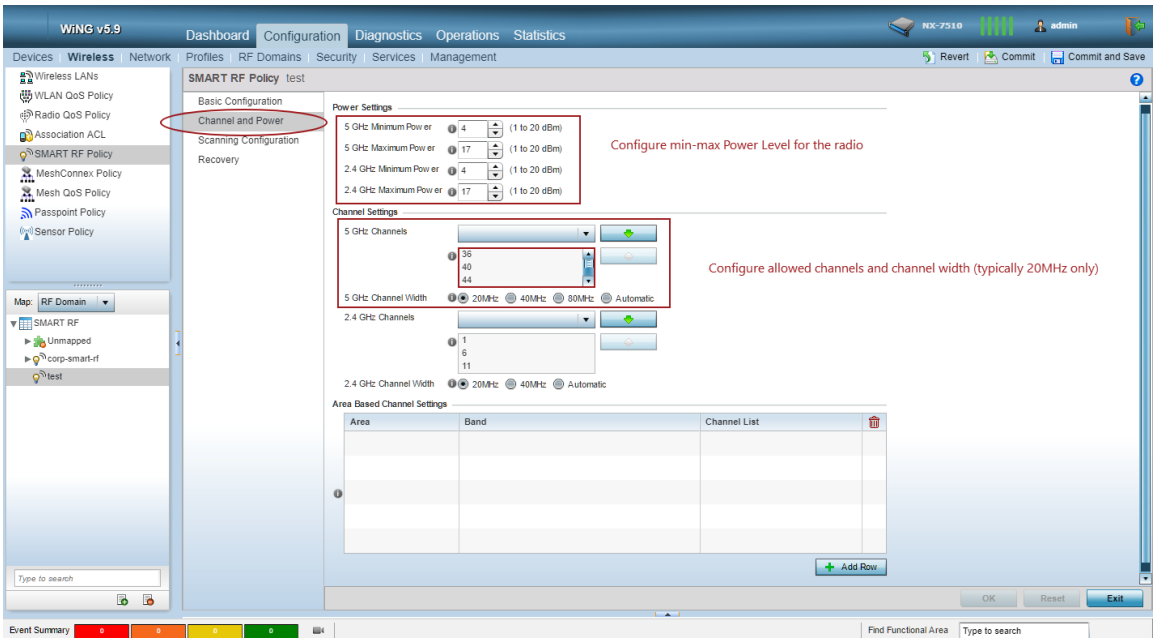
WLAN Network Optimization

Knowing the applications that are required to be supported and the type of client devices, the next step is to determine how to optimize the network for performance. Following are some features that should be exploited to ensure the network is being utilized to its fullest potential:

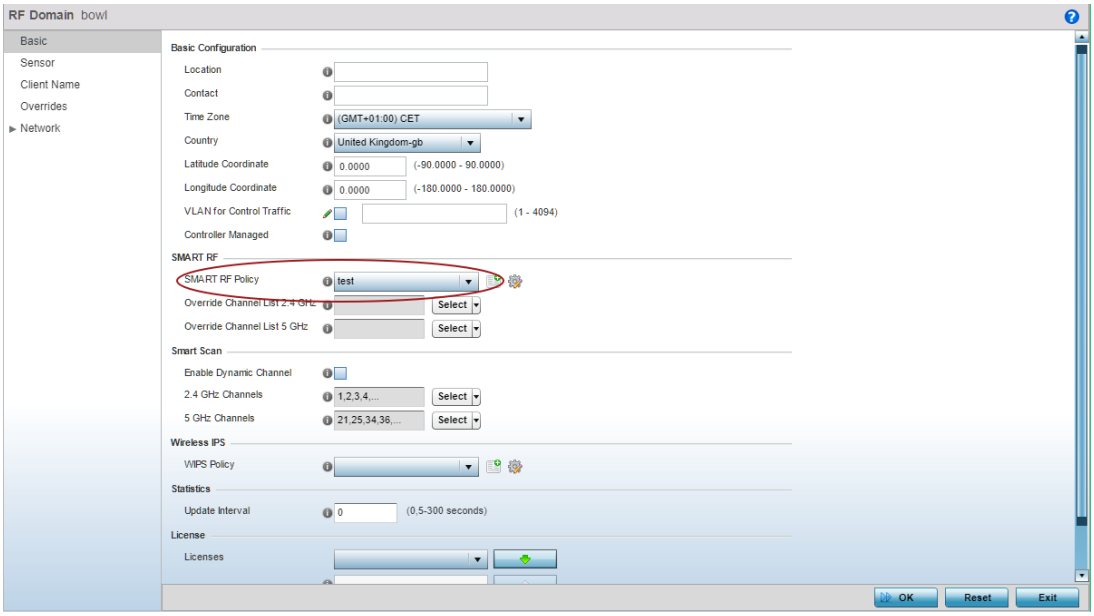
Smart-RF

The Smart-RF feature of WiNG 5 scans the environment and dynamically selects the channel and AP transmits power on which APs' would operate. This dynamic channel and power selection is made by considering factors like interference, ACI, CCI, noise, that would degrade the performance of the network. The Smart-RF feature can be used with a minimum of 3 neighboring APs'. In other words, for the Smart-RF feature to be implemented, each AP must see minimum 3 other neighboring APs' to make a real time dynamic AP Tx power and channel selection. The Smart-RF feature can be configured in WiNG 5 through the UI as shown below:

1. Navigate to Configuration → Wireless → Smart RF Policy and create a Smart-RF policy (e.g. test)
2. Configure the respective parameters as shown below and click OK, Commit and Save.



3. Make sure to click OK, Exit, and Commit and Save.
4. Map the created Smart-RF Policy to RF-Domain. Navigate to Configuration → RF Domains → <RF Domain Name> and select the Smart RF Policy under Smart RF section. This is shown in below figure.



Smart Load Balancing

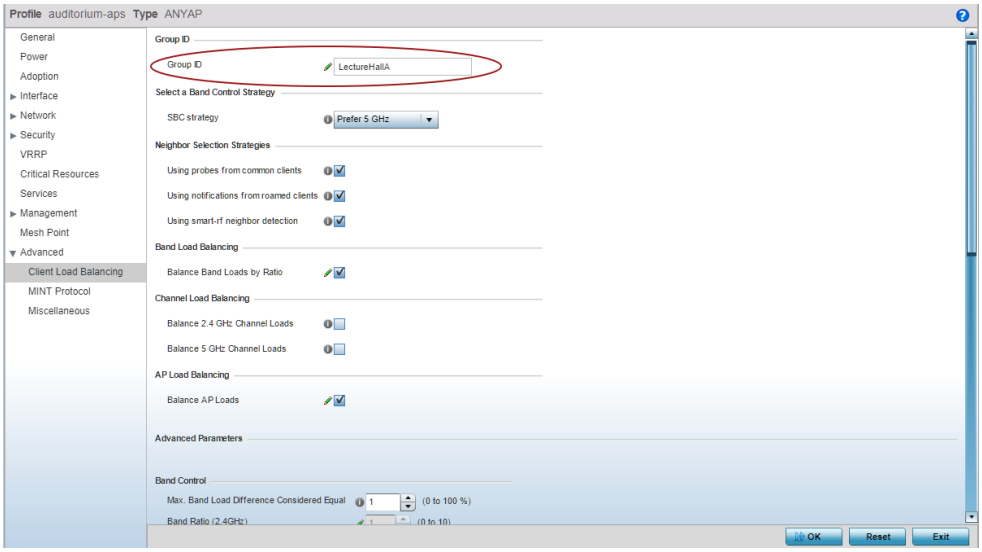
When all clients in a classroom/auditorium/stadium associate to the WLAN at once an AP can choke if there aren't algorithms to share the load across radios in a high density environment. WiNG Smart Load Balancing algorithm is designed to evenly spread the load across AP's

Since these AP's can share information with each other, they intelligently balance the client load amongst each other. This ensures all clients are connected on first attempt and there is no single choke point.

Without client load balancing there is a disproportionate distribution of clients across AP's leading to at least 14% less throughput when compared to client load balancing as seen in the figure above. This feature ensures all AP's are approximately evenly loaded hence maximizing the performance of the network.

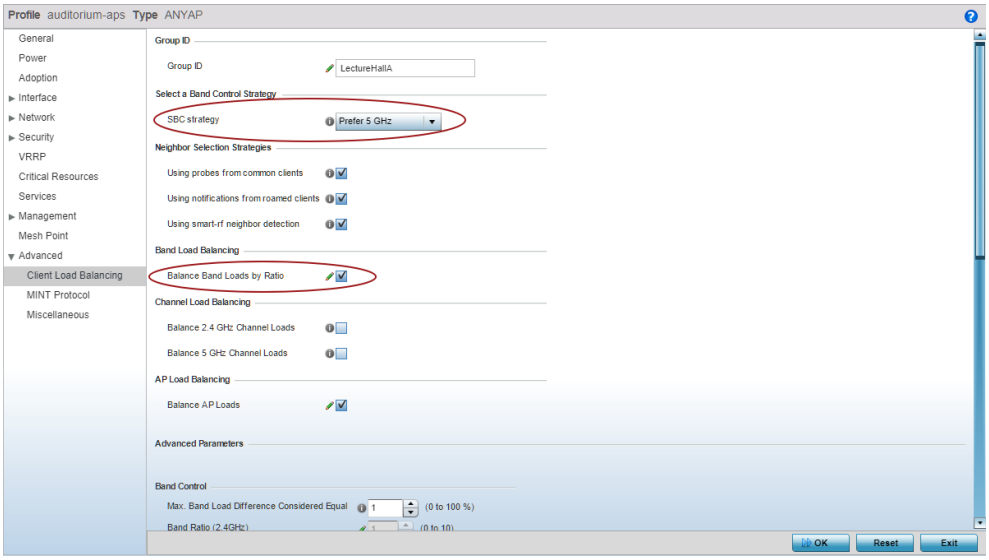
Following are the steps to configure Load Balancing:

1. Navigate to Configuration → Profiles → {Edit respective AP Profile} → Advanced → Client Load Balancing
2. Configure the following parameters:
    - Group ID – this should be a unique name to identify neighboring APs that should participate in Load Balancing Algorithm, for example "LectureHallA" or "SouthStand". This will prevent APs from adjacent areas or rooms to steer clients between each other.

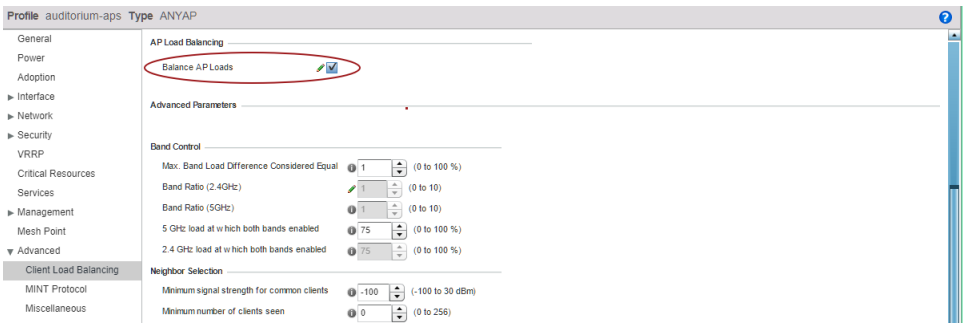


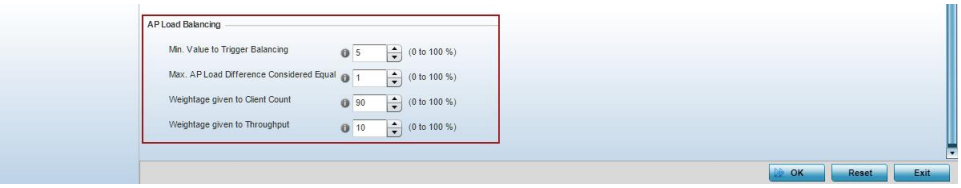
- Band Load Balancing – this parameter will enable Band Steering of clients. By default, it will try to move every dual-band capable client to 5GHz. It is also possible to set custom band steering ratio between 2.4GHz and 5GHz, which may be useful in some environments with less crowded 2.4GHz band. Generally speaking, in most of the public areas 2.4GHz band should be avoided at all cost, as people will bring their MiFi's, personal hotspots, non-WiFi transmitters that will destroy 2.4GHz band and make it unusable.

  Note: do not enable Band Steering on APs with only single radio enabled.



- Balance AP Loads – this parameter will enable AP load balancing based on a combination of traffic load per radio and number of clients associated per radio (90 vs 10 % weight by default, respectfully)





- Neighbor Selection Strategy – this is a very important parameter that determines how Access Points will consider its own neighboring APs for Load Balancing algorithm processing. By default, all 3 neighbor selection strategies are enabled by default, that are:
  - Using Probe Requests heard from common clients (i.e. if two APs can hear the same client probing at above "minimum signal threshold for common clients" level, these two APs will consider each other as load balancing neighbors, assuming they see at least at "minimum number of clients seen")
  - Using WNMP roam notifications from roamed clients
  - Using SmartRF neighbor table (i.e. based on the threshold on how well an AP can hear another AP)

What this means in practice is that by default CLB will work best with SmartRF enabled. By default, common clients selection strategy is disabled as you can see above since signal threshold is -100dBm with min clients set at 0.

WLAN Broadcast Optimization

In many deployments, especially with a huge amount of BYOD devices like in any high density public areas, there is always a big amount of broadcast and multicast traffic being generated by the wireless clients, as well as the wired network.

Most often than not, most of the broadcast/multicast traffic is not used at all, like for example IPv6 multicast being generated by an unconfigured IPv6 stack on the clients. Other great source of broadcast traffic is ARP. In 802.11 space both multicast and broadcast are treated the same*, i.e. this traffic must be broadcasted out of the radio using one of the basic data-rates. In WiNG by default all non-unicast traffic is being sent out using highest basic data-rate allowed in the configuration, which by default is 24 Mbps. This already helps to use precious airtime more efficiently. Additionally, thanks to the embedded stateful firewall functionality on the AP, WiNG has many more features to help in broadcast optimization, some of them are enabled by default, some of them should be enabled by the administrator for all hospitality deployments:

Limit the Number of SSIDs broadcasted per Radio

As an industry best practice it is strongly recommended to limit the number of advertised SSIDs per radio to a minimum (1 SSID ideally, maximum up to 3), since each advertised SSID requires an AP to send beacons, which are forwarded at the lowest basic rate and each beacon will require the AP to contend for the medium, reducing overall airtime.

For outdoor deployments a single SSID is recommended.

DHCP Offer Conversion

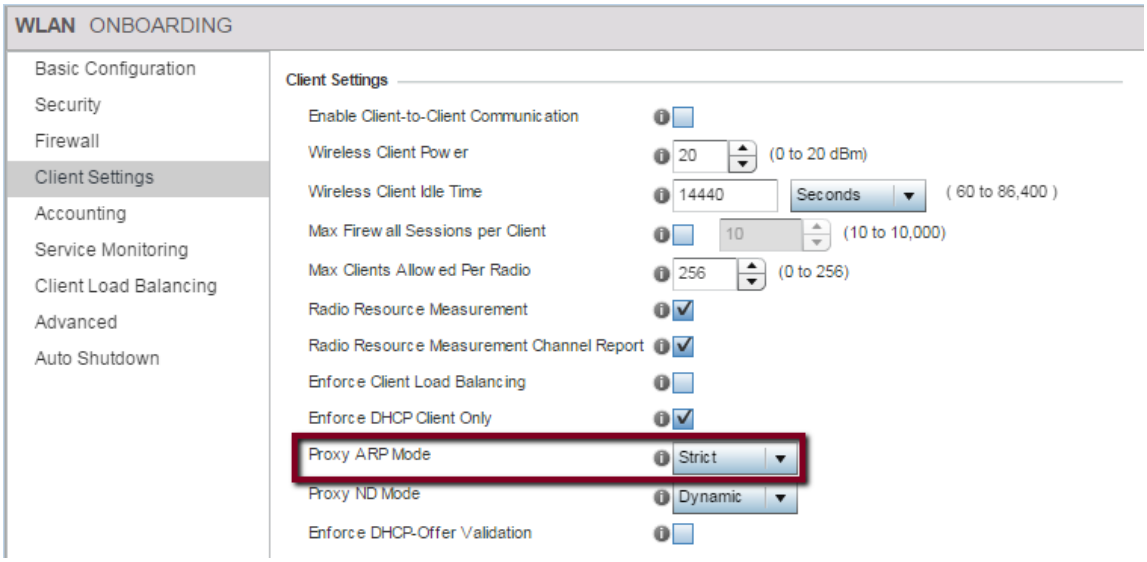
Broadcast packets go at the basic rate which is detrimental to a wireless network. The higher data rate packets suffer when more and more broadcast packets are on the air. With DHCP offer conversion, broadcast DHCP offers from the DHCP server are converted to unicast. This unicast packet will not get flooded and go at the highest data rate thus contributing to good network performance. In large client deployment scenarios this is a useful feature.

Proxy ARP

Just like DHCP Offer, ARP packets are broadcast. With the Proxy ARP feature the infrastructure can send proxy for ARP requests for other devices if they know their MAC address.

Proxy ARP allows wireless controllers and access points to respond to ARP requests on behalf of wireless clients. In this way, clients do not have to wake up to respond (which saves client battery life!), and ARP requests will not be forwarded to the air, which will dramatically improve overall airtime. It is enabled by default in the default and user defined firewall policies.

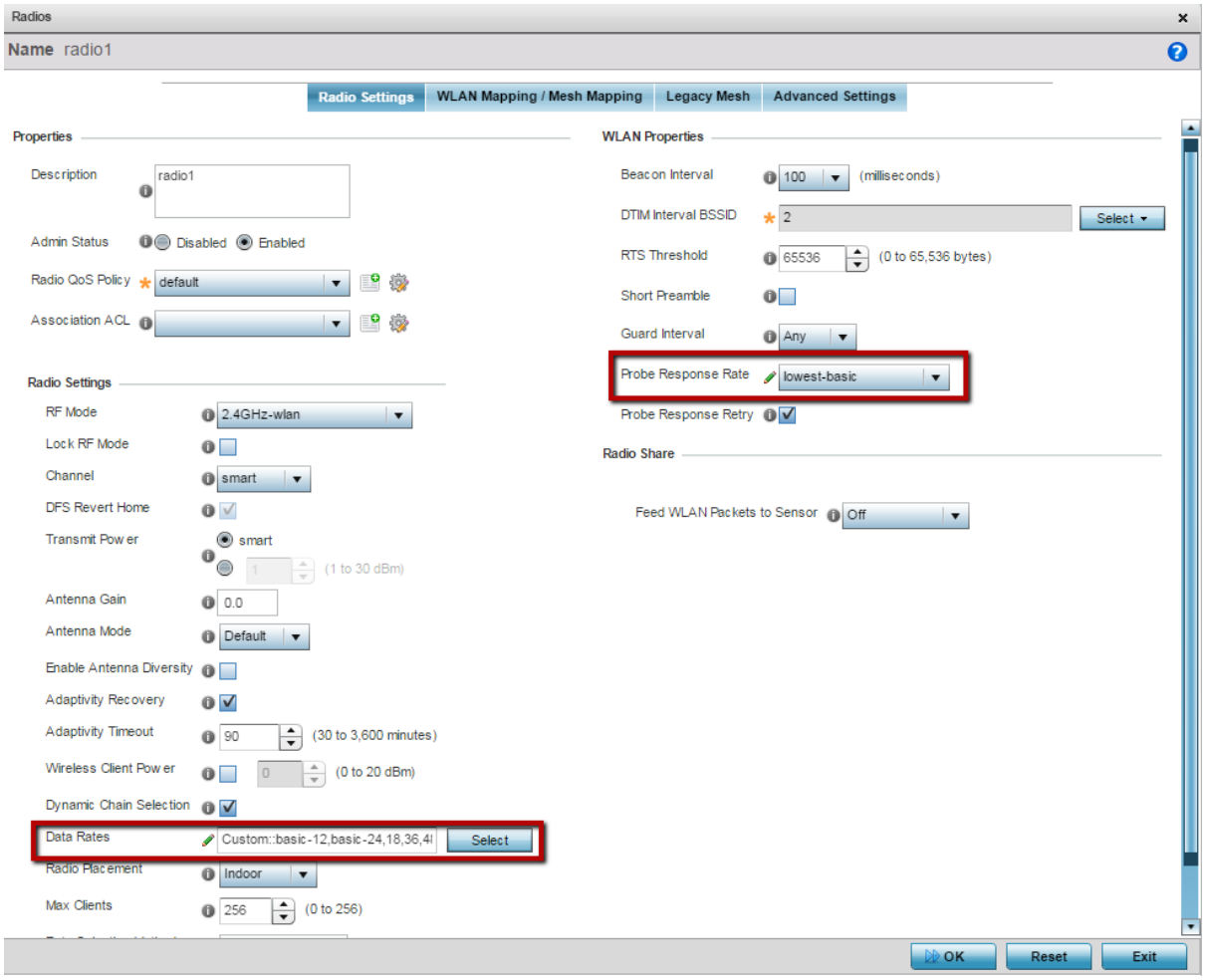
Additionally, it is recommended to enable *strict Proxy ARP* under all WLANs where no clients with static IP addresses are in use. This will prevent any misconfigured wired or wireless device from flooding the wireless network with never ending ARP requests:



Probe Response Rate & Radio Data Rates

Even if data rates are adjusted at the profile to exclude legacy rates, clients will still probe at the lowest supported rate for that device type; this is always 1 Mbps. Within the device profiles of WiNG 5, at the device level, there is a parameter called `probe-response rate`. The default is to respond at the same rate received by the client, which would be 1 Mbps. Changing this parameter to `lowest-basic` means that probe responses will be at the lowest data rate configured for the WiNG 5 devices, which would be 6Mbps rates if we follow the recommendation mentioned previously. This will reduce lowest rate traffic by up to one-half, and further optimize overall throughput.

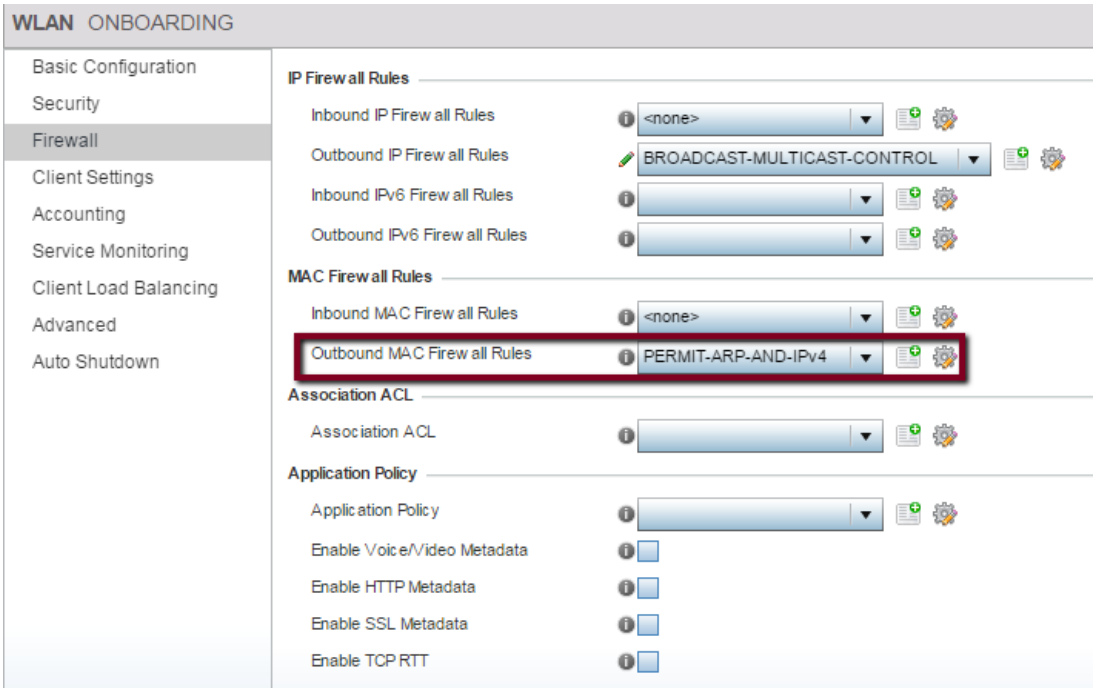
Also note, that in high density environments with plethora of clients per radio, the most impact on the performance and overall throughput comes from the 802.11 control traffic. Typically, it is sent using basic data-rates (i.e. mandatory rates). By default, WiNG forwards control traffic using highest basic rate allowed on a radio or SSID



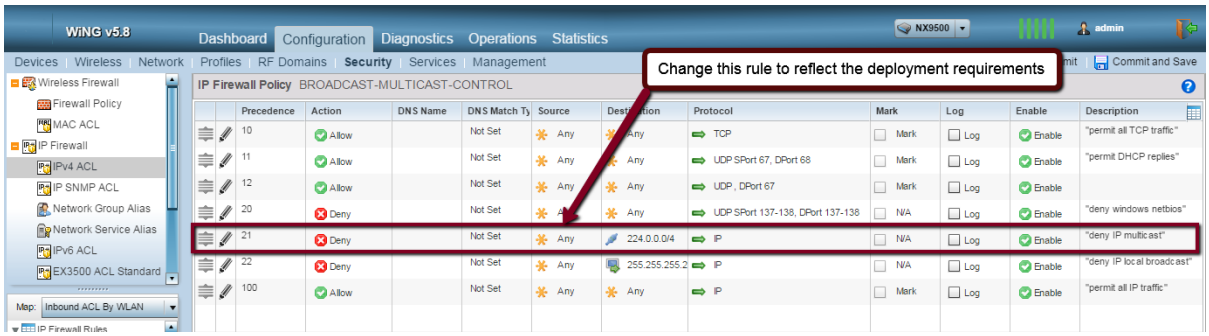
Default IPv4 and MAC Access Lists

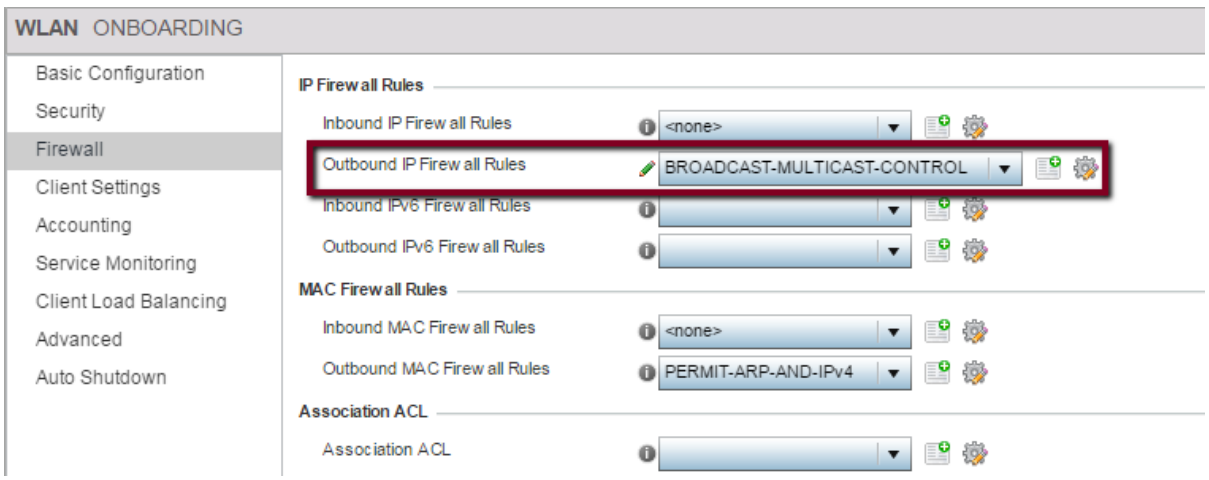
By default, in WiNG configuration there are two pre-defined Access Lists that can be attached to the WLAN in the outbound direction to help with optimizing the amount of broadcast and multicast traffic that is being forwarded to the air.

One of them is the MAC Access List named “PERMIT-ARP-AND-IPv4”. This MAC ACL will only allow ARP and IPv4 traffic, as the name suggests. It is very useful in mitigating excessive IPv6 multicast coming from the unconfigured clients that only use IPv4. It should be assigned to all WLANs outbound direction to prevent IPv6 multicast flood to go out of the radio, therefore saving the airtime:



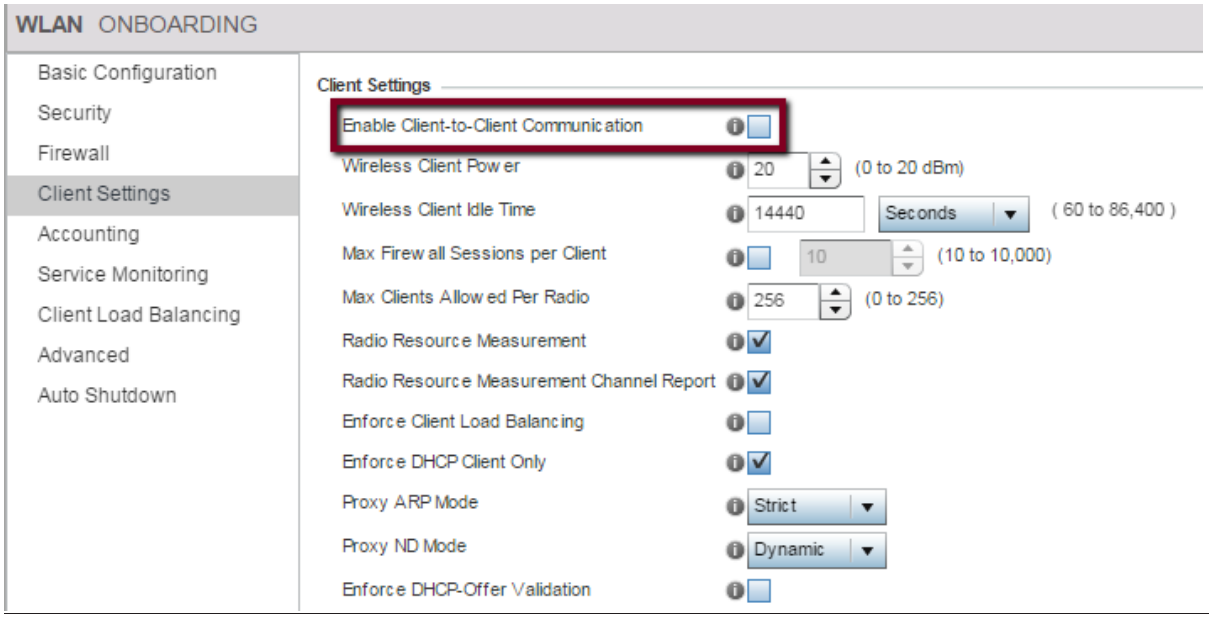
Another ACL named "BROADCAST-MULTICAST-CONTROL" can be leveraged to block unwanted IPv4 multicast to be forwarded to the airspace. A good example is a VRRP update. Typically, VRRP routers send updates on a LAN as Multicast up to few milliseconds, which generates enormous amount of broadcast traffic from the wireless perspective, as by default it must be forwarded out to the radios. It is important to note that by default BROADCAST-MULTICAST-CONTROL ACL will block all IPv4 multicast. In hospitality environments, there is a need to IPv4 multicast, such as Google Chromecast, Apple Bonjour etc. Therefore, it is advised to either – allow all IPv4 Multicast and block the traffic that should not go out (like VRRP) or block all IPv4 Multicast and allow only specific IPv4 Multicast addresses or ports to be forwarded (like Chromecast/Bonjour):





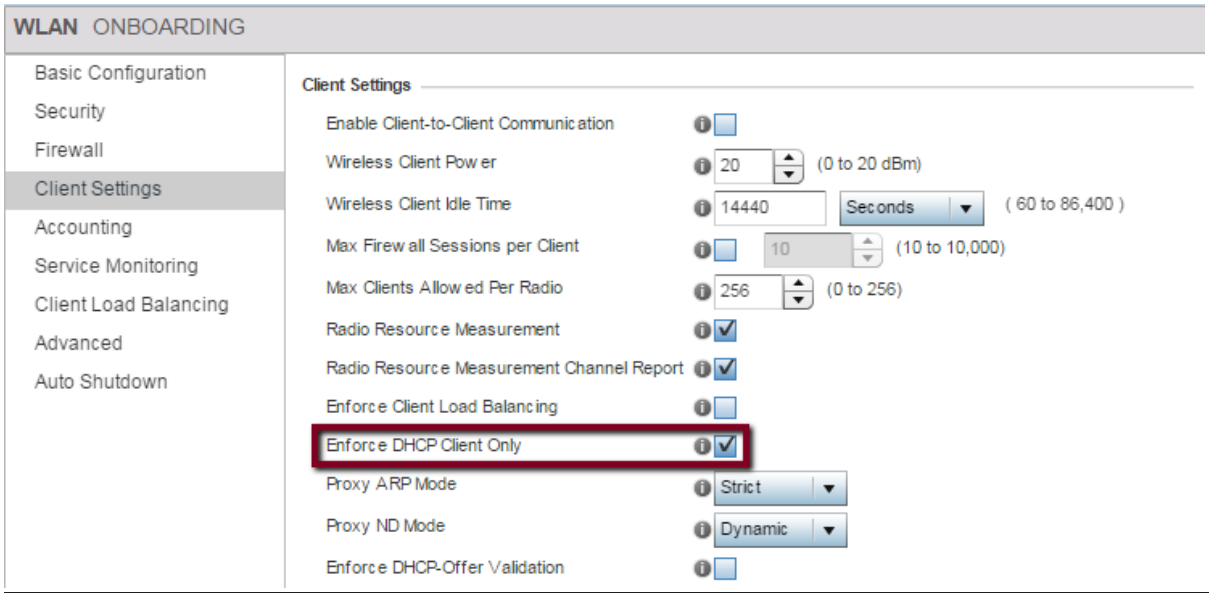
Client to Client Communication Block

As a general security recommendation, it is required to disable all peer-to-peer communications on the guest network to prevent guest clients from talking to the each other. In WiNG thanks to the distributed nature of the firewall it is possible to do that across all APs with either tunneled or locally bridged traffic forwarding:



Enforce DHCP-Only Clients

In some cases, there may be clients on the network which were misconfigured with the static IP address. When these clients attach to the network, not only they have no access to the network itself, they generate a lot of ARP traffic flooding the wireless space. To prevent such misconfigured wireless clients from associating with the guest networks it is recommended to enabled DHCP client enforcement on the WLAN:



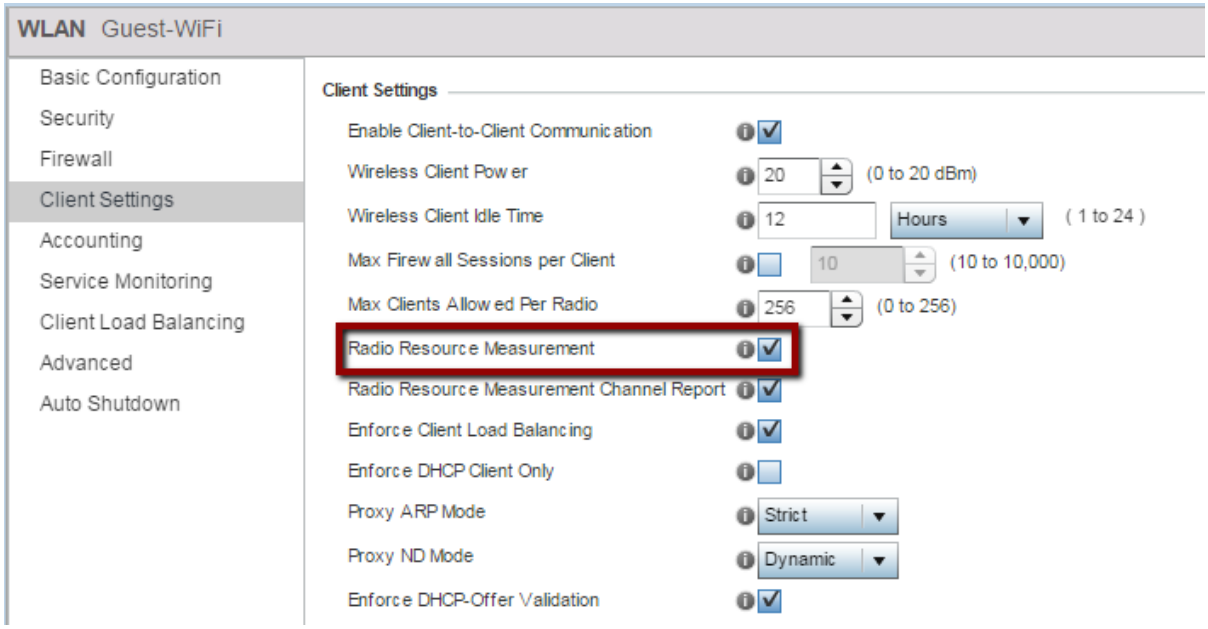
Client Association Control

Radio Resource Management (802.11k)

Devices moving away from an AP face a potential roaming decision, but per the original Wi-Fi standard it was left up to the client to find candidate APs and decide which one to roam to. The 802.11k standard enhances this process by allowing clients to request a list of neighboring APs from the current AP they are associated to. This list narrows the potential candidates and channels the client needs to consider, and speeds up the roaming process. It also reduces the amount of probing, probe responses, and other management traffic that is sent at

the lowest BRS. Newer smartphone/tablets and OS versions typically support 802.11k (iPhones / iPads, most of the Android devices starting with KitKat), as does WiNG 5.

By default, 802.11k is disabled on the WLAN context for compatibility reasons for legacy devices, but it is recommended to enable it for any kind of public guest networks to help mobile devices find neighboring APs faster.



Roaming Assist

Roaming Assistance is a feature in WiNG5 platform to address the issue of “sticky client”:

- Some clients do not roam despite moving away from current AP
- This impacts their wireless experience negatively
- And impacts clients nearby because they are wasting airtime (lower data rates and higher retries)

It is recommended to utilize Roaming Assist feature in a Guest Access network environment when hundreds of unknown client types are present with different behavior, which might affect overall performance.

With roaming assist the client initially associates with an access point which it hears first or the access point with best signal strength. As soon as the wireless client moves away from the access point, its signal strength drops. Roaming Assistance keeps a continuous check on wireless clients by sampling the client’s signal strength at configured intervals. Once the client’s signal strength crosses the configured threshold, Roaming Assistance starts monitoring the client aggressively. If the client’s signal strength is consistently below the threshold for a small interval, Roaming Assistance triggers an action to force a client to roam and directs the client to find the best AP. When the client now looks for an access

point, only the access point with the minimum load and a minimum signal strength threshold will respond to the client. Roaming Assistance helps clients to initiate a roam as the signal strength degrades and find the best access point with which to associate.

Roam Assist feature has two different actions available to trigger once handoff-threshold is reached:

1) Legacy Roaming Assistance (action "deauth", pre-5.8.0)

AP will send a de-authentication frame to the client, forcing it to find a better AP. While the client will move to the new AP eventually, this is not a roam (re-association), but a new association. Once client will receive the deauth frame all firewall sessions for this client will be purged by an AP. This type of handoff is intrusive and will break current sessions. It is not recommended to use in enterprise environment for corporate devices, but it's a good compromise in guest networks to maintain the level of service to majority of the clients

2) Assisted Roam (action "assisted-roam", post-5.8.0)

Instead of sending a *de-authentication* message to the sticky client, the client is requested to perform a graceful roam using the 802.11v *BSS Transition Management Request Action Frame* to the client. The message provides a list of roam candidates to the client (candidate AP list is built from the 802.11k neighbor report).

The Client has 3 choices:

Client can Accept the request and select an AP from the list provided in the transition request.

1. Accept the Transition request, but start its own roam scan to select an AP
2. The client can *Reject* the request

If Client accepts the request it will then perform a graceful roam with no impact to the running sessions

Clients must support 802.11k and 802.11v to be able to fully leverage this feature. Client support can be checked by enabling `debug wireless client rasst level debug` on the Access Point. This mode is also backwards compatible to clients that do not support 802.11v and 802.11k.

Configuration is available in CLI only:

```
!
roaming-assist-policy RASST
 aggressiveness medium-low
 detection-threshold -70
 handoff-threshold -75
 action assisted-roam
!
wlan GUEST-WiFi
 ssid GUEST-WiFi
 vlan $GUEST
 bridging-mode local
 encryption-type none
 authentication-type none
 radio-resource-measurement
 802.11v bss-transition
 assoc-response rssi-threshold -82
 assoc-response deny-threshold 3
 use roaming-assist-policy RASST
!
```

Probe Response Threshold

Probe Response RSSI threshold: (3 dB less than handoff threshold). The probe response RSSI means the access point will respond to wireless client's probe request only if their signal strength is greater than the probe response threshold. This ensures that only APs in close proximity to the client will response to active discovery, saving airtime on a channel and giving better options for the client as well

Configuration is available in CLI only under Radio Interface:

```
!
profile ap8533 stands
 ...
 interface radio1
  wlan Guest bss 1 primary
  no dynamic-chain-selection
  probe-response rssi-threshold -72
 interface radio2
  wlan Guest bss 1 primary
  no dynamic-chain-selection
  probe-response rssi-threshold -72
 ...
!
```

Association Response Threshold

Association response RSSI threshold: (3 dB less than handoff threshold). The associate response RSSI means the access point will respond to wireless clients only if their signal strength is greater than -72 dBm. This ensures when the client roams from the current access point due to Roaming Assistance, the same access point does not respond back to the client's association request.

Configuration is available in CLI only under WLAN:

```
!
wlan GUEST-WiFi
 ssid GUEST-WiFi
 vlan $GUEST
 bridging-mode local
 encryption-type none
 authentication-type none
 radio-resource-measurement
 802.11v bss-transition
 assoc-response rssi-threshold -72
 assoc-response deny-threshold 3
 use roaming-assist-policy RASST
!
```

Estimating AP Count Example

This section covers a real world high density deployment scenario using the design principles discussed earlier in the document. Following is the requirement defined by the customer:

> ABC School district wants to adopt video based teaching methodology in all of its auditoriums. The auditoriums are identical and have a capacity of 300 students. Each student will be given an iPad and asked to watch online videos. At the end of the video students will answer multiple choice questions. Each video will be YouTube-style and encoded at 1Mbps. Video will be the primary application and web browsing will be secondary.

Given this problem definition the we can apply the design principle to come up with an AP count. Let's first define the known parameters:

Step 1: Define Applications

Based on the requirement we know video is the main application. Using Network management tools and sniffers it has been determined that the application sends TCP frames

Application Throughput (AT) = *1Mbps*

Application Type (YouTube Style) = TCP

Step 2: Identify Client Types

The requirements spell out iPads being the clients. iPads are single stream clients that support

65Mbps data rates. Client Type = *65 Mbps capable*

Estimate Network Throughput

The defined application is downstream TCP. A quick IPERF TCP test with a single client yields the Aggregate Network Throughput of the client

Aggregate Network Throughput (ANT) = *40Mbps*

Predict AP Capacity

Following the Flow Chart in Figure 8, we can now calculate the total AP Count:

> Base Client Count (BCC) = ANT / AT = 40 Mbps / 1Mbps = 40 clients
>
> Client Count (CC) or FCC = BCC x CF = 40 * 0.8 = 32 clients

Hence a maximum of 32 iPads can be associated with a single radio.

> Access Point Count (APC) = Expected # of Clients / 2* FCC = 300 / 64 = ~5

5 Access Points will be needed for this deployment

Terms & Condition of Use

Revision History

Date	Revision	Changes Made	Author
17th November 2017	1.1	Minor updates	Slava Dementyev