



best practice
design guide

Deploying Very High Density Wi-Fi

DESIGN AND CONFIGURATION
GUIDE FOR STADIUMS



Table of Contents

Intended Audience	3
Overview.....	4
Design Process Overview	5
Discovery	5
Initial customer meetings to determine:	5
On-site Visit	5
First physical visit to the site to determine:.....	5
Wi-Fi Design	5
Installation	6
RF Survey.....	6
Testing & Acceptance	6
Coverage vs. Capacity in Very Dense Environments.....	7
Why Are Stadiums Different?	7
5 GHz: The Future of Wi-Fi	8
Decreasing Cell Size	9
Breaking Away from Traditional 2.4 GHz Channel Plans	9
RF Simulations	10
Configuration Optimizations.....	10
What About Reducing Transmit Power?	10
Capacity Optimization.....	11
Summary.....	11
Performance Requirements.....	12
Understanding the Applications.....	12
Other Performance Factors	12
Reference Design Example.....	13
Key Performance Indicators (KPI)	13
Application Types and Metrics.....	14
Latency and Jitter	15
Signal Quality	15
The Impact of Client Devices.....	15
Correctly Sizing Client Load	15
Client Capability.....	16
Estimating Goodput	17
RF Interference	18
Wi-Fi	18
Non-Wi-Fi.....	20
Guidelines for Performance.....	22
Estimating Client and AP Counts	23
How many clients can I connect to a single AP?	23
Estimating the Number of Client Devices.....	23



Stadium Example:	24
Estimating the Access Point Association Limit	25
Estimating Access Point Throughput	25
Stadium Example.....	25
Estimating Clients per AP Capacity	26
Estimating Additional APs	27
Distance from AP to Client.....	27
Guidelines for Estimating Capacity	28
AP Installation and Hardware	29
Antenna Selection	29
AP Hardware Selection	31
Signal Attenuation	31
AP Mounting Locations.....	32
Guidelines for AP Installation and Hardware	34
Configuration Optimizations	35
Client Load Balancing.....	35
Channelfly.....	36
Channel Width.....	37
AP Transmit Power	38
A word about minimum power settings	40
Rate Limiting.....	40
OFDM and CCK Rates.....	41
Background Scanning.....	43
Maximum Clients per Radio/WLAN	45
Open vs. Encrypted WLANs.....	46
Intrusion Detection	47
Limiting Broadcast Traffic	48
Client Isolation	50
Summary.....	51



Intended Audience

This document addresses factors and concerns related to very dense Wi-Fi environments such as stadiums. Because venues can differ radically, it is impossible to develop a single approach that adequately addresses all potential design and installation issues.

This document is written for and intended for the sole use of system integrators or professional services with significant background in Wi-Fi design and 802.11/wireless engineering principles. This document is not appropriate for end-user design work without the help of an experienced professional services team.



Overview

As more Wi-Fi capable devices enter the market the average number of devices in any given area of a network increases. In the case of extremely dense venues such as stadiums or exhibit halls, these very dense populations can introduce significant stress on the network and require specific design considerations. There are a number of factors that can impact a very high density environment, including:

- Performance requirements
- Number and density of APs
- Number and density of clients
- Wi-Fi capabilities of clients
- Current RF environment
- AP hardware
- AP mounting

Each of these conditions can potentially cause severe network degradation. This document addresses ways to mitigate these negative performance issues and increase overall performance and network stability. There are many types of high-density environments and each may have its own unique requirements. This guide will focus exclusively on very dense environments such as those found in stadiums, arenas, large exhibit halls, etc. These environments have unique properties that are not found in other Wi-Fi deployments.

Note: other high density applications such as school classrooms and smaller convention center venues should use the "Best Practices: High Density Design Guide" from Ruckus Wireless instead.

The rest this document will examine each of these points in-depth and offer guidelines and suggestions for optimized very high-density design configuration with Ruckus wireless equipment. Where needed, specific configuration commands are documented for step-by-step configuration instructions.



Design Process Overview

Although specifics can vary, any design team is expected to be familiar with the following process and tools. These are required for a successful design and deployment.

Discovery

Initial customer meetings to determine:

- Venue specific documentation (CAD drawings, photos, cabling maps, etc.)
- Expected capacity (users)
- Supported applications
- Key Performance Indicators (KPIs)
- Coverage areas
- Client devices that need to be supported

On-site Visit

First physical visit to the site to determine:

- Walkthrough of coverage areas
- Confirm accuracy of received documentation
- Confer with venue representative on places that cannot be used for mounting positions and other potential issues (I know you said something above but this is more specific)
- Gather additional intelligence, i.e. where are the VIPs and what type of events occur there. What type of events would need special wireless services or to have the Wi-Fi turned off because of exhibitors' equipment running on same frequencies.

Wi-Fi Design

All of the information previously gathered is used to do a simulation of the venue. This is used to create an initial design including:

- Bill of materials (BOM) for the wireless network
- BOM for supporting equipment (wired network build-out, conduit, wire hangers, etc.)
- Installation locations for equipment
- Hardware/workers required for installation (cherry pickers, etc.)
- Estimated coverage and capacity report



Installation

After the design is approved, the equipment is procured and installed at the venue. This needs to be coordinated with the venue manager as to not interfere with the primary functions of the venue. Sports teams may have strict guidelines as to when access will be granted and when workers may not be in the building. Also there will be a requirement for the project completion. This schedule will be very important to define so that all parties will have their portions of the project ready for installation at time required. Any delays here can cause long delays in completing the project and cause friction with the venue management or owner.

RF Survey

Once the equipment is installed, the design model is verified against the deployed environment. This step consists of a follow-up visit to site to conduct actual RF testing and initial design validation.

Testing & Acceptance

This consists of on-site validation and confirmation of the initial design goals and success criteria.



Coverage vs. Capacity in Very Dense Environments

Why Are Stadiums Different?

Most Wi-Fi networks are designed for offices, public buildings, schools, warehouses, hospitals, etc. These sites typically require a wireless network that is optimized for good capacity with a fairly large coverage area for each AP.

Very dense venues such as stadiums have very different requirements that break this model. These deployments feature a very large number of people and devices within a large but highly concentrated area where much of the network, users and Access Points are LOS to each other. What works in an office will definitely **not** work in a stadium. The key difference is capacity.

Very high-density designs require new thinking, see Table 1.

	Coverage	Capacity
Number of APs	Prefer low	Prefer high
Limiting factor	Path loss	Interference
Obstacles	Bad	Good
RF frequency	Lower is better	Higher is better
Antenna pattern	Omni is better	Sector is better
AP placement	Higher is better	Lower is better
Design metric	SNR area	SINR area

Table 1



The most significant factor in very dense deployments is the need to support a large number of people packed very closely together. The large number of people and devices requires a large number of APs that are also close together. But placing that many APs so close together brings its own challenges; namely increased RF interference.

RF interference is a huge driver with immense impact on the final design. Fortunately, there are some strategies to help mitigate its effect. These include:

- Increased use of 5 GHz RF spectrum for less interference and more channels (capacity)
- Shrink AP cell sizes as much as possible
- Increase AP count, but only to the extent of estimated capacity (more is not better).
- Understand required capacity to avoid over-building network (increases interference unnecessarily)
- High frequency re-use
- Via directional antennas
- Structural separation and attenuation
- Non-traditional 2.4 GHz channel plans
- RF simulation tools to optimize design before final design or installation
- Configuration optimizations
- Adaptive algorithms to handle changing RF conditions without manual intervention

5 GHz: The Future of Wi-Fi

Increased use of 5 GHz is on the rise; newer clients are usually dual-band meaning they can use either 2.4 GHz or 5 GHz. This is true even of newer smartphones as well as tablets and laptops. This trend is expected to accelerate as device vendors position themselves to support 802.11ac, which only operates in the 5 GHz spectrum. All of this has positive implications for Wi-Fi.

5 GHz is preferred for several reasons, not least of which include a wider frequency spectrum. This band typically offers 6 to 7 times the bandwidth of 2.4 GHz in most countries. With a larger amount of spectrum comes more non-overlapping channels. As the number of available channels increases, the opportunity for channel re-use goes up. Channel re-use is the frequency with which a single channel can be used again by other APs without causing undue co-channel interference. Unlike 2.4 GHz which only has 3 non-overlapping channels (and therefore a frequency re-use factor of 3), 5 GHz supports re-use factors of 4, 7, 9 or even 12 or higher. Smaller channels reused more times will give more capacity than larger channels reused less often.

Higher channel re-use has huge implications for very dense deployments because it reduces the limiting factor of co-channel interference. A higher re-use factor increases the number of APs, which is necessary to meet capacity demands. This equates to 8 – 10 times increase in Mbps/m² over the 2.4 GHz band.



Decreasing Cell Size

Each AP in a wireless network represents additional capacity. Large venues demand very high capacity and therefore far more APs than would be required for a strictly coverage-oriented model. Therefore, the goal of a very dense deployment is very small AP coverage (cell) sizes.

Keeping cell size to a minimum requires placing APs as close to the users as possible and keeping them isolated from other APs. Isolation is achieved via non-overlapping channels, structural isolation (attenuation or blocking of signals) and directional antennas to keep the coverage area small.

Breaking Away from Traditional 2.4 GHz Channel Plans

Although 5 GHz is becoming more popular, 2.4 GHz-only clients will be around for a long time and must be supported. But very dense deployments are not 2.4 GHz friendly due to the requirement for high channel re-use and minimal interference. Traditional 3 or 4 channel plans are not good enough.

2.4 GHz is vulnerable to RF interference both Wi-Fi and non-802.11. In an urban environment, the vast majority of interference comes from neighboring Wi-Fi networks. These networks prefer 3 channel plans (1, 6 and 11), which are the only non-overlapping channels available in this band. There can also be interference from the concession areas because of the use of microwaves for food preparation.

It is very easy to dismiss these neighboring networks because they appear usually appear at very weak signal strengths in the target venue. But lower power has worse implications for new 2.4 GHz deployments. The reason is most of these APs are using the minimum transmission rate (1 Mbps) for beacon and management frames. Therefore there is a constant sea of low power, low speed traffic almost everywhere.

This traffic is completely irrelevant to the venue network and is received at a very low power. The simple solution is to increase power on the venue APs; that is easily done. But higher power doesn't solve the intrinsic problem with co-channel interference: preambles.

A preamble is the first part a frame transmitted by a Wi-Fi client. It is used by a station to tell the AP it's about to transmit. It does not contain much useful information but it is required by the standard. In the 2.4 GHz band there is a "legacy" long preamble and a shorter preamble. All 802.11g 2.4 GHz stations are required to support both. Not only do long preambles take longer to transmit, they are always sent at the lowest possible speed (1 Mbps).

Traditional networks can only solve this problem by trying to be on a different non-overlapping channel. But since there are only 3 in the 2.4 GHz band, this is not realistic. A better solution is to make use of the other channels. These channels do overlap with traditional plans but have a huge benefit: clients that are on these channels do not hear stations on channels 1, 6 or 11. A client on channel 7 does not need to pay attention to a neighboring network transmitting on channels 6 or 11. It freely ignores these irrelevant preambles.



RF Simulations

Unlike most other (indoor) deployments, large venues incur significantly higher installation costs. A stadium does not have as many available installation locations as an office and they are much more difficult to reach. Because of this, there is a much higher incentive to know exactly where to put the AP before it is installed. Cherry pickers are expensive to procure and use; installing new cable runs is also costly compared to a more standard indoor environment. Many venues require that all cabling is placed in conduit which further increases cost and makes proper the next step so important.

The only way to solve this problem is with the use of sophisticated RF simulation software used by knowledgeable designers and engineers. These predictive models help determine the most advantageous locations before a single AP is deployed. This reduces the possibility of later costly adjustments.

Configuration Optimizations

Overall performance is further improved with the use of configuration adjustments that help with the unique requirements of large venues. These include:

- OFDM only in the 2.4 GHz band (drop support for 802.11b clients)
- Disable background scanning by APs
- Enable RTS-CTS to mitigate collisions
- Limit the number of SSIDs as much as possible to reduce management traffic and overhead
- Disable any service that may potentially deny service such as WIPS

What About Reducing Transmit Power?

A common tactic used to shrink AP cell size and reduce interference is lowering the AP transmit power. But this rarely has the desired effect. Reducing power might lower contention on the medium, but there are better ways to do this. Ruckus products use a dynamic, adaptive antenna array that automatically steers around interference and does not transmit extraneous RF outside the targeted client area.

Lower power also doesn't reduce the signal to self-interference ratio. Even worse, it is guaranteed to reduce the signal to noise ratio from neighboring interference. This only makes things worse for clients, which will now have a harder time hearing the AP. Reducing power also lowers the transmit speed to the clients. This means they spend more time on the air listening; further reducing capacity.



Capacity Optimization

Capacity is critical for large venues. Incorrectly estimating capacity can result in poor performance and coverage holes from insufficient APs. On the other hand, overestimating the number of APs does not make clients perform better it just increases interference unnecessarily. This ultimately reduces capacity. Capacity is a key part of RF simulation software such as iBwave or Motorola's Enterprise Planner. These packages include capacity estimation metrics – in particular, the percentage of coverage area that provides a SINR of at least 25 dB or greater and this is key.

This percentage should be verified for individual sections of the venue and then iterated across the entire coverage area. Every area must be accounted for in the design before a final signoff.

Summary

This section described key elements of design vital for deployment of very large and dense Wi-Fi networks. The rest of this document delves into these topics in greater detail and explanation. Unlike a standard indoor deployment, large venues must meet all of these requirements and have them carefully validated at every step in the process. Each step is critical because errors in the design are magnified and have much larger impacts than other most other wireless deployments.



Performance Requirements

Understanding the Applications

The first thing that any high-density design should determine and document are the key performance metrics. These applications can include general internet access, voice (VoIP), video, food service, ticketing, just to name a few. The service requirements for these applications define the minimum device requirements for successful operation. These are vital to calculate the number of devices per AP and, from that, the number of required APs.

Other Performance Factors

The second significant part of the design is the number of APs required to meet the KPIs. This number is critical but cannot be determined based on KPIs alone. There are several other factors that will impact overall performance, AP capacity and consequently the number of APs. These factors include:

- Number of devices expected on the Wi-Fi network
- Type of device that will be utilized, scanners, handsets, tablets, etc.
- Device capability
- RF interference

Reference Design Example



The easiest way to show how these factors can be derived and used is by example. The rest of this document will use a 20,000-seat stadium as a reference design. As with any high-density venue, specific deployments may have slightly different requirements. However the principles outlined here are applicable for any size venue.

Venues rarely have a single application and a single type of user. Instead, there are typically many groups with specific requirements, applications and coverage needs. This document addresses the most common or significant criteria for a successful deployment.

Key Performance Indicators (KPI)

KPI metrics are the ultimate measure of a successful deployment. Therefore they should be as accurate as possible. Under estimating requirements will result in poor performance and a design that does not meet required needs. Over estimating could potentially result in a network that is so large it interferes with itself and reduces overall capacity.

Common KPIs include:

- Type of applications that will be supported
- Minimum bandwidth required to satisfy supported applications
- Minimum, maximum and average number of Wi-Fi enabled devices
- The expected number of active Wi-Fi devices at peak traffic time.
- Maximum latency and jitter tolerated
- Service area definition



Application Types and Metrics

Supported applications may vary depending on the venue and on the intended audience. For example, guest attendees are usually offered web and email while venue employees use ticketing or point of sales (POS) applications. Table 2 illustrates common applications as well as their specific performance requirements:

Supported Applications by Group/Application

Group	Applications	Minimum Bandwidth	Max Latency Tolerance
Guests/attendees	Web access Email Video playback	~ 300 Kbps ~ 200 Kbps ~ 500 Kbps	Medium High Medium
Ticketing	Ticket scanning	< 200 Kbps	High
Services (Restaurants, etc.)	POS	Determined by application	Determined by application
Venue staff	Web access Email VoIP	~ 300 Kbps ~ 200 Kbps ~100 Kbps	Medium High Low
Guests/attendees	Web access Email Video playback	~ 300 Kbps ~ 200 Kbps ~ 500 Kbps	Medium High Medium
Ticketing	Ticket scanning	< 200 Kbps	High
Services (Restaurants, etc.)	POS	Determined by application	Determined by application
Venue staff	Web access Email VoIP	~ 300 Kbps ~ 200 Kbps ~100 Kbps	Medium High Low

Table 2

Performance requirements are critical and drive the design process. *They must be fully understood before proceeding to the next phases of designing the network.*

As the table shows, typical bandwidth consumption is fairly low and latency tolerance is high with the exception of voice and video. Video streaming can be difficult to characterize since bandwidth is dependent on the resolution, encoding, etc. A value of 500 Kbps is sufficient for highly compressed MPEG-4 videos to deliver attendees videos such as replays of events, interviews or special features.



Latency and Jitter

Another value of interest is the latency and jitter tolerance of an application. Low bandwidth applications such as Voice over IP (VoIP) have very little tolerance for network delay. Other applications like email have no particular requirement for latency and can handle long delays.

As a general rule, most venue coverage (the seating) does not require high bandwidth per user. Bandwidth requirements should be optimized for the most likely devices, i.e. smartphones and tablets. These devices do not have the same processing power as laptops and tend to use lighter weight applications.

Signal Quality

The maximum client connection rate is highly influenced by the received signal. The signal strength should also be high compared to background noise and interference in order to ensure a high Signal to Noise Ratio (SNR). SNR is used to describe client signal quality. A strong SNR means higher data rates, less errors and fewer re-transmissions. If the signal strength is very low or the noise is very high, the client will be unable to distinguish the transmission well enough to decode it. A good high capacity design should target an average SNR of at least 20 dB for all the client devices. SNR can be measured as part of an on-site propagation RF survey (live AP) on-premise.

The Impact of Client Devices

Correctly Sizing Client Load

The number of APs required is driven in large part by the number of simultaneous clients on the network. The number of and location of these devices at a venue at any particular time is highly variable and primarily based on attendance numbers. However a network design must take into consideration a range of client numbers. Finding that value can be challenging. A common mistake is assuming a 20,000-seat stadium deployment must be able to handle 20,000 devices simultaneously. The likelihood of this happening is vanishingly small. Planning a Wi-Fi deployment for 20,000 active users would create a network far larger than will ever be required, cost far more money and probably wouldn't deliver the same performance as a network with fewer APs. For more specific information on estimating the number of clients, please see the section Estimating the Number of Client Devices.

In a very dense deployment, the usual rule of thumb is often "less is more". This seems counter-intuitive but is far more realistic and typically produces better results. Interference comes in two forms: interference from other Wi-Fi devices and interference from non-802.11 equipment. The first case is by far the most prevalent. Wi-Fi can be its own worst enemy. Therefore, any deployment that places many APs near each other in an open environment automatically puts Wi-Fi RF interference high on the list of design variables.



Client Capability

All Wi-Fi devices are not the same. They had different supported modulations, throughput, and radio types, transmit power, etc. Understanding the impact each of these is helpful when it comes to determining overall capacity.

How quickly a device can get on and off the air helps determine how many clients can be supported given the required performance metrics. An 802.11n-capable device will transmit much faster than a legacy 802.11abg device. This reduces latency and increases the amount of data that can be sent at any given time.

The maximum transmission speed of a wireless device is typically listed as a reference but the actual throughput that can be achieved will always be less. The following table lists some common transmission rates¹:

Common 802.11 Rates (Max.)

Client Capability	Channel Width	Spatial Streams	Minimum PHY Rate*	Maximum PHY Rate
Legacy 802.11b	20 MHz	1	1 Mbps	11 Mbps
Legacy 802.11g	20 MHz	1	1 Mbps	54 Mbps
Legacy 802.11a	20 MHz	1	1 Mbps	54 Mbps
802.11n 1 stream client (1x1:1)	20 MHz	1	6.5 Mbps	72.2 Mbps
802.11n 1 stream client (1x1:1)	40 MHz	1	13.5 Mbps	150 Mbps
802.11n 2 stream client (2x2:2)**	40 MHz	2	13 Mbps	300 Mbps

Table 3

* Minimum PHY rate does not include management frames, which are typically sent at 1 - 2 Mbps.

** Most client hand held devices are only single stream devices. The AP is multi-stream therefore permitting STC (space time coding) in the downlink and MRC (Maximal Ration Combining), which permits higher throughputs.

As noted, the rates listed here are PHY rates. A PHY rate is the maximum throughput of raw symbols. This is not the same as application data, which is what is normally considered throughput (or goodput). Higher layer data such as Layer 2 TCP/IP and UDP/IP traffic adds overhead and reduces the amount of actual bandwidth available for applications such as web browsing and email. This overhead is a necessary part of any IP network. Additional overhead from transmissions such as management frames on the wireless network also reduce available client throughput. Management traffic includes AP beacons and acknowledgements, which are vital of operation.

¹ This is not intended to be a complete list of all possible PHY rates but rather an indication of highest and lowest scenarios. For more information, please consult the [802.11 standard](#) or similar [documentation](#).



Estimating Goodput

For example, a legacy 802.11g client has a maximum PHY rate of 54 Mbps, but once the overhead for TCP/IP is subtracted this typically reduces actual throughput to about 20 Mbps. 802.11n on the other hand, has many improvements that result in greater efficiency such that even a single stream 802.11n device can still achieve up to 72.2 Mbps on the same 20 MHz wide channel as the 802.11g device. From this it could be estimated that available client throughput could be about 40 Mbps. Some protocols, such as UDP, have fewer overheads and will return greater numbers. Likewise, other additions such as encryption will also add to the overhead.

802.11b is a very old 2.4 GHz standard a maximum PHY rate of 11 Mbps. It was the first widely adopted Wi-Fi standard, but was quickly replaced by faster 802.11g devices. 802.11b has not been sold in smartphones or tablets in many years and is unlikely to represent any significant part of a public population.

Unfortunately there is no precise calculation to determine these theoretical limits. These numbers depend greatly on the type and amount of traffic generated by a particular protocol. Other factors such as driver-specific implementations can also vary. This doesn't even include the fact that most clients are not always connected at the maximum PHY rate. A client transmission rate can vary even during a single session at a single location due to conditions such as congestion, changing RF, etc. Interference and congestion can cause a client to reduce or increase transmit speed as it perceives changes.

In general, it is safe to assume that 802.11n clients will perform about twice as well as legacy clients. Current estimates² suggest that approximately 60% of current consumer devices are 802.11n-capable but this number is climbing. Nearly all-new Wi-Fi devices are 802.11n, which implies the number of legacy devices will drop over time.

² This estimate is based on Ruckus field tests and monitoring at large venues.
© 2012 Ruckus Wireless, Inc



RF Interference

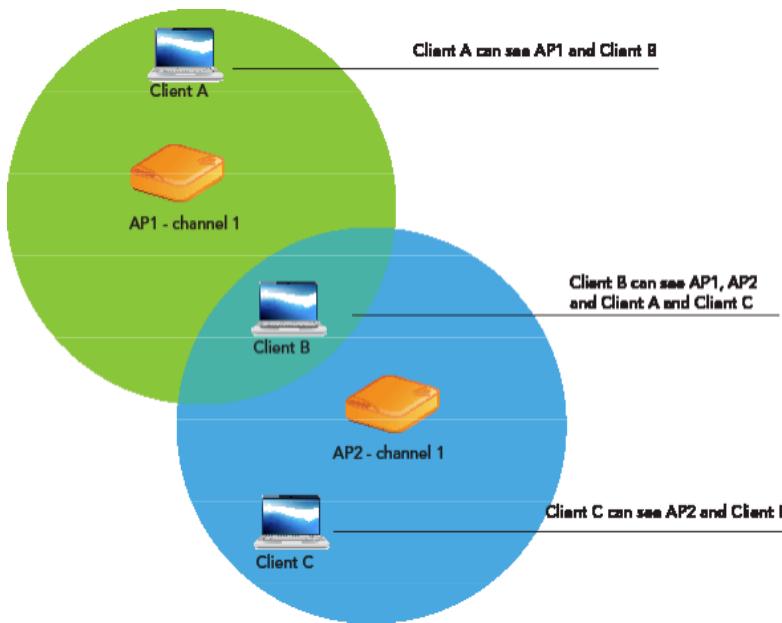
Wi-Fi

Most designers are aware of the impact of non-802.11 RF signals on Wi-Fi networks. Non-802.11 devices include some wireless security systems, cameras, DAS, etc. But this usually doesn't represent the majority of RF interference in a high-density environment. It is critical to account for this as a consequence of deploying the Wi-Fi network. Wi-Fi interference typically derives from congestion or co-channel interference.

Congestion is caused by the presence of many active Wi-Fi devices on the same channel. Since 802.11 is a half-duplex medium, only one of these devices can send or receive data at a time. This includes the AP. The more client devices contending for airtime, the less time is available for any individual device. Many devices also introduce the possibility of several clients transmitting at the same time. Simultaneous transmission can result in corrupted data and re-transmitted data, slowing the network down. The 802.11 standard has collision detection and avoidance mechanisms to help prevent multiple devices transmitting at the same time.

The above description of congestion assumes there is a single AP with many clients talking to it. But if there are many APs that happen to be on the same RF channel it can cause something called *co-channel interference*.

Multiple APs and their clients on the same channel is a problem whenever those devices are close enough to hear each other. When one device transmits *all other devices on that channel stop transmitting*. This means clients on AP1 will stop transmitting if they hear a client on AP2 transmitting. Or AP1 will hold its transmission if it hears AP2 while it's transmitting. When this occurs, there is no increase in aggregate capacity, just coverage, since AP1 and AP2 share the capacity of the channel.



A related event is called the *hidden node* problem; a client can hear other devices but those stations can't hear it. When this happens, *mid-air collisions* can occur. A collision is when two devices transmit at the same time; corrupting the data. Neither station can tell which data was intended for it and which was destined for the other client. The only option for the client is to re-transmit.

Venues such as stadiums have a higher likelihood of experiencing Wi-Fi interference. This is because these venues have a lot of open space, which also happens to be where the majority of attendees are located. When APs that have Line of Sight (LoS) to other APs (just as attendees can see one another in the stadium/arena), they will cause interference if they occupy the same channels.

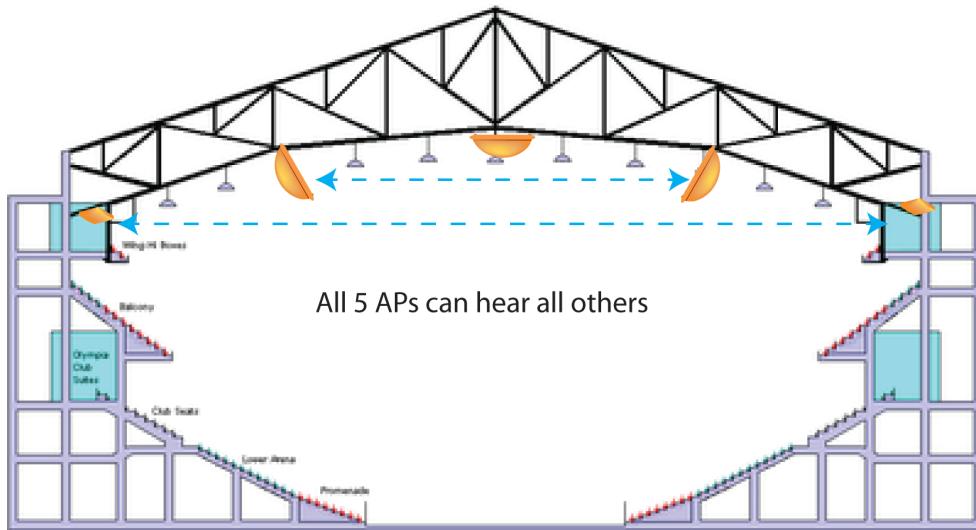


Figure 1 - Open spaces do little to restrict RF propagation

Most APs are installed in this space simply because this is where most devices are located. This means the likelihood some of APs will occupy the same channel is very high. The reuse factor can be calculated by dividing the total number of APs that can hear one another by the number of channels used. The higher this number in any given space the higher the self-interference experienced.

Exactly how much self-interference the Wi-Fi network generates depends on several factors such as the type of AP, antenna selection, where it is mounted, etc. The number of client devices will also fluctuate from one event to another based on attendance. The best rule of thumb is to keep potential interference as low as possible. This is the number one reason why deployments that over estimate the number of required APs see diminishing or even negative returns. Less is definitely more. The goal is to maximize capacity to the point where adding more APs no longer increases the aggregate capacity.

Non-Wi-Fi

While 802.11 interference will likely be the single largest source of RF interference, there are other sources. Non-Wi-Fi devices that use the same spectrum can cause problems. These devices commonly use the 2.4 GHz spectrum, although there are some that also use the 5 GHz range as well. Examples of this include microwaves, non-Wi-Fi cameras, cordless phones, [Zigbee](#) wireless telemetry, headsets, frequency hopping microphones.

Non-802.11 RF interference can be difficult to diagnose since it is often generated at random times and is not always obvious. A site survey is always recommended for any Wi-Fi deployment before installation. This can be as elaborate as a formal survey or as simple as a quick tour of the building during business hours with an inexpensive RF analyzer such as the Wi-Spy 2.4x from [MetaGeek](#), Fluke ([AirMagnet](#)) Spectrum XT, or a portable spectrum analyzer, such as those from [Agilent](#) or [Anritsu](#).

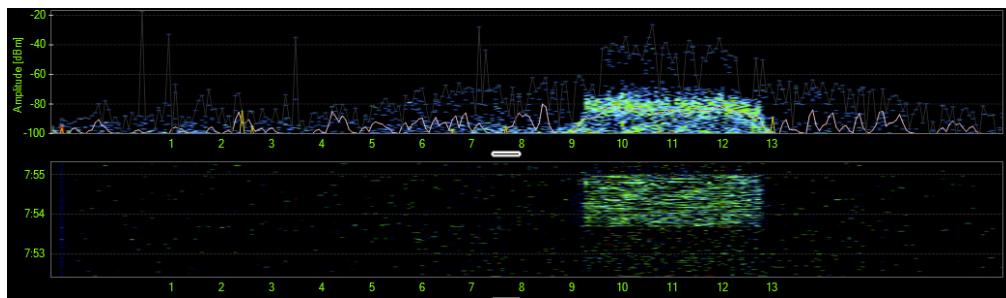


Figure 2 - Wi-Spy recording of a lightly used Wi-Fi network on channel 11

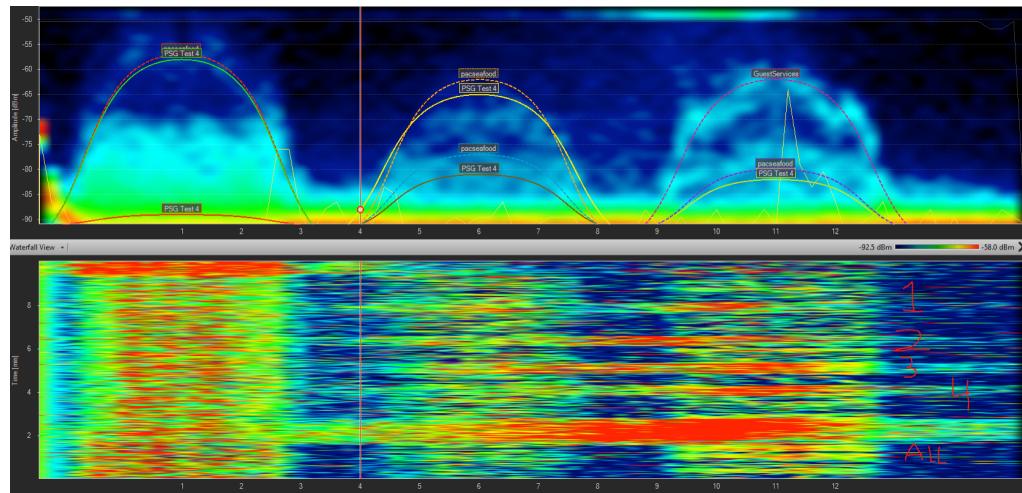


Figure 3 - A Wi-Fi network on channels 1, 6 and 11 with very heavy non-802.11 interference. This network is unusable.



Guidelines for Performance

As a general rule, the following will hold true for most very high-density Wi-Fi installations:

- As density goes up, the amount of airtime dedicated to management traffic (scanning for APs, broadcasts, etc.) will go up. This is also true as the number of SSIDs broadcast increases. Both decrease the amount of airtime available for applications
- Avoid or reduce co-channel interference as much as possible
- Consider mounting APs in non-Line of Sight (NLoS) locations - this will help attenuate the signal, which reduces the cell size and potential for co-channel interference. High-density applications have more than enough APs to make individual coverage a non-issue
- Make sure there are no other sources of RF interference nearby (non-802.11 sources)
- The more dense the population of devices, the higher the average latency and jitter - this can limit the types of applications that can be supported in the most dense situations
- The goal for capacity is to maximize the SNR per AP



Estimating Client and AP Counts

The previous section discussed determining minimum performance requirements and factors that can affect the final deployment's ability to deliver them. Without this information the rest of this document is as helpful since it cannot be tuned to correct parameters. This section discusses the next step which is how many APs will be required for the design.

How many clients can I connect to a single AP?

This is the most common question asked about Wi-Fi. The answer changes dramatically depending on:

- Key performance metrics (applications, bandwidth, latency)
- Client capability
- Estimated number of devices per AP
- Physical density of people
- AP hardware selection
- Whether encryption will be utilized and what type

As discussed in the previous chapter, the minimum bandwidth and latency requirements for a device heavily influences how many clients an AP can support. This number in turn is used to calculate the amount of APs needed to satisfy the requirements.

Estimating the Number of Client Devices

While it is obvious all that all 20,000 attendees at a stadium will not use the network simultaneously, we still need to determine some reasonable number for network sizing. The state of a Wi-Fi device becomes an important factor i.e. if it is active and transmitting or associated but idle. Correctly scaling capacity needs to consider both the number of clients that might be connected as well as the number actually using the network. There should always be enough APs such that any random client can associate at any time and transmit data from any part of the coverage area.



Stadium Example:

The chance of all 20,000 attendees bringing a Wi-Fi device, connecting it and transmitting at the same time is almost nil; but there is no easy way to determine what number *is* likely. This is further complicated by the assumption the number of devices will increase over time. One way to estimate this number makes the following assumptions:

- The maximum number of Wi-Fi devices associated but idle on the network will always be greater than the number that are active
- Attendees will typically use one wireless device at a time
- Not all attendees will bring Wi-Fi devices or connect them to the network - estimate 70%
- Unless otherwise indicated, no more than 80% of these devices are connected to the network
- Unless otherwise indicated, no more than 30% of all devices that are connected to Wi-Fi are active at the same time

Assuming an event at full capacity, some reasonable numbers to start with might look like this (see Table 4):

	Percentage of Uptake	Number of Clients
Maximum capacity	100%	20,000
Attendees bringing a Wi-Fi device	70%	14,000
Devices connected to the WLAN	80%	11,200
Active devices	30%	3,360

Table 4

The percentages offered here represent a place to start³. If an existing wireless network exists, it may have valuable information about the current number of active devices. If this is the case, the percentages should be adjusted accordingly.

There are several factors used to determine AP counts;

- Association limit
- Capacity limit
- Coverage limit⁴

³ These percentages are based on actual observations during a sporting event in a sold-out stadium. The observed percentages were much lower (about half) of the guidelines offered here. This number was doubled to account for future smartphone growth and Wi-Fi enabled device usage.



Estimating the Access Point Association Limit

Ruckus APs currently support a maximum of 512 clients per AP. Therefore, the total number of APs needed to ensure all the Wi-Fi devices can get service if desired is calculated as follows:

Maximum number of Wi-Fi devices / 512 associations per AP

Estimating Access Point Throughput

The estimated aggregate throughput for an AP can be calculated as follows:

Maximum PHY rate * % of Overhead - Loss from interference (%)

As discussed earlier, TCP/IP networks often have as much as 40% overhead. This is subtracted from the raw available throughput to yield a clean RF number. However, high-density venues will see this number reduced due to collisions. This number is hard to pin down, but for these examples 35% is a reasonable place to start.

Stadium Example

The average expected throughput for an AP radio in the reference stadium is:

$$72.2 \text{ Mbps} - (72.2 \text{ Mbps} * .40 \%) = 43.3 \text{ Mbps} - (43.3 \text{ Mbps} * .35) = 28.12 \text{ Mbps}^5$$

These numbers shown above are per radio. The lower number (2.4 GHz) is specifically called out here. 5 GHz radios should expect a slightly higher number.

When many APs are able to influence one another, such as in a very high-density deployment, the noise floor will rise. The same type of increase comes from the higher number of end user devices. The result is not all the user devices are able to achieve the highest modulation rate due to the noise floor increase and/or they are further away from the AP than the others. The resulting AP capacity will be a function of the blended rates of each end user devices modulation rate resulting in the weighted average.

$$43.3^6 \text{ Mbps} - (43.3 \text{ Mbps} * .40 \%) = 26 \text{ Mbps} - (26 \text{ Mbps} * .35) = 16.9 \text{ Mbps}$$

This average is per radio, so a dual-radio AP could be expected to deliver twice this amount across two radios. However, since the second radio is 5 GHz and less subject to interference, it should deliver a higher number.

⁴ Coverage limits are typically not an issue in very dense deployments and will not be discussed further.

⁵ This number is for 2.4 GHz radios – a 5 GHz radio should be higher

⁶ This value was estimated by computer modeling the SNR in the specific venue



Estimating Clients per AP Capacity

The maximum number of client devices a single AP can support with the required KPIs is then calculated as:

AP aggregate throughput / Minimum bandwidth per client

With the information so far, the maximum capacity for the example is:

Number of associated clients = 11,200

Estimated number of concurrent active devices = 30% of 11,200 = 3,360

Required throughput per client = 500 Kbps

Latency tolerance = high

RF environment = very high during peak usage

Percentage of retransmissions/loss due to interference = 35%

Estimated throughput per AP radio = 16.7 Mbps

These figures are then calculated:

Maximum clients per AP to meet capacity = 33 (16.7Mbps / 500Kbps per client)

Number of APs required to meet number of active clients = 102 APs (3360 / 33)

Total APs for 11,200 associated devices = 22 (11,200 / 512)

Seats covered per AP = 196 (20,000 / 102)

The largest calculated number of APs, either for capacity or associations, is what is required to meet the service requirement.

Using these guides, 102 APs is the required number assuming the client devices are distributed evenly across all APs. However this is not a guarantee – some venues changing seating areas based on event type. It is always a good idea to allow for additional APs to cover this eventuality.

The only way to accurately estimate the weighted average capacity per AP is to do a computer simulation of the venue and calculate the SNR of each AP and the entire service area. Just estimating and using the peak value will yield to few APs and underestimating the per AP capacity will drive the AP count higher, which will in turn further reduce the weighted average per AP capacity.

Most venues will also require additional APs to cover areas outside the main stage. Coverage for concourses, ticketing areas, media areas offices, coaching, player ready area and backstage staging areas will increase the AP count. The exact number should be determined through an on-site survey and computer coverage simulation that accounts for exact construction and square footage.



Estimating Additional APs

Determining how many extra APs are required beyond the minimum count requires additional information:

- Distance from AP to client
- AP cell (coverage) size
- Additional coverage areas outside the main bowl/stage

Because venues such as stadiums are very large and very dense, APs should ideally have small coverage areas. This increases performance and allows for narrower beam antennas that can boost signal gain. More APs also increases the receive signal for clients since there are more APs closer to any client location. This has the benefit of better SNR, which is required for high performance and capacity.

The directional antenna requirement is driven by the need for higher signal gain due to higher installation locations. They also help reduce interference. For more information on AP mounting strategies, please see section AP Installation and Hardware.

Distance from AP to Client

In general, an AP should be mounted as close to the clients as possible. RF signal strength is calculated as the inverse square of distance so the signal degrades quickly as distance increases. A client that is 30 meters (98 feet) from an AP receives a signal that is only 1/4th that (-6dB) of a client 15 meters distant. A large enough distance can reduce the signal strength to the point where a client cannot hear it. This is particularly true if there is any background interference or noise.

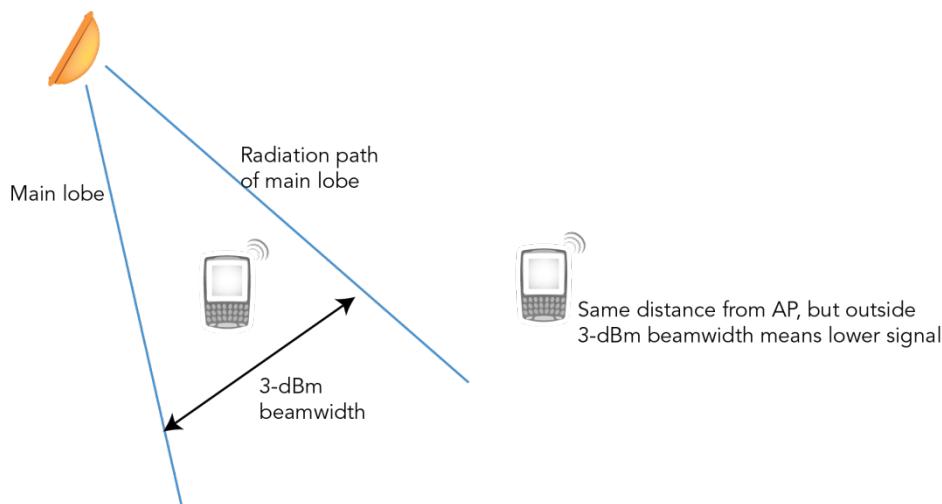


Figure 4 - Position APs to place clients in 3-dBm beam width

Using this model of AP positioning based on its beam width helps determine the coverage area for each AP. The need to get the APs closer is required to keep the AP footprint from being too large. It can help to think of each AP supporting a particular spot or section of seats within the stadium itself. Each additional AP adds another group of seats until all are covered.

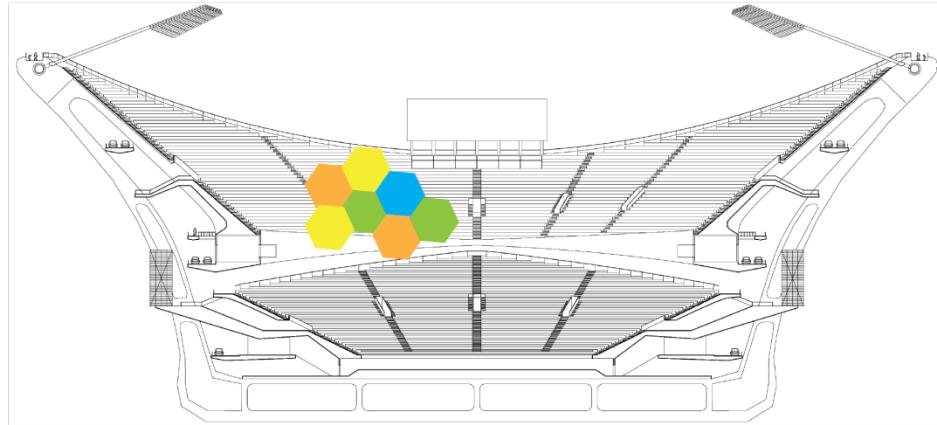


Figure 5 - Each region is the 3-dBm beam width coverage of an AP

Some venues will not necessarily have a structure in every location to support ideal AP installation. Open roof stadiums or outdoor sports fields are particularly challenging for this reason. In these cases compromises such as additional APs located at less than ideal spots may be required.

Guidelines for Estimating Capacity

Determining the number of APs required for a design can be complex. There are many variables that can come into play. As a general rule, the following rules of thumb will almost always apply:

- Plan for an adoption rate of about 50%-60% and 15% concurrent users
- Estimate realistic AP goodput capacity that takes IP and 802.11 overhead into consideration
- Do a RF SNR plan to estimate the interference and impact on the AP capacity
- Ensure the number of clients per radio leaves some headroom (i.e. don't plan the initial design to max out AP clients)



AP Installation and Hardware

AP hardware and where it is actually installed contributes significantly to the total number of APs. There are several factors that need to be considered when selecting AP hardware and installation:

- Desired coverage area
- Mounting of AP (best signal to client, best isolation from other APs)
- AP hardware: radio band, transmit power, antennas, etc.

The previous chapter discussed the importance of finding a balance between the size of an individual AP coverage area while maintaining good signal quality and the capacity required. In general, any AP mounted to serve clients in the general seating areas should use a directional antenna to increase the signal gain for better link quality as well as confine the energy to the specific cluster of seats.

Antenna Selection

Because the density is very high in the main bowl area, an omni-directional antenna is not a good choice for APs covering this area. Narrow beam directional antennas are highly recommended. A directional antenna has two major advantages: first, the narrow focused antennas produce less interference for other nearby devices, and second, it has a higher signal gain which assists in the link budget in both directions. A higher signal gain allows the AP to be positioned further from clients without reducing signal strength.

Several Ruckus APs feature highly directional antennas with signal gains of up to 11 dBi and a 3-dBm beam width of only 30°. These are excellent choices for open areas. More enclosed spaces can take advantage of Ruckus APs with larger beam width of up to 120° or omnidirectional antennas.

Figure 6 shows the $30^\circ \times 30^\circ$ degree antenna pattern for both Vertical and Horizontal polarities.

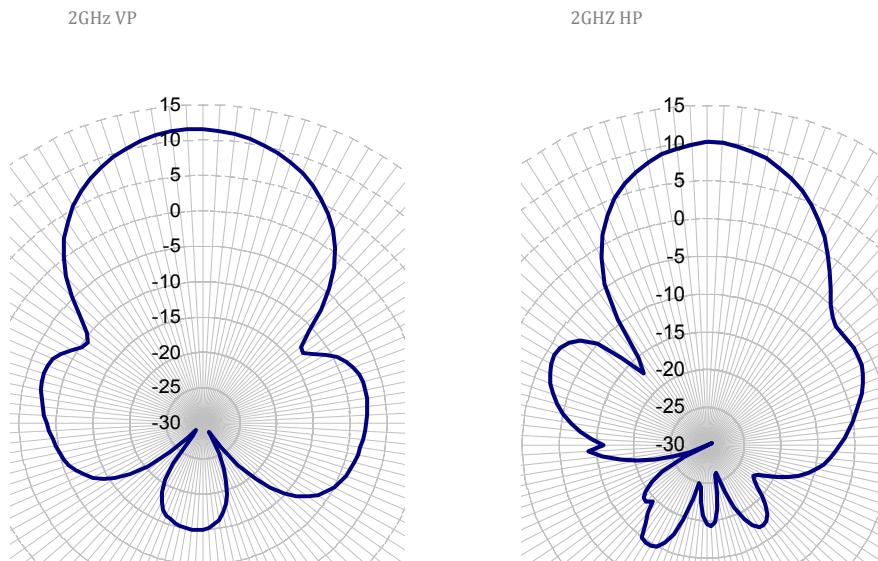


Figure 6 - Ruckus 30° directional antenna polar plots

Another hardware option uses external, directional antennas on the APs. Although the adaptive antenna array (BeamFlex) in Ruckus APs includes directional antennas, the overall coverage will effectively cover an area similar to traditional omnidirectional antenna. A directional antenna can keep the RF energy focused even more tightly to shrink cell size. The ZoneFlex 7762-S already comes with a $120^\circ \times 30^\circ$ directional antenna that can be used if more directional antennas are not desired. Note that the 7762-S can also be mounted sideways to reduce the degrees of freedom (coverage and spread) even further. One very common attenuation technique is to mount APs both inside the area with clients and on the other side of a wall. Most interior walls will attenuate the signal somewhat but likely not enough to dramatically drop the signal strength for clients directly on the other side. Still, this kind of attenuation is an easy way to increase AP density while keeping interference down.



AP Hardware Selection

In general, all Ruckus APs are able to work in the densest environments and can be placed closer to each other due to built-in interference mitigation. Therefore any enterprise-class ZoneFlex AP can be adequate. However in dense deployments it is extremely desirable to deploy dual-radio models. These APs have two radios, one for 2.4 GHz and one for 5 GHz spectrums. This means they can support twice as many devices. This is particularly true of newer wireless devices, which are typically dual-band and can connect to either radio. Since the 5 GHz spectrum is often much cleaner any devices moved to this band will experience higher transmit speeds with fewer errors; boosting overall performance and capacity. Also, because there are more non-overlapping 5 GHz channels there is far less co-channel interference for these clients. In some cases it might be feasible to turn off some of the 2.4 GHz radios on dual-radio APs to achieve very high AP density without impacting performance for 2.4 GHz clients.

Signal Attenuation

One factor, which is rarely considered in Wi-Fi deployments, is the physical effect of the human body. A person's body naturally absorbs and attenuates any RF signal that travels through it. The difference between the RF characteristics of an empty room and one filled with devices and people is extreme. Testing should always involve an environment as close to the actual deployment as possible. This is particularly true if the AP mounting location is low and likely to travel through people or other sources such as furniture.

In the very densest deployments this can be exploited for higher performance. A great example is mounting an AP low - such as under seating. In this case attenuation is high but can actually help since it will reduce the signal propagation and keep cell size small. This is desirable, as it allows more APs to be deployed closer to each other.

A directional antenna is also helpful for keeping cell size small. The further an AP is from the client, the lower the signal strength and the larger the cell size. Keep in mind; the RF energy does not stop at the antenna's 3-dB point. It continues to propagate in all directions, albeit at weaker levels. But it *will* continue and therefore does have some impact.

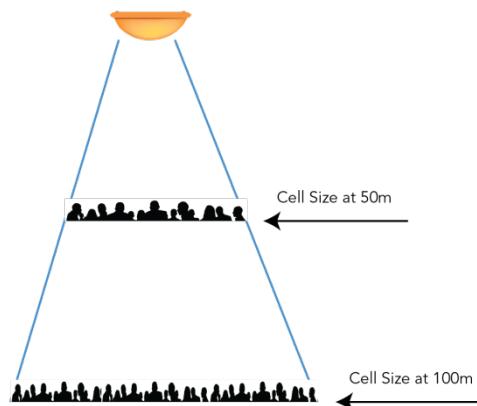


Figure 7 - The further clients are from an AP, the larger the cell size

The next section discusses some mounting options related to optimizing AP positioning for performance.

AP Mounting Locations

AP locations are dictated to a large degree by the structure of the venue. Although mounting locations will vary by venue, some common areas to consider include:

- Roof (non-retractable)
- Overhangs above seating (terracing)
- Catwalks
- Underneath seating (catacombs/walkways)
- Suites and private boxes

Ideally, an AP is mounted such that the 3-dB beam width intersects the seating area to create the capacity coverage zone needed. In the reference design used in this document, 20,000 seats are served by 102 APs. In this case the coverage target is a cluster of about 196 seats. So mounting too far away from the clients may end up covering too many seats; this would overlap with other AP coverage clusters. Figure 8 below describes an example of creating coverage zones which becomes the AP capacity coverage targets.



Figure 8 - APs target coverage zone (seat clusters) at or close to 3-dB beam width

In figure 9, the APs are mounted to be as close to the seating as possible, covering the target number of seats (coverage zone) and at the same time are positioned such to direct the energy away from other APs.

Never mount the AP at the back of the venue pointing towards the back of the clients. Remember as stated earlier, the body loss is much higher than free space loss, so the signal from the AP will propagate across the venue at a much higher signal level than it will to those seating nearby with their backs turned.

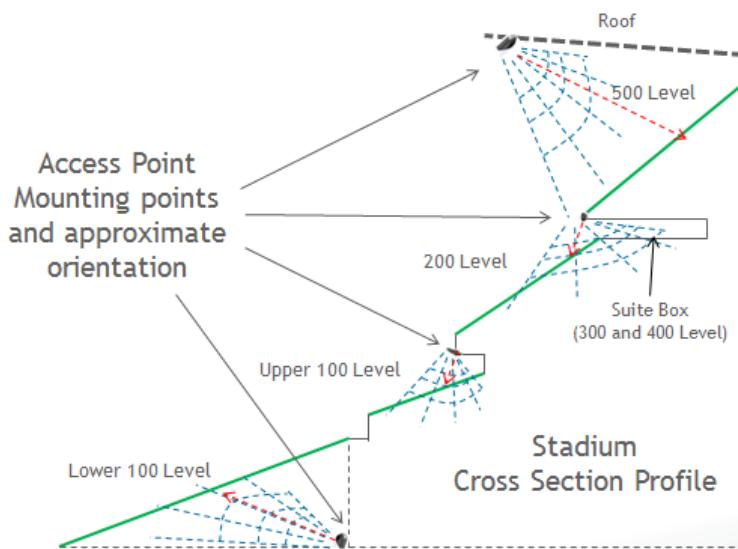


Figure 9 - APs mounted to isolate the energy to the coverage zone

In reality, the AP might not be able to be installed at the ideal position. This is usually because there is no place to mount the AP at that spot or the AP is partially obstructed. Sometimes this can be overcome with a higher gain antenna; other times there is no choice but to select a different location. The only way to accurately assess this is with an on-site survey of the physical structure. A survey will take into account the available mounting locations, distance, line of sight to seating areas, and construction materials.

The easiest part of a stadium to cover is typically private boxes and suites. These rooms are usually rooms with standard ceilings that allow the AP to be mounted within a few meters of the guests. Unlike most of the other APs, these can be indoor models with omni-directional antenna coverage instead of directional. This allows the use of a cheaper AP model without sacrificing coverage. These APs can often cover more than one room or even some areas above and below, depending on the building construction. Do keep in mind that when mounting APs in the Suites, the energy from these APs will influence the APs servicing the general seating area, so during the survey, consider the proper AP model, its orientation with antenna pattern in mind, the structure of the suite all to try to keep the energy in the suites and not out in the open area seating.



Other coverage areas for ticket holders include concourses, concessions and ticketing areas. These areas tend to have lower density of both APs and devices and better mounting choices. General coverage type mounting practices are best here. The same goes for covering the offices, lockers, and event staging and player ready areas if coverage is also required in those areas.

Note: one issue that can arise with ticketing scanners involves their Wi-Fi capability. Many older scanners do not support standards such as WPA2 with AES encryption. If scanners only support TKIP some additional APs may be required in ticketing areas. The reason this may be necessary is because TKIP encryption does not support as many clients as AES. Moving the scanners off of stadium APs that are targeted towards higher density, prevents the scanners from causing a choke point on the AP for other devices.

Guidelines for AP Installation and Hardware

As a general guideline, the following will hold true for most high-density Wi-Fi installations:

- Choose outdoor AP models for any environment subject to water, dust or outdoor conditions
- Very large venues will require small AP cells to maximum signal quality
- Directional or narrow-beam antennas are an excellent choice when density is very high and coverage cell size is small – better signal and less interference
- Indoor APs are good choices for interior spaces such as suites, meeting rooms and non-public areas such as offices
- Install APs as close to ideal locations for best signal quality with the least interference (isolate the AP signal)
- Non-optimal choices can still work well if planned correctly



Configuration Optimizations

The previous sections described general guidelines to determine project performance requirements and AP capacity, mounting and hardware. This section describes further optimizations that may be configured on the Ruckus ZoneFlex products. These include the following:

- Client load balancing
- Channelfly
- Rate limiting
- Restricting minimum rates
- OFDM and CCK rates
- Background scanning
- Maximum clients per radio/SSID
- Open vs. encrypted networks

Many of these options can be used for high-density deployments while others may only be used in certain situations. The rest of the chapter includes descriptions of common scenarios and step-by-step configuration instructions.

Client Load Balancing

Many high-density designs make use of balancing clients to prevent excessive load on a single AP. This can be desirable when there are under-utilized APs near a large number of clients. Ruckus APs create groups of APs that offer similar service levels by using background scanning to discover neighboring APs. Client load balancing relies on a performance trade-off between distributing client load vs. small service interruptions due to the APs going off channel for background scanning. For most environments, this is an excellent balancing between performance and overall capacity.

Client load balancing is not recommended for very dense deployments however. With extreme density, clients will naturally distribute themselves simply because there are so many APs with similar signal strength near any given client. The probability all clients will go to one AP is very low. Given this case, there is no reason to enable client load balancing; even the small amount of capacity lost due to background scanning should be avoided since the benefit is too small to justify.



Channelfly

Channelfly is a sophisticated method of determining the optimal channel selection for an AP. As discussed earlier, RF interference is a major cause of performance problems. Channelfly is unique in that it not only takes the current noise into consideration (both 802.11 and non-802.11) it also looks at the potential capacity available on a channel as well. Unlike many other vendor solutions, Channelfly might choose any possible channel rather than restricting itself to traditional non-overlapping channels. This is fine and will not negatively impact performance if the current RF environment mandates those channels. Theoretically, using more than 3 2.4 GHz channels can introduce co-channel interference with other devices on nearby channels but in reality it may not be a problem. In particular, when APs and devices are subject to attenuation, the signal strength drops off more quickly. This is particularly true for the energy transmitted outside the center channel.

For example, let's consider the number of APs required for our example, 102. Since there are 3 non overlapping channels in the 2.4GHz band, each channel is being reused 34 times.

($102/3=34$) If using the best mounting you could effectively isolate the RF energy so that any AP only hears 1/3 of the other APs, still 11 others can be heard. The co-channel interference is a real issue if the RF energy from other APs is heard at levels higher than that from clients within any given APs coverage zone. When considering using more channels, an AP might be said to transmit on channel 6, but it is actually transmitting across the "overlapping" nearby channels 4 and 5 and 7 and 8. But the main power and highest signal strength will be on the center frequency, channel 6. As the signal strength drops, the RF energy across all occupied sub-channels drops as well. With enough attenuation, the energy on the non-center channels can drop below an acceptable noise floor and be used by another AP. This means Channelfly might move APs to occupy an "overlapping" channel but not see as much of the other device's transmissions due to the signal drop-off beyond the center frequency.

Channelfly uses the 802.11h channel announcement method of notifying clients that it is about to change channels on an AP. Support for 802.11h is mandatory in 5 GHz clients but not 2.4 GHz. Because of this, some 2.4 GHz clients not deal as well with channel changes. If this is a problem, please turn Channelfly off for the 2.4 GHz radios.

Channelfly usage is always recommended in high-density environments.

Channel Width

Legacy 802.11 devices all use 20 MHz wide channels for transmission. This allows a maximum data rate of 54 Mbps. Part of the performance gain of 802.11n devices is the use of 40 MHz wide channels. This change allows 802.11n devices to leap from a maximum of 72.2 Mbps on 20 MHz to 150 Mbps on 40 MHz. Therefore, when planning for maximum performance per client, a wider width channel might be preferred because it allows the higher transmit rates⁷.

In many high-density environments however 40 MHz wide channels are not always recommended. This is because doubling the size of a channel more than halves the number of non-overlapping/interfering channels available. High-density implies more APs closer together; the need for more clear channels is generally a higher priority than ultimate throughput rates. The goal is to have a higher aggregate capacity from all the APs rather than just having higher burst speeds.

A 20 MHz channel width makes even more sense when the devices do not require a large amount of bandwidth. Also, not all 802.11n devices support or will use the wider channel size. Many handheld devices such as smartphones and tablets use a maximum of 20 MHz channel size regardless of what the AP supports.

A network where only 802.11n devices are allowed is known as a *Greenfield deployment*. If legacy devices are on the network only 20 MHz wide channels are allowed for backwards compatibility. By default, all Wi-Fi networks are set to allow backwards compatibility. Since public venues have no control over the device type or capability it often makes more sense to tradeoff better throughput for some devices in exchange for a performance gain that benefits *all* devices.

Access Point Groups				
This table lists your current AP groups and provides basic details about them. Click Create New to add another AP group, or click Edit to make changes				
#	Name	Description	# of Members	Actions
1	System Default	System default group for Access Points	5	Edit Clone
2	Greenfield	Restrict WLAN to 802.11n clients only	0	Edit Clone

Editing (Greenfield)				
Name	Greenfield			
Description	Restrict WLAN to 802.11n clients only			
Radio Settings	Radio B/G/N (2.4 GHz)	Radio A/N (5.0 GHz)		
Channelization	<input type="checkbox"/> Override System Default	Auto	<input checked="" type="checkbox"/> Override System Default	40
Channel	<input type="checkbox"/> Override System Default	Auto	<input checked="" type="checkbox"/> Override System Default	Auto
TX Power	<input type="checkbox"/> Override System Default	Auto	<input type="checkbox"/> Override System Default	Auto
11N only Mode	<input type="checkbox"/> Override System Default	Auto	<input checked="" type="checkbox"/> Override System Default	N-only

Figure 6 - Configure Greenfield Mode on ZoneDirector. Configure->Access Points->Access Point Groups

⁷ Although the 802.11n standard allows 40 MHz wide channels for both 2.4 GHz and 5 GHz in practice the wider channels are only used on 5 GHz. This is because there is far less spectrum available in 2.4 GHz; the maximum number of 40 MHz channels is only 1 which is generally not practical.

In the CLI, the command to enable and disable Greenfield mode for an AP group is:

```
ruckus (config) # ap-group Greenfield
```

```
ruckus(config-apgrp)# radio 5 11n-only
```

In both the Web UI (in the figure shown) and the CLI a mandatory channel width may also be specified as well. Individual APs may also have the channel width fixed as well - this will override the AP group settings.

CLI command:

```
ruckus (config-apgrp) # radio 5 channelization number 40
```

Example

Public venues have no control over the type of device that will use the network. Therefore a Greenfield deployment is simply not practical. 20 MHz wide channels should be preferred for both 2.4 GHz and 5 GHz.

AP Transmit Power

Ruckus APs can attempt to choose the best possible power setting as well as the best channel. Channelfly will normally choose the channel. The APs can be configured to choose their own power settings or accept a manual setting. The default Tx power for APs is Auto. In practice this often means the APs transmit at full power. Full power is generally preferred because it results in the highest signal strength to a client; resulting in a faster connection. If for some reason the bleed over between two APs on the same channel is too much (co-channel interference) and attenuation or a narrow-beam antenna doesn't solve the problem the power might be lowered.

The AP Tx power can be set on a per-AP basis or for a group of APs in the ZoneDirector Web UI or the CLI.

Editing (74:91:1a:0e:a3:10)	
MAC Address	74:91:1a:0e:a3:10
Device Name	Outdoor DUT
Description	
Location	
GPS Coordinates	Latitude <input type="text"/> , Longitude <input type="text"/> (example: 37.3881398, -122.0258633)
Group	System Default <input type="button" value=""/>
Radio B/G/N (2.4 GHz)	
Channelization	<input type="checkbox"/> Override Group Config <input type="button" value="20"/>
Channel	<input type="checkbox"/> Override Group Config <input type="button" value="6"/>
TX Power	<input checked="" type="checkbox"/> Override Group Config <input type="button" value="-3dB (1/2)"/>
WLAN Group	<input type="checkbox"/> Override Group Config <input type="button" value="single-outdoor-wpa2"/>
WLAN Service	<input checked="" type="checkbox"/> Enable WLAN service for this radio.

Figure 7 - Configure static AP transmit power. Configure->Access Points->Edit AP->Radio->Tx Power

Editing (System Default)	
Name	System Default
Description	System default group for Access Points
Radio Settings	Radio B/G/N (2.4 GHz) Radio A/N (5.0 GHz)
Channelization	20 40
Channel	6 149
TX Power	-3dB (1/2) Full
11N only Mode	N-only N-only
WLAN Group	single-wpa2 single5GHz-wpa2

Figure 8 - Configure static transmit power for an AP group. Configure->Access Points->AP Group->Radio->Tx Power



The CLI commands for a single AP are:

```
ruckus(config)# ap 74:91:1a:0e:a3:10
```

```
ruckus(config-ap)# radio 2.4 tx-power
```

Auto	Sets the 2.4GHz radio to use 'Auto' Tx. power setting.
Full	Sets the 2.4GHz radio to use the specified Tx. power setting.
½	Sets the 2.4GHz radio to use the specified Tx. power setting.
¼	Sets the 2.4GHz radio to use the specified Tx. power setting.
1/8	Sets the 2.4GHz radio to use the specified Tx. power setting.
Min	Sets the 2.4GHz radio to use the specified Tx. power setting.
Num	Sets the 2.4GHz radio to use the specified Tx by number from 1-10 (-1dB ~-10dB).

```
ruckus(config-ap)# radio 2.4 tx-power 1/2
```

The commands to set tx power power for an AP group are:

```
ruckus(config)# ap-group Greenfield
```

```
ruckus(config-ap-group)# radio 2.4 tx-power
```

A word about minimum power settings

It can be tempting to lower the transmit power to the lowest possible setting for a very dense environment. But this is not recommended. BeamFlex technology works to automatically adapt transmit power. By focusing energy primarily in the direction of the client, Beamflex effectively reduces Tx power in directions away from the client. This has the same interference reduction effect as turning down Tx power but without the considerable downside of reducing SINR to the client.

Rate Limiting

It is sometimes tempting to consider using rate limiting to try to guarantee a certain amount of traffic for every client. But a better mechanism already exists to address this problem. Ruckus' Airtime Fairness algorithm will keep available capacity and airtime evenly distributed amongst all clients. This guarantees no clients are able to "hog" all of the bandwidth and, consequently, none bandwidth starved either.

Rate limiting does not tend to help in high-density environments and can even reduce aggregation size and overall Wi-Fi capacity.

OFDM and CCK Rates

Connection rates are important to ensure high performance and it is even more important for high-density applications. The higher the connection rate for clients, the faster they can go on and off the air. This directly correlates to higher aggregate performance. Channelfly, a smart RF channel selection system, already tries to get the cleanest and highest capacity environment possible for clients. This can potentially be further improved with two other mechanisms: Orthogonal Frequency Division Multiplexing (OFDM) rates and Complementary Code Keying (CCK) rates. Each of these modulations schemes is used in 802.11 networks. CCK is a legacy system that is only used by 802.11b networks. All newer technologies such as 802.11g and 802.11a use OFDM. This also includes 802.11n versions, which employ several mechanisms to achieve higher rates beyond simple modulation.

OFDM and CCK (see Tables 5 and 6) are distinguished by a different set of basic rates that also have different receiver sensitivities as well:

CCK Rates

Transmit Speed*	Rx Sensitivity
11 Mbps	-82 dBm
5.5 Mbps	-85 dBm
2 Mbps	-86 dBm
1 Mbps	-89 dBm

Table 5

OFDM Rates

Transmit Speed*	Rx Sensitivity
54 Mbps	-68 dBm
48 Mbps	-68 dBm
36 Mbps	-75 dBm
24 Mbps	-79 dBm
18 Mbps	-82 dBm
9 Mbps	-87 dBm
6 Mbps	-88 dBm

Table 6

* Each scheme employs modulation techniques as applied to subcarriers such as 64-QAM, 16-QAM, BPSK and QPSK. For the sake of brevity and simplicity these are not detailed here as the overall techniques discussed apply regardless. Data shown is for 2.4 GHz since CCK is not supported by 802.11a, which is OFDM only.

Two obvious pieces of information that can be extracted from these tables is that OFDM has much better receive sensitivity as well as higher overall rates. If a client has a choice, OFDM will give much better performance. It cannot be assumed that an 802.11g device will always use OFDM however. If there are devices present on the network that use CCK, OFDM devices must go into *protection mode* and could drop to CCK rates.

Much better overall performance can be achieved if all Wi-Fi devices are restricted to OFDM only. This would improve sensitivity as well as allow higher connection speeds.

Removing CCK rates will effectively prevent any 802.11b devices from connecting to that SSID. Make sure there are no 802.11b devices that need access before disabling CCK.

Ruckus equipment can be configured to not support CCK rates and require OFDM only. This is configured on a per-SSID basis via the CLI.

```
ruckus(config)# wlan highdensity-ssid
```

```
ruckus(config-wlan)# ofdm-only
```

This command removes CCK rates as an acceptable connection rate by a new client. Note that this does not prevent a connected client from dropping to lower rates; it simply disallows it at the initial client association. Clients that later drop to very low rates typically do so due to excessive interference and other PHY errors.



Most modern Wi-Fi devices are 802.11g at a minimum and do not require CCK rates. Therefore disabling CCK support will often have very little impact. The main exception is some venue equipment such as ticket scanners or POS devices that may be 802.11b only. Before disabling CCK, check all required devices to ensure they do not require CCK.

Background Scanning

Background scanning allows an AP to periodically go off-channel and scan other channels. This information is used in many ways:

- Gather information to determine optimal channel selection (only used if Channelfly is not active. Not recommended)
- Discover neighboring AP candidates for load balancing
- Discover neighboring APs for Opportunistic Key Caching (OKC) which improves client roaming speeds
- Discover rogue APs

Some functions, in particular AP neighbor discovery, are required to take advantage of features such as client load balancing. Other functions such as rogue AP discovery or client roaming may not be required. The tradeoff is that whenever the AP is off-channel it is not available to service clients (this is unlike Channelfly behavior). Background scanning happens fairly quickly, but it can impact overall performance in a busy network. One way to mitigate this is by increasing the time in between AP off-channel scans. Since the number and position of APs does not change frequently, a longer scan rate like 3600 seconds (1 hour) may be preferred to the default of 20 seconds.

To take advantage of background scanning and maintain performance, the scanning interval can be tuned for specific environments. Background scanning can be set on a global basis as well as a per-SSID basis from either the ZoneDirector's Web UI or via the CLI. Background scanning is enabled by default every 20s.

Background Scanning
<p>Background scans are performed by APs to evaluate radio channel usage. The process is progressive; one frequency is scanned at a time. This scanning enables rogue device detection, AP locationing, and self-healing.</p> <p><input type="checkbox"/> Run a background scan on 2.4GHz radio every <input type="text" value="20"/> seconds</p> <p><input type="checkbox"/> Run a background scan on 5GHz radio every <input type="text" value="20"/> seconds</p> <p><input checked="" type="checkbox"/> Report rogue devices</p>

Figure 9 - Configure a global background scanning policy on the ZoneDirector. Configure->Services->Background Scanning



Editing (highdensity-ssid)

General Options	
Name/ESSID*	highdensity-ssid
Description	
WLAN Usages	
Advanced Options <ul style="list-style-type: none"> Accounting Server Disabled Send Interim-Update every 10 minutes Access Control L2/MAC No ACLs L3/4/IP address No ACLs Rate Limiting Uplink Disabled Downlink Disabled (Per Station Traffic Rate) Multicast Filter <input type="checkbox"/> Drop multicast packets from associated clients ACCESS VLAN <input type="checkbox"/> Attach VLAN Tag <input type="text"/> <input type="checkbox"/> Enable Dynamic VLAN Hide SSID <input type="checkbox"/> Hide SSID in Beacon Broadcasting (Closed System) Tunnel Mode <input type="checkbox"/> Tunnel WLAN traffic to ZoneDirector (Recommended for VoIP clients and PDA devices.) Background Scanning <input type="checkbox"/> Do not perform background scanning for this WLAN service. (Any radio that supports this WLAN will not perform background scanning) Load Balancing <input type="checkbox"/> Do not perform client load balancing for this WLAN service. (Applies to this WLAN only. Load balancing may be active on other WLANs) 	

Figure 10 - Configure per-SSID background scanning policy on the ZoneDirector. Configure->WLANS->Edit SSID->Advanced Options->Background Scanning

The CLI commands to enable and set background scan intervals are:

```
ruckus(config)# services
ruckus(config-services)# background-scan radio-2.4-interval 900
ruckus(config-services)# background-scan radio-5-interval 900
```

These commands set the enable background scanning and set the scan interval for both radios to 15 minutes (900 seconds).

```
ruckus (config) # wlan highdensity-ssid
ruckus(config-wlan)# bgscan
```

These commands enable background scanning for the specified SSID. Note that the scanning interval cannot be changed on a per-SSID basis. It will always use the global settings since this is a radio function.

Maximum Clients per Radio/WLAN

Because high-density deployments involve very high numbers of devices, the maximum number of connections can likewise be high. The default client limit on a Ruckus APs is 100 clients per radio and per SSID by default. This can be increased to a maximum of 256 clients on a per-AP or per radio basis, depending on the AP model⁸.

A large public venue should definitely increase this number. In general, this number should be set to maximum number of clients that might want to associate with the AP with some additional headroom. An associated device will not necessarily authenticate or become active; but if a client wants to associate it should always be allowed to do so. Otherwise users may perceive a problem if they want to use the wireless later and cannot connect.

The maximum clients can be configured either via the Web UI or the CLI on the ZoneDirector.

Note that configuring maximum clients on an AP allows different numbers depending on if the device is a legacy client or an 802.11n capable client. This allows an administrator to effectively limit these devices. For high-density environments, the highest possible speeds should always be maintained for the client device. In general, the more legacy devices per radio, the lower overall performance.

The screenshot shows the 'Editing (highdensity-ssid)' screen in the ZoneDirector web interface. It is divided into two main sections: 'General Options' and 'Advanced Options'.

General Options:

- Name/ESSID***: highdensity-ssid
- Description**: (empty)

WLAN Usages (This section is currently empty)

Advanced Options:

- Accounting Server**: Disabled, Send Interim-Update every 5 minutes
- Access Control**: L2/MAC No ACLs, L3/4/IP address No ACLs
- Rate Limiting**: Uplink Disabled, Downlink Disabled (Per Station Traffic Rate)
- Multicast Filter**: Drop multicast packets from associated clients
- ACCESS VLAN**: Attach VLAN Tag, Enable Dynamic VLAN
- Hide SSID**: Hide SSID in Beacon Broadcasting (Closed System)
- Tunnel Mode**: Tunnel WLAN traffic to ZoneDirector (Recommended for VoIP clients and PDA devices.)
- Background Scanning**: Do not perform background scanning for this WLAN service. (Any radio that supports this WLAN will not perform background scanning)
- Load Balancing**: Do not perform client load balancing for this WLAN service. (Applies to this WLAN only. Load balancing may be active on other WLANs)
- Max Clients**: Allow only up to 150 clients per AP radio to associate with this WLAN

Figure 11 - Configure a per-SSID maximum clients policy on the ZoneDirector. Configure->WLANS->Advanced Options->Max Clients

⁸ For information on specific maximum number counts for an AP, please consult the Ruckus AP User Guide documentation.

Max Clients	100	For Radio B/G.	150	For Radio N.
--------------------	-----	----------------	-----	--------------

Figure 12 - Configure a per-AP maximum clients policy on the ZoneDirector. Configure->Access Points->Max Clients

The CLI commands to configure maximum clients per SSID are:

```
ruckus(config)# wlan highdensity-ssid
ruckus(config-wlan)# max-clients 150
```

and on a per-AP basis:

```
ruckus(config)# ap c4:10:8a:1d:e3:c0
ruckus(config)# wlan highdensity-ssid
ruckus(config-wlan)# max-clients 150
```

Open vs. Encrypted WLANs

Depending on the application, data encryption may or may not be required. This is usually driven by the design and security requirements. However it is worthwhile to observe that adding encryption will increase overhead. The more overhead there is, the less throughput is available for application data. If the network designer has the option of choosing, an open network might be preferable assuming it does not obviate any security requirements.

The recommended rule of thumb is an open network for the guest network and an encrypted network for internal and administrative usage.

Intrusion Detection

The Ruckus ZoneDirector supports several intrusion detection mechanisms. These are disabled by default on the ZoneDirector. It is typically a good idea to leave these disabled in a high-density environment. Large numbers of devices inherently cause more over the air congestion and interference. These conditions raise the likelihood of corrupted packets and transmission retries for both the client and the AP. In the very worst environments a client might exceed the number of authentication requests due to retransmissions and be blacklisted temporarily. Preventing a client from connecting, even for just 30 seconds, adds to user confusion about what is happening and overall dissatisfaction.

This type of behavior can also be observed on a client that repeatedly asks for a PSK/D-PSK or other login credentials. Even if the credentials are saved and known to be good. The client might perceive its inability to authenticate as a problem with the credentials and prompt the user for new ones.

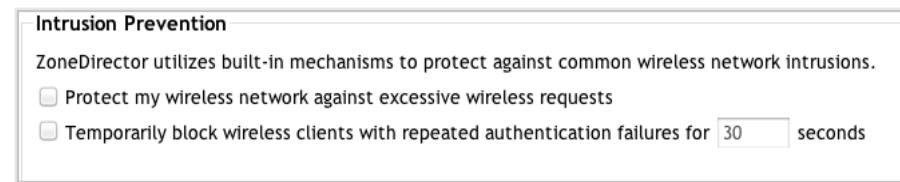


Figure 13 - Configure Intrusion Detection on the ZoneDirector. Configure->Services->Intrusion Prevention

The CLI command is:

```
ruckus(config)# services  
ruckus(config-services)# no temp-block-auth-failed-client
```



Limiting Broadcast Traffic

All wireless devices will send broadcast (non-unicast) traffic from time to time. Some of this, such as ARP requests, is required for proper operation. By definition every broadcast packet must be sent to all devices on the network. This means APs and clients must periodically spend time sending broadcasts instead of application data. This is fine if the broadcast is necessary but there are a lot of broadcast packets that are not necessary. Anything that can be done to restrict this type of traffic from being sent over the air will greatly improve performance.

Broadcasts can be limited on the device itself if the administrator has control of the machine. For example, discovery mechanisms such as Bonjour can be disabled if not needed. This might work in a corporate or school environment where IT controls the devices but is unlikely to be useful in more public venues.

If the client cannot be prevented from broadcasting, it is possible to limit the client traffic at the AP. This is done via Access Control Lists (ACLs). An ACL is a set of rules that specify what kind of traffic is and is not permitted. Because this happens at the AP it is a great mechanism for stopping traffic before it can go over the air on every AP. Examples of common broadcast traffic include:

- NetBIOS/NetBEUI - Windows-specific name servers, printers, file servers, etc. Ports used include:
 - 137 - Windows name services
 - 138 - Network neighborhood
 - 139 - File sharing and print services
 - AFP (Apple File Sharing)
 - TCP 548
- UDP 5353 - Bonjour Apple specific-discovery mechanism for printers, file shares, multicast-DNS (mDNS), etc.
- UPnP - Client to client peer services
- UDP 1900
- TCP 2869

*Unless specifically noted, port numbers are TCP and UDP.

This traffic can be blocked both via a firewall⁹ on the wired network or at the Ruckus AP. ACLs are constructed on the ZoneDirector and then applied on a per-SSID basis. In public venues such as convention centers, hotels, etc. it is unlikely the network operator needs to support these protocols and they should be blocked. Other networks such as corporate or schools may or may not need some or all of these services. ACLs can be constructed via the ZoneDirector's Web UI or CLI.

The screenshot shows the 'Editing (Block NetBIOS)' dialog box. It includes fields for 'Name*' (Block NetBIOS), 'Description' (empty), and 'Default Mode' (radio buttons for 'Deny all by default' and 'Allow all by default', with 'Deny all by default' selected). The 'Rules' section contains a table with six entries:

Order	Description	Type	Destination Address	Application	Protocol	Destination Port	Action
1		Allow	Any	DNS	Any	53	Edit Clone ▼
2		Allow	Any	DHCP	Any	67	Edit Clone ▲▼
3	NetBIOS 135	Deny	Any	Any	Any	135	Edit Clone ▲▼
4	NetBIOS 137	Deny	Any	Any	Any	137	Edit Clone ▲▼
5	NetBIOS 138	Deny	Any	Any	Any	138	Edit Clone ▲▼
6	NetBIOS 139	Deny	Any	Any	Any	139	Edit Clone ▲

Buttons at the bottom include 'Create New', 'Advanced Options', 'Delete', 'OK', and 'Cancel'.

Figure 14 - Configure an ACL to block NetBIOS traffic on the ZoneDirector. Configure->Access Control->L3/4/IP Access Control

The equivalent CLI command is:

```
ruckus (config)# l3acl "NoBroadcasts"
ruckus(config)# mode allow
ruckus(config)# l3acl NoBroadcasts
```

Once the ACL has been created, it can then be applied to the appropriate SSID.

The screenshot shows the 'Editing (highdensity-ssid)' dialog box. It includes fields for 'Name/ESSID*' (highdensity-ssid) and 'Description' (empty). The 'WLAN Usages' section is visible below.

⁹ Wired firewalls are beyond the scope of this document. Configuration is vendor-specific but the rules used here generally apply.

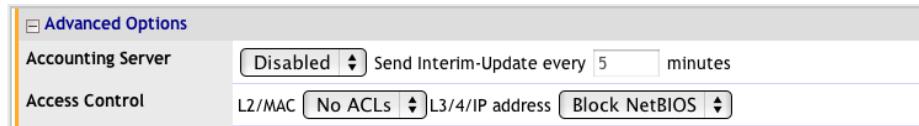


Figure 15 - Apply an ACL to an SSID on the ZoneDirector. Configure->WLANS->Edit->Advanced Options->Access Control

In the CLI:

```
ruckus (config)# wlan highdensity-ssid  
ruckus(config-wlan)# acl l3acl NoBroadcasts
```

Client Isolation

The Ruckus ZoneDirector also has a client isolation mode that can be applied on a per-SSID basis. This blocks wireless-to-wireless traffic and can help reduce excessive broadcasts and other unsupported traffic. Note that this will block *any* wireless-to-wireless traffic so it may not be suitable if some applications such as wireless printers, etc. Fortunately client isolation is configured on a per-SSID basis; guest networks can be kept isolated while internal networks are not.

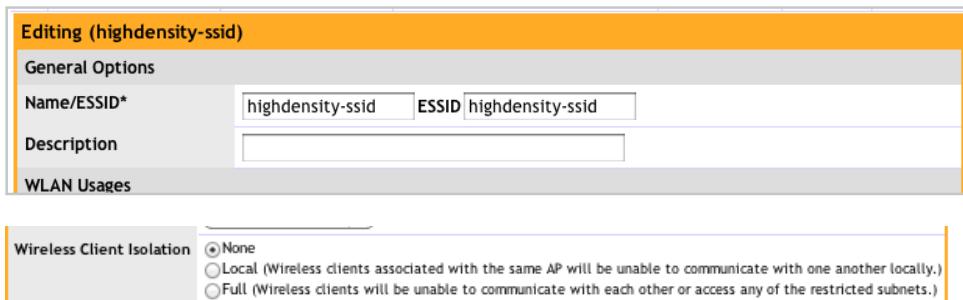


Figure 16 - Client isolation is enabled on a per-SSID basis from the ZoneDirector. Configure->WLANS->Edit->Wireless Client Isolation

In the CLI:

```
ruckus (config)# wlan highdensity-ssid  
ruckus(config-wlan)# client-isolation full
```



Summary

High-density Wi-Fi networks pose unique deployment and performance challenges. Many things that might not be a problem in smaller networks can have a huge impact on larger and higher density Wi-Fi networks. Any deployment that has or expects to have a large number of wireless devices should have the following issues addressed as fully and as early in the design process as possible:

- Performance requirements (key performance indicators)
- Supported applications
- Minimum bandwidth
- Minimum, average and maximum devices per AP
- Maximum latency tolerated
- Number and density of APs
- Client capabilities (802.11n vs. legacy)
- Clients per AP
- RF environment (multipath, attenuation, coverage and cell size)
- AP mounting and location

Ruckus provides many tools and built-in features that help ease deployment in such challenging environments. Once the network is installed and deployed, more tools are available to further tune the network for a specific application or environment. Large, dense Wi-Fi networks bring inherent problems but with the right deployment these networks can also provide high performance and reliability for years to come.

Ensuring you get the most out of the equipment and meet your design KPIs, seek expert support to help with your design. Consult with your Ruckus Sales Engineer or Ruckus Professional Services before your start.