UBIQUITI ACADEMY

Ubiquiti Enterprise Wireless Admin

Table of Contents

Foreword

The *Ubiquiti Enterprise Wireless Admin* (UEWA) training book is made freely available to you as a learning resource to prepare you for taking Ubiquiti certification exams. During classroom training events, students engage in real-world lab activities using the latest Ubiquiti hardware, led by a Ubiquiti-Certified Trainer proficient in the course topics to guide class discussions.

To empower our global user base, the Ubiquiti Academy provides this training book as a reference, to be used to begin and accelerate your learning - it is not a substitute for training courses led by a qualified instructor. When you're ready, sign up for an official Ubiquiti training course and gain recognition as a Ubiquiti-certified professional in your industry expertise.

Ubiquiti acknowledges that professional success in the rapidly-evolving technological world of today requires a strong commitment to continued learning through diverse methods of study. As you read this training book, be sure to participate in our active User Community, where thousands of users come together daily to discuss best practices for configuring, deploying, and troubleshooting real-world projects designed and built on Ubiquiti's cutting-edge platforms.

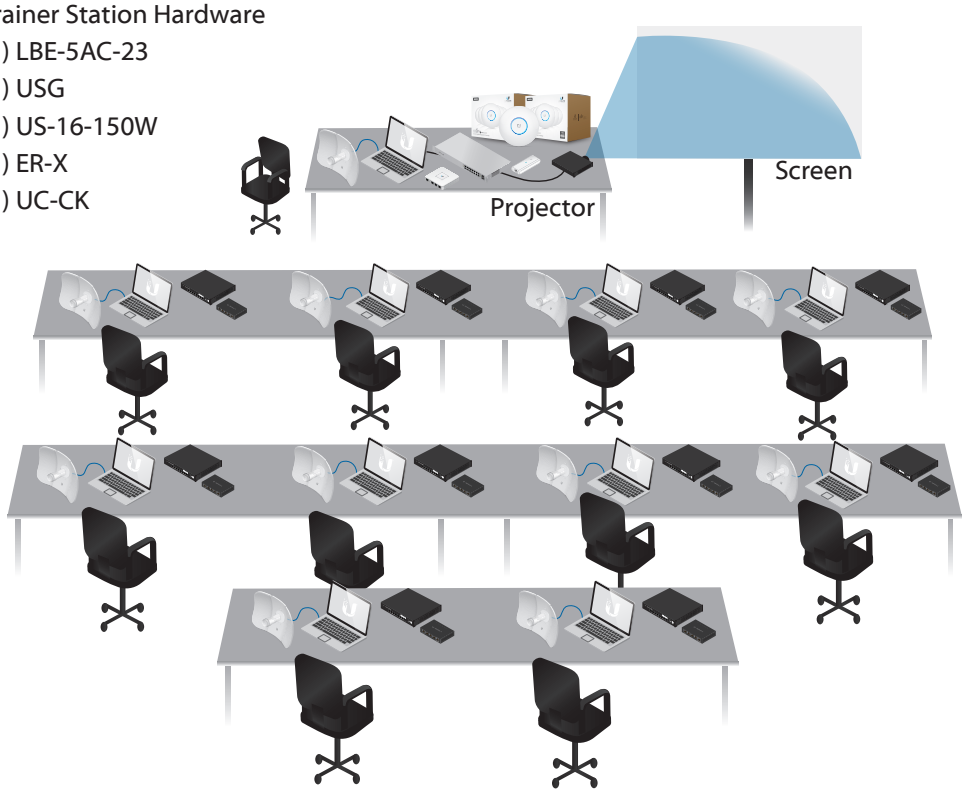
Jamie Higley
Global Director of Training
Ubiquiti Networks, Inc.
March 2017

Preface

This training book is a supplementary guide to be read prior to and during the official Ubiquiti training course. Led by a Ubiquiti-Certified Trainer, Ubiquiti certification courses feature hands-on lab activities, hardware systems, and instructional slides, which together culminate into a unique learning experience.

Typical Classroom Layout

Trainer Station Hardware
(1) LBE-5AC-23
(1) USG
(1) US-16-150W
(1) ER-X
(1) UC-CK



Student Station Hardware

UBWS/UBWA	UBRSS /UBRSA	UEWA
LBE-5AC-23	ER-X ES-8-150W LBE-5AC-23	UAP-AC-LITE LBE-5AC-23

At the conclusion of the classroom event, Ubiquiti-Certified Trainers administer the online exam to students who have participated in the course and now seek training certification.

To sign up for an upcoming Ubiquiti certification course, visit www.ubnt.com/training.

I. UEWA Course Overview

Welcome to the Ubiquiti Enterprise Wireless Admin course! This two-day, in-class training course teaches the most important concepts in Enterprise Networks, focusing especially on Wireless Networks. The course has been completely redesigned with new course materials and lab activities using UAP-AC-LITE and other UniFi hardware to emphasize on how to design, build, and manage the latest, top-performing WLANs.

- WLAN Fundamentals
- WLAN Planning
- Deployment
- Basic Adoption & Setup
- Advanced Management
- Guest Portal & Hotspot

Ubiquiti Enterprise Wireless Certification Track

While not a prerequisite to the UEWA course, the UBRSS (Ubiquiti Broadband Routing & Switching Specialist) course teaches you basic, foundational networking concepts, regardless of your technical background. It also explains how different Ubiquiti products, such as routers, switches, and access points are configured and deployed in broadband & enterprise networks. The UEWA course targets students who have some experience in wireless networking, independent of vendor. Both courses are fast-paced and feature plenty of lab activities to reinforce theory and practice technical concepts. At the conclusion of the course, you can take an exam to certify at the level of Ubiquiti Enterprise Wireless Admin. If you pass at 65% or higher, you will receive a student certificate. To certify as a trainer, you must attend a Train-the-Trainer event hosted by Ubiquiti.

Lab Overview

The UEWA course is written with great detail so you can follow each step closely and understand the technical objective of the activity. Your trainer will provide you with a LiteBeam-ac 5 GHz, 23dBi radio/antenna (LBE-5AC-23) and UniFi AP-AC Lite (UAP-AC-LITE). For each lab activity, read the description at the beginning to understand the objectives. Then proceed to follow the instructions step-by-step as you configure your airMAX-ac and UniFi devices. At the conclusion of the lab activity, compare your lab topology with the topology diagram shown, then answer the questions in the review.

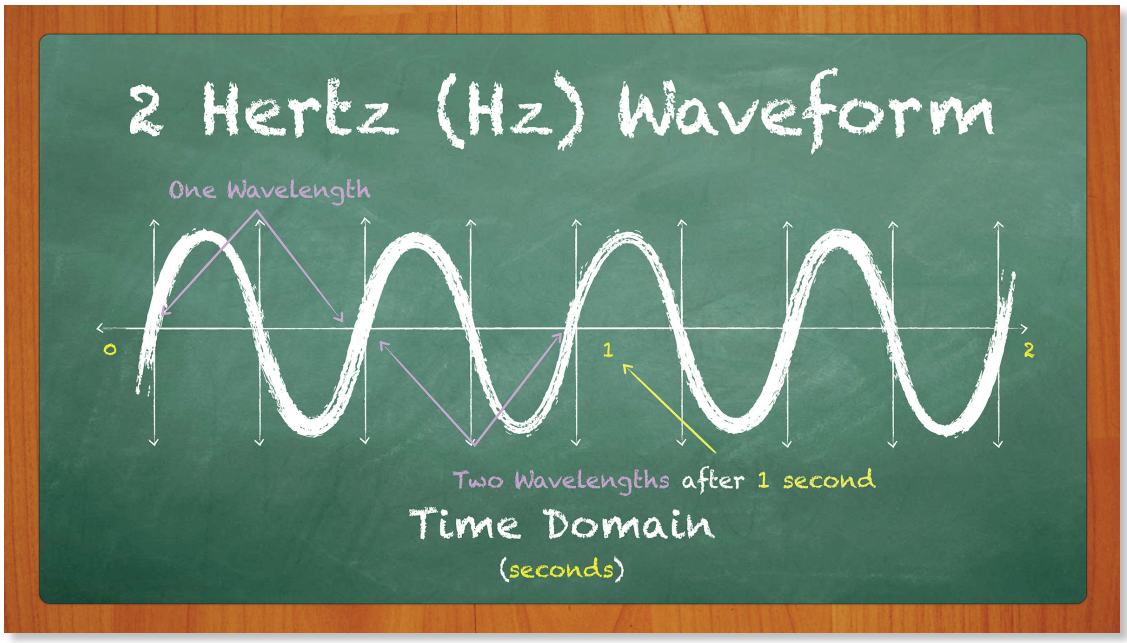
Your trainer will assign you a unique number (X) to differentiate your IP settings from that of others. Later, you will work in groups (Student A and B) to complete lab activities, where your unique number (Student X) is still used for reference. As an example, Student 1 (A) and 2 (B) work in a group and use their unique numbers (1 and 2, respectively). If the lab activity requires Student 2 (B) to set an interface address to "10.1.(100+A).B", then Student 2 (B) would set the interface address to "10.1.101.2", since (100+A) = (100 +1) = 101 and B = 2.

II. WLAN Fundamentals

Wireless LANs (WLANs) follow simple laws of physics, which, when adhered, lead to high user performance and scalability. The purpose of this section is to introduce basic wireless physics and explain channel assignments so you can begin planning for a WLAN deployment. Understanding these concepts allows you to more confidently plan your deployment, or troubleshoot an existing WLAN.

Wave Properties

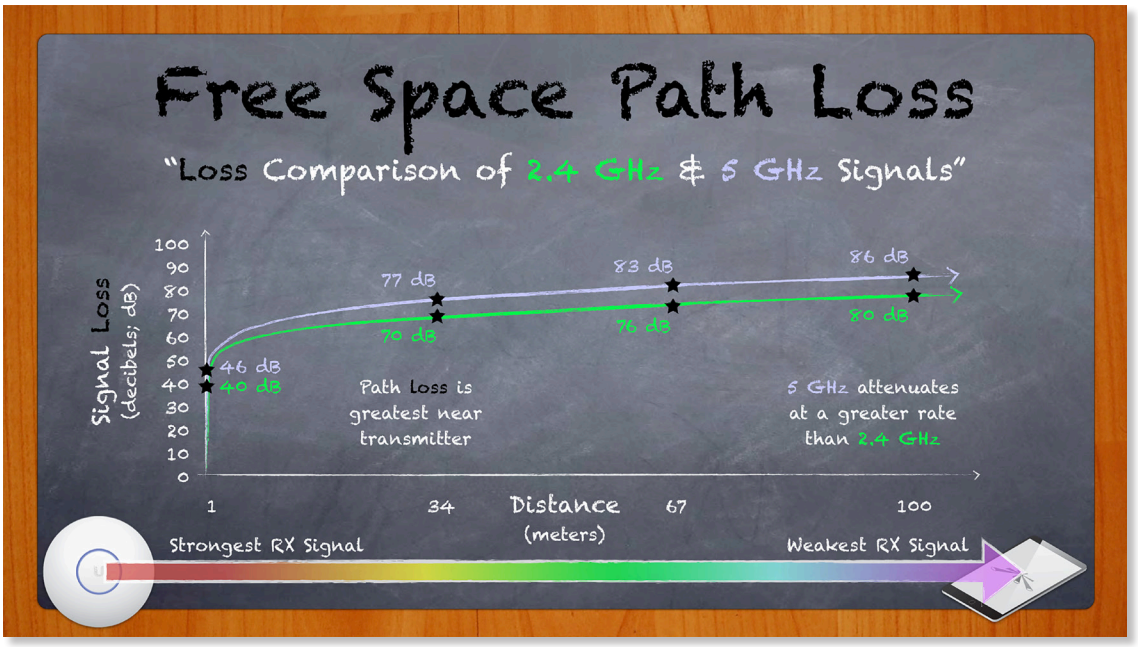
In order to transmit data from one location to another, stations (wireless APs and client radios) generate energy in the form of electromagnetic waves, which travel at the speed of light. These electromagnetic waves operate at different frequencies, which are defined as the number of periodic cycles traversed per second. The frequency and wavelength of an electromagnetic wave are inversely proportional and related by the speed of light:



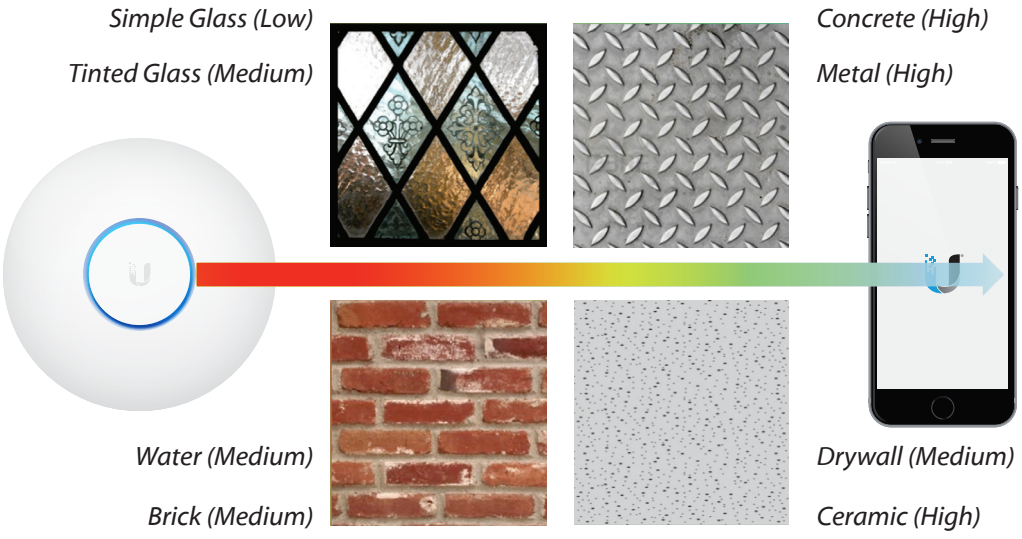
Frequency is measured in Hertz (Hz), which individually represents one period, wavelength, or wave cycle. As a waveform travels from one point to another, it undergoes signal loss due to a phenomenon known as Free Space Path Loss (FSPL). However, lower frequencies (ex. 2.4 GHz) have much longer wavelengths and can propagate further than higher frequencies (ex. 5 GHz).

To relate the levels of energy associated with wireless receive signals, including attenuation (loss) of a wireless signal, we use decibels (dB). Decibels follow a logarithmic relationship where adding & subtracting decibels corresponds to exponential growth or reduction on the linear domain. Each time you add 3 dB or 10 dB, the value on the linear domain increases or decreases by a factor of x2 or x10, respectively.

The relationship between frequency and propagation is best illustrated by the Free Space Path Loss (FSPL) chart for 2.4 and 5 GHz waveforms. At a given distance, 5 GHz (the higher frequency) undergoes more attenuation. Therefore, 2.4 GHz WLANs are ideal for coverage scenarios, while 5 GHz are well-suited for density.

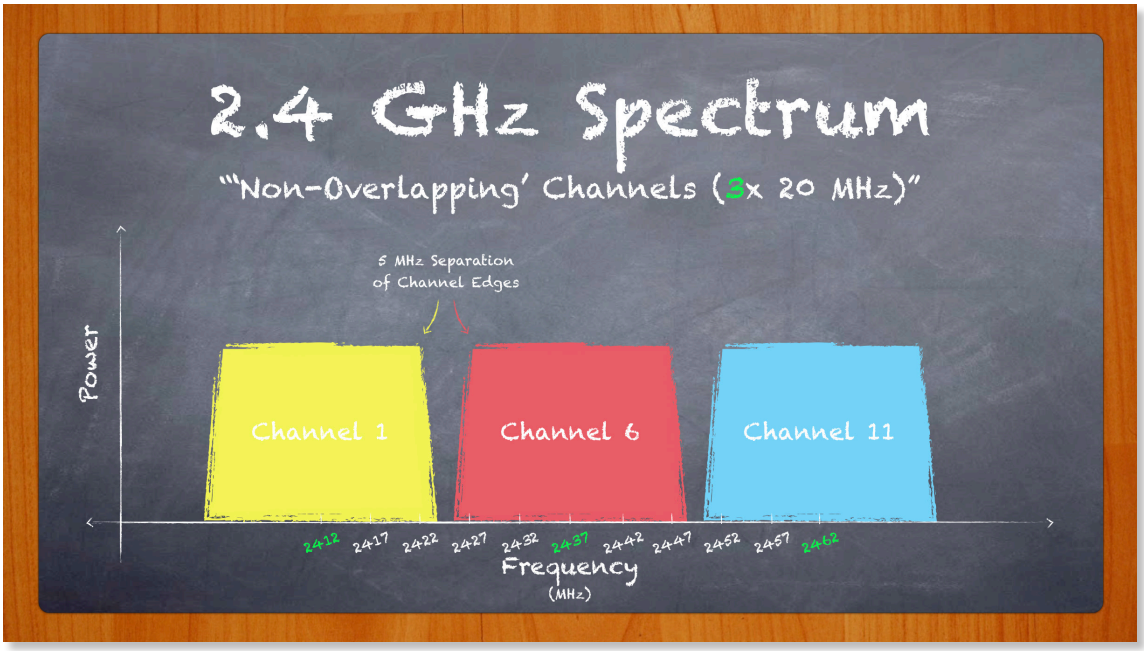


Different materials can affect the level of attenuation faced by wireless signals. For example, concrete attenuates wireless signals more than wood. Certain materials may also cause a wireless signal to propagate, or, 'behave' differently. For example, some metal surfaces can cause wireless signals to reflect, leading to less predictability throughout the WLAN environment. Other materials, like water (or people) can absorb wireless signals. Strategically, the construction of the WLAN environment can help or hinder how you design your wireless network.

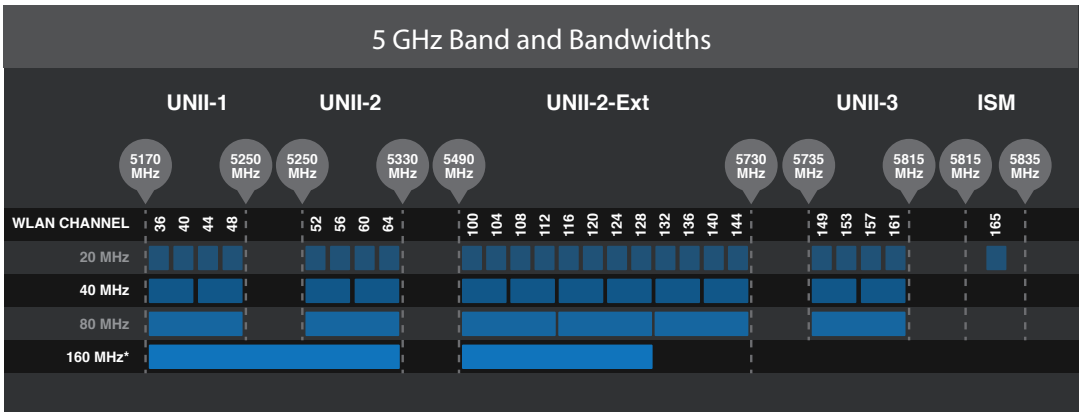


Unlicensed Radio Spectrum

As a worldwide, unlicensed radio spectrum, the 2.4 GHz and 5 GHz bands allow virtually anyone to extend the range of networks with wireless access points. In spite of such universal availability, the unlicensed bands face problems from crowded use and inefficient channel assignments; both of which lead to increased co-channel interference. Faced with these issues, wireless administrators must pay close attention to details in order to plan for the most effective, efficient wireless network possible.



In the past, the 2.4 GHz band has been favored over 5 GHz due to its propagation characteristics. 2.4 GHz waveforms pass more easily through walls and reach clients at long distances. Over time however, the small range of unlicensed spectrum (approximately 83.5 MHz) belonging to the 2.4 GHz band has become overcrowded with competing access points. Furthermore, a prevalence of consumer devices (ex. cordless telephones, baby monitors, Bluetooth devices) using the same frequency range as the 2.4 GHz spectrum is considered 'saturated.'



Compared to the 2.4 GHz spectrum, 5 GHz offers much more flexibility for wireless operators due to greater availability of spectrum and relaxed transmission power requirements. Although the 2.4 GHz band only allows for 3 reuse channels without overlap (1, 6 and 11), the 5 GHz band allows for as many as 24, depending on region (36, 40, 149, 153, etc.). Given the abundance of available channels and short-range propagation characteristics, high-density WLANs benefit greatly from the 5 GHz band.

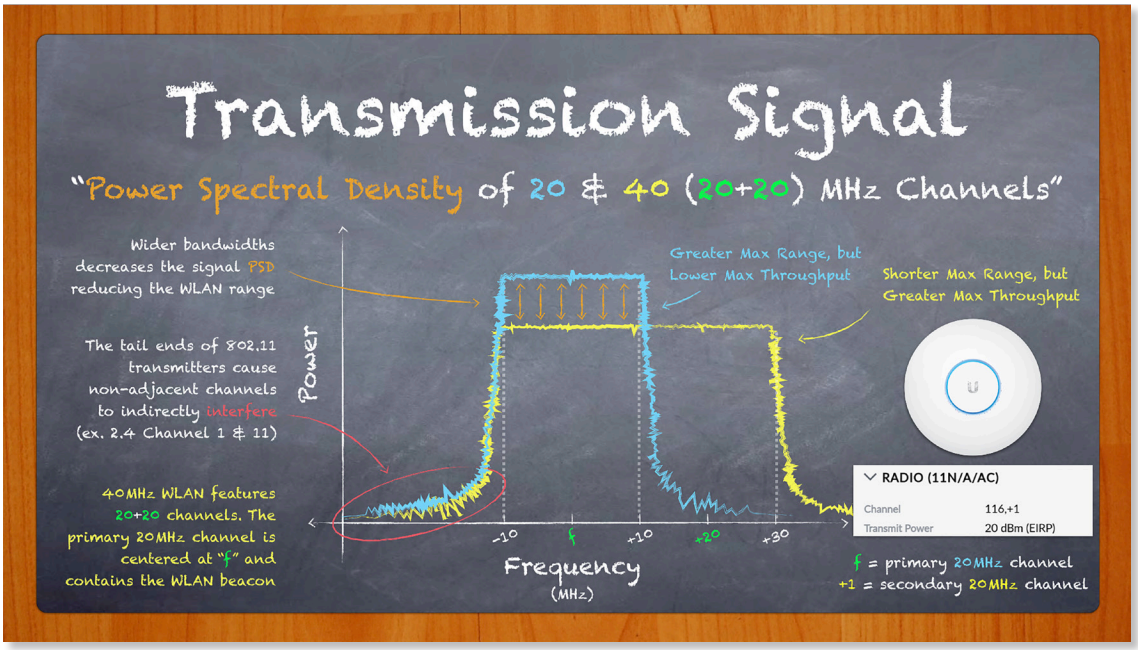
Channel Operation

Understanding how channels operate is key to avoiding interference and maximizing the performance/scalability of the WLAN. In radio communication, a wireless station (like a UniFi Access Point) receives a channel assignment and a specific bandwidth over which it transmits and receives signals to and from nearby stations. This channel assignment pertains to the center frequency of the first 20 MHz channel used by the station.

Channel bandwidth refers specifically to the frequency range over which data signals are transmitted. However, the actual transmission signal generated by 802.11 radios looks similar to a volcano, where 'peak' power levels are spread across the channel bandwidth, and power levels drop off at the edges of the channel bandwidth near the 'tail ends.'

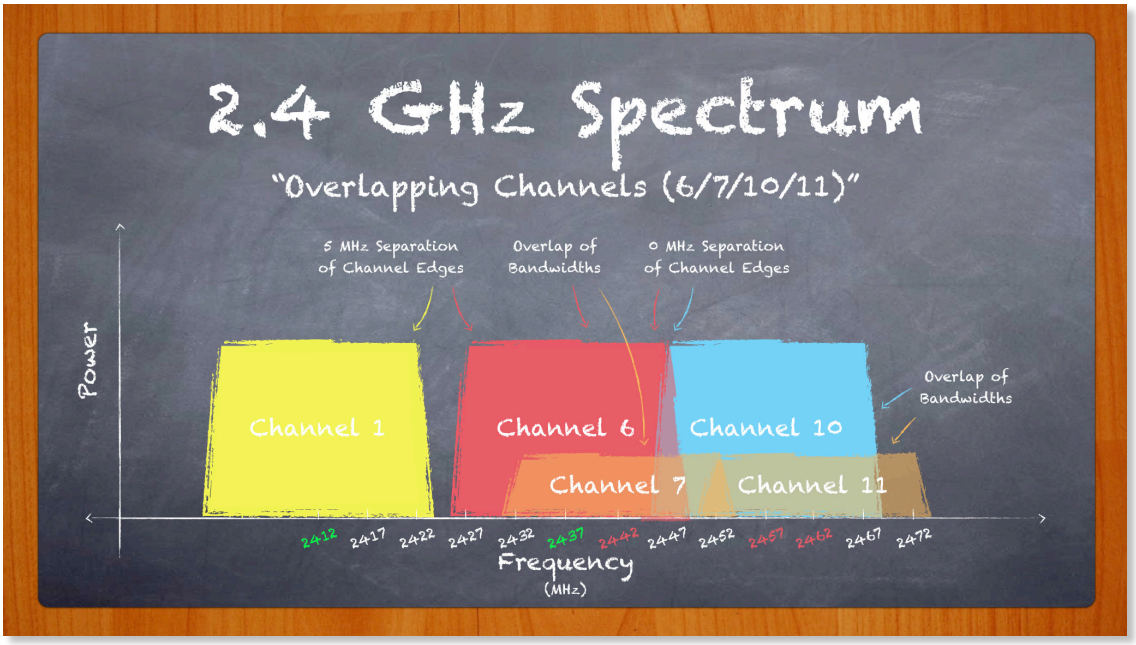
The following figure demonstrates two APs in competing WLANs. The 20MHz WLAN (blue channel) is centered at frequency "f", while the 40 MHz WLAN (yellow channel) actually bonds two 20 MHz channels together. Of the two 20MHz channels, the primary channel (centered at frequency "f") contains the WLAN beacon announcements, while the secondary channel is optional for compatible, connecting Stations.

The 'tail ends' of adjacent channels can incur noise for nearby wireless networks. For this reason, it is very important to apply a channel planning pattern across the WLAN, to avoid co-channel interference (which reduces speeds and limits the scalability of the network).



The yellow WLAN depicted in the chalkboard graphic represents a 'bonded' 40 MHz channel (20+20) according to the 2009-802.11n standard. With bonded channels, 802.11n capable stations can communicate at higher data rates, called "High Throughput" (HT) rates. By comparison, the 802.11ac standard supports 'bonded' 80MHz channels (20+20+20+20) for "Very High Throughput" (VHT) data rates. A wireless network whose clients all support the same data rates is called 'Greenfield'. For example, a greenfield VHT network would only be comprised of 802.11ac stations.

Channel availability depends on the world region where the radio will be deployed and is specified in the UniFi Controller under Country Site Settings. In 2.4 GHz deployment scenarios with multiple APs, use only 20 MHz bandwidths on channels 1, 6 and 11, since use of other channels (ex. 3, 5, 9) or larger bandwidths (ex. 40 MHz) overlaps with neighbor channels. In other words, channels 1,6, and 11 allow for proper channel re-use patterns. Contrast this with a channel plan that uses overlapping channels, as illustrated by the image below.



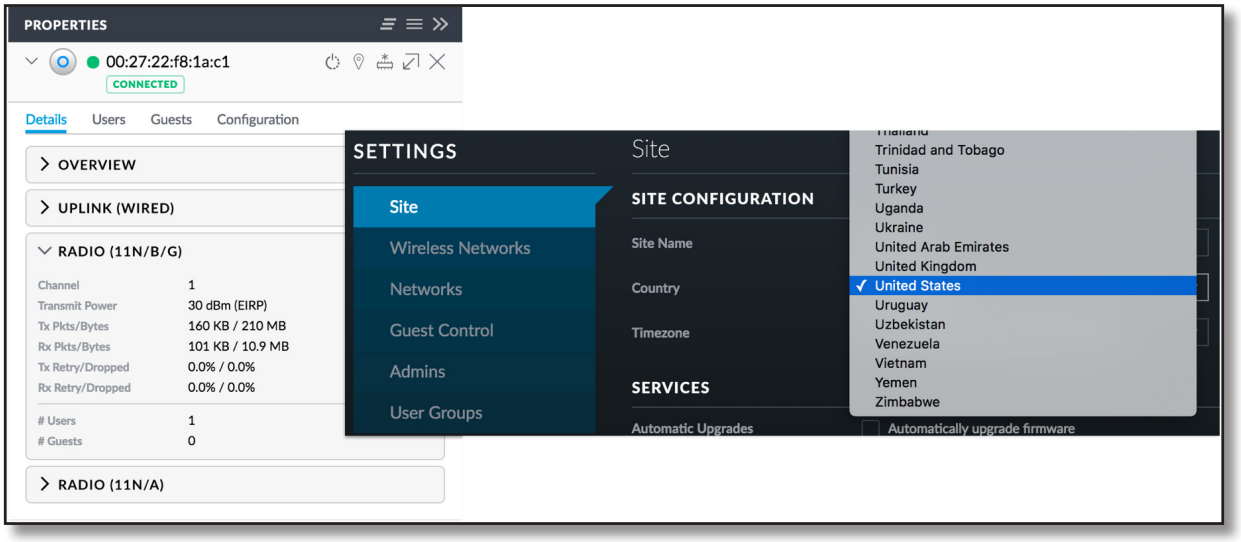
Given its worldwide support of an abundant number of channels, the 5 GHz band allows for more complex 20 MHz channel re-use patterns (as illustrated by the seven neighboring wireless cells. The wider range of available frequencies in the 5 GHz band also permits wider channel assignment (as illustrated in the previous graphic), including 40 and 80 MHz, for greater WLAN throughput. Because wider channel bandwidths require more channel space, be conscious limits the ability of the WLAN administrator to create effective channel re-use patterns across the wireless coverage area.

In order to minimize interference, assign non-adjacent channels to neighboring AP cells. When followed, the WLAN can scale more effectively. When disobeyed, WLANs cannot scale and result in poor performance (higher latency, lower throughput).

Before assigning WLAN channels, conduct site surveys to analyze noise levels across the spectrum. 2nd Generation 802.11ac UAPs feature RF Scan tools to help WLAN administrators decide the best channel, based on all sources of interference, including competing, in-band WLANs, EMI (electromagnetic interference), etc.

Regulatory Bodies & EIRP

Despite using worldwide unlicensed bands, wireless networks must comply with regulation and norms set by regional governments. Organizations like the FCC and ETSI are responsible for both creating and enforcing these rules. Wireless operators that do not comply with these laws face penalties ranging from fines to prison time. Fortunately, Ubiquiti's Compliance teams make sure that the listed channels for your UniFi radios legally operate according to the available channels, bandwidths, and power limits in your region. As long as your UniFi hardware is adopted to a Site whose settings are configured to the correct country, your hardware should operate legally.



Check the *Properties* settings for your UniFi AP to see its EIRP level (in dBm). To determine its actual Transmit (TX) Power level (in dBm), subtract its Antenna Gain (in dBi) from its EIRP (in dBm). The Transmit Power for the UAP-AC-LITE pictured in the previous image is 27 dBm, since the EIRP = 30 dBm and its Antenna Gain = 3 dBi.

WLAN Standards

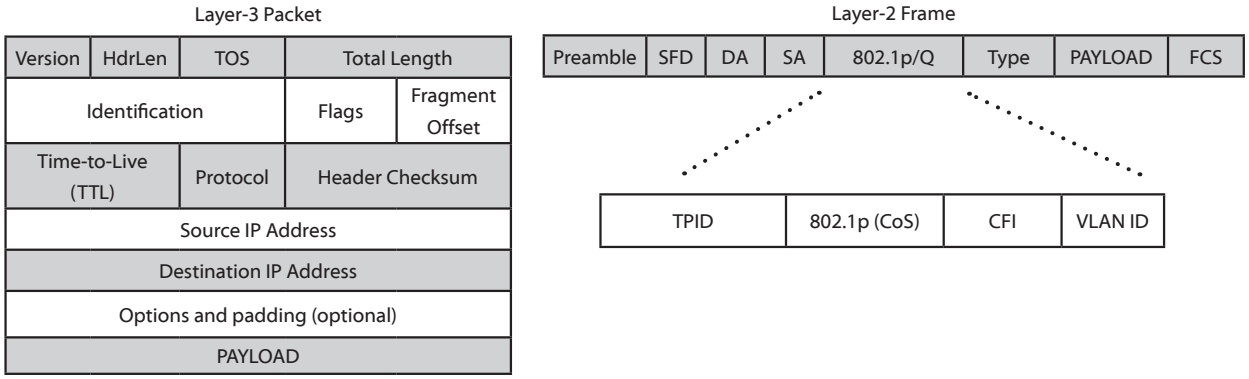
The IEEE published the first 802.11 WLAN standard in 1997, which earned it a reputation as slow and somewhat unreliable. Subsequently, the standard underwent several revisions that improved the overall speed, functionality and reliability, while following an alphabetical order: a, b, g, n, and now, ac.

WLAN Protocol	Frequency	Total Bandwidth	Max Data Rate (x Streams)	Modulation
802.11 (June 1997)	2.4 GHz	22 MHz	2 Mbps (x1)	DSSS, FHSS
802.11a (Sept. 1997)	5 GHz	20 MHz	54 Mbps (x1)	OFDM
802.11b (Sept. 1999)	2.4 GHz	22 MHz	11 Mbps (x1)	DSSS
802.11g (June 2003)	2.4 GHz	20 MHz	54 Mbps (x1)	DSSS, OFDM
802.11n (Oct. 2009)	2.4 GHz	20 MHz	72.2 Mbps (x4)	OFDM (Up to 64 QAM)
		40 MHz	150 Mbps (x4)	
	5 GHz	20 MHz	72.2 Mbps (x4)	
		40 MHz	150 Mbps (x4)	
802.11ac (First Draft 2013) (Second Draft 2014*)	5 GHz	20 MHz	87.6 Mbps (x8)	OFDM (Up to 256 QAM)
		40 MHz	200 Mbps (x8)	
		80 MHz	433.3 Mbps (x8)	
		160 MHz*	866.7 Mbps (x8*)	

In supporting newer, improved protocols, the latest 802.11n/ac networks are backwards-compatible, meaning they support older, "legacy" devices (802.11b/g) for mixed device operation. Additionally, Ubiquiti employs proprietary mechanisms on UniFi APs in mixed network mode to ensure the highest possible performance, even with legacy devices present.

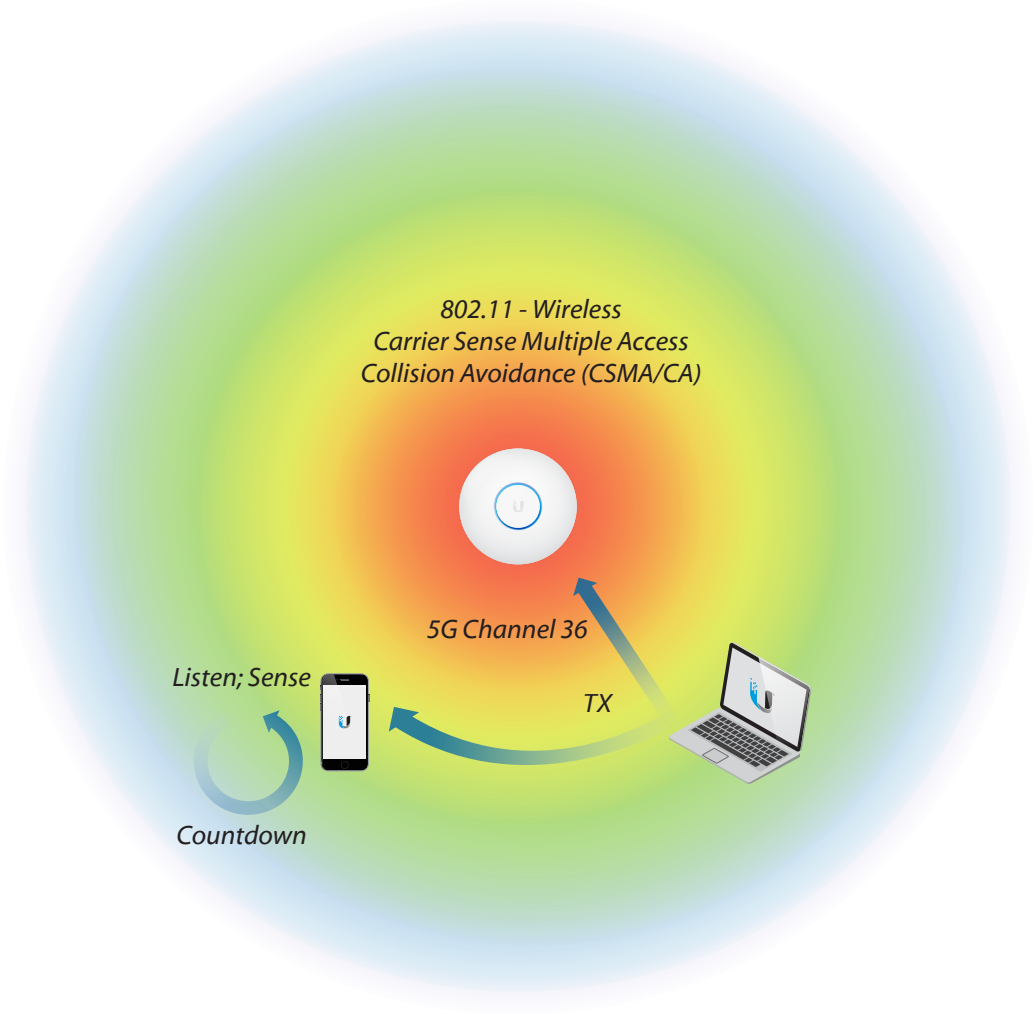
Historically, WLANs have struggled to compete with wired networks given the speed, reliability and other practical problems. Notwithstanding past shortcomings, wireless performance has improved dramatically and now stands to compete with wired networks on a much larger scale. Offering faster speeds and greater range than its predecessor, 802.11n shattered expectations for 2G & 5G wireless networking through new technologies such as MIMO operation, frame aggregation and channel bonding. 802.11ac further increases the throughput and performance enhancements first introduced by 802.11n, albeit in 5G networks only. At a cost-disruptive price point, Ubiquiti UAP-AC products bring true Gigabit and scalable enterprise wireless networking to the masses.

One important characteristic of a high performance network is QoS (Quality of Service). Using QoS parameters, certain network traffic can be prioritized over other less important traffic. This is especially useful for enterprise networks seeking to provide the highest possible performance with applications that demand low latency, jitter or packet loss, such as streaming video, VoIP, or online gaming. WMM (Wi-Fi Multimedia) defines QoS standards for wireless networks based on a DSCP (Differentiated Services Code Point) value in the packet header. Higher values like voice and video receive priority over lower values like background and best effort. The DSCP values respected by UniFi are listed in the Appendices of your Student Manual.



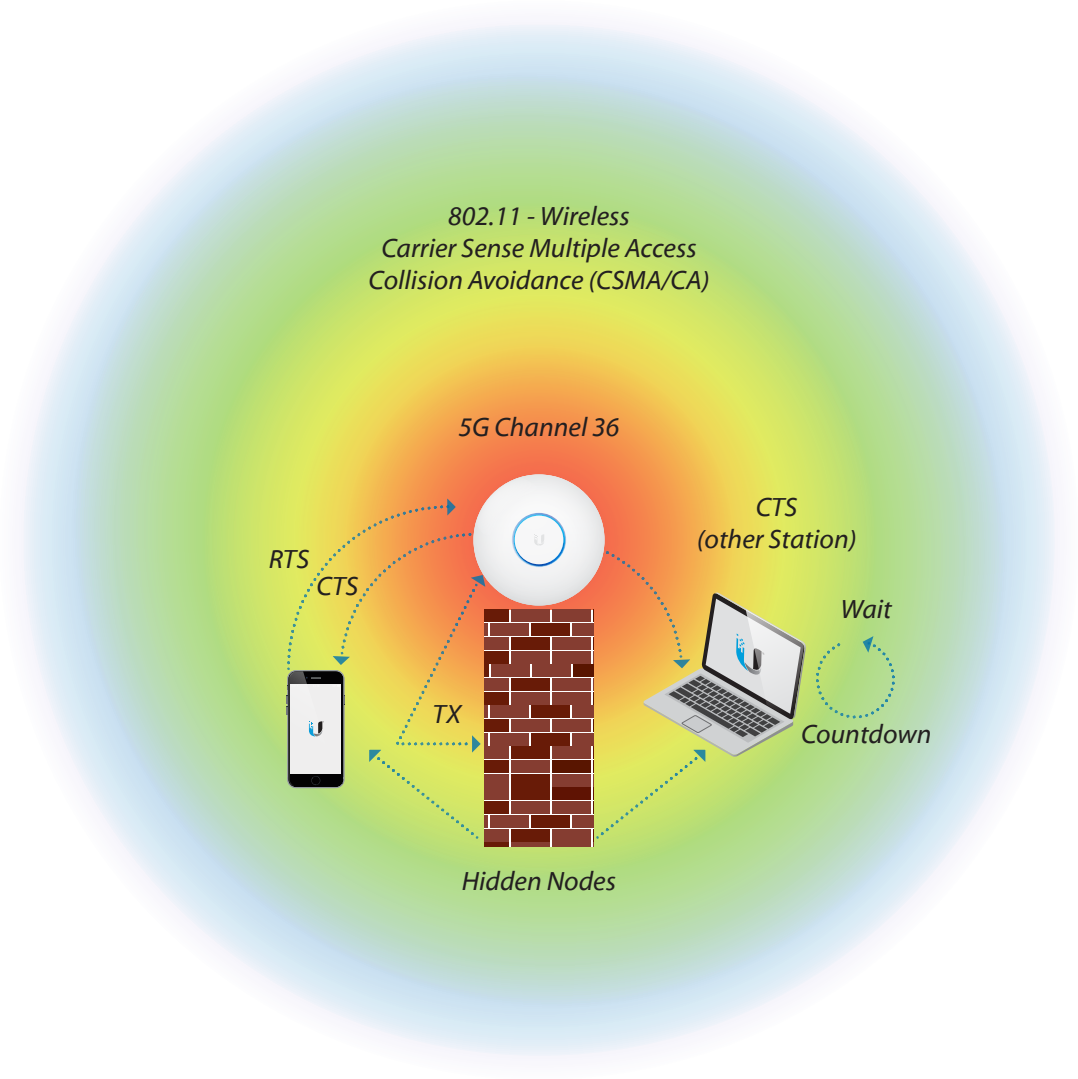
Wireless Access Methods

The 802.11 standard is based on the CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) protocol. Similar to a group conversation where participants wait to talk until one person finishes talking, 802.11 clients will listen to the wireless channel prior to transmitting frames (data). If the wireless channel is available, then the station transmits. But if the wireless channel is occupied, then the station will start a random countdown timer, after which, it will listen again before attempting to transmit. In this way, stations compete for access to the wireless medium. In the event that two stations listen and transmit simultaneously, the receiver may experience a collision and data will need to be re-transmitted.



As more and more stations are added to the wireless network, the likelihood of a collision increases. The probability of a collision also increases whenever the distance between stations is so great that they cannot hear each other. This can also occur if obstacles exist between stations. This is known as the hidden node problem. For example, if Station A is close to the AP but far from Station B who is talking, Station A will wrongfully assume that the wireless channel is available and transmit, causing problems (collisions) at the listening AP.

The 802.11 protocol partially overcomes this problem through a mechanism known as RTS/CTS (Request to Send/Clear to Send). Whenever a station needs to send data, it first sends an RTS frame indicating how much data it would like to send. Upon receiving the RTS frame, the access point will reply with a CTS frame, announcing to all stations that the channel will be occupied for the time it would take for the station to pass the data. Then, the station begins delivering data, after which the recipient acknowledges successful delivery using acknowledgement (ACK) replies. RTS/CTS isn't always used in 802.11 communication, like when the payload (packet size) is too small.

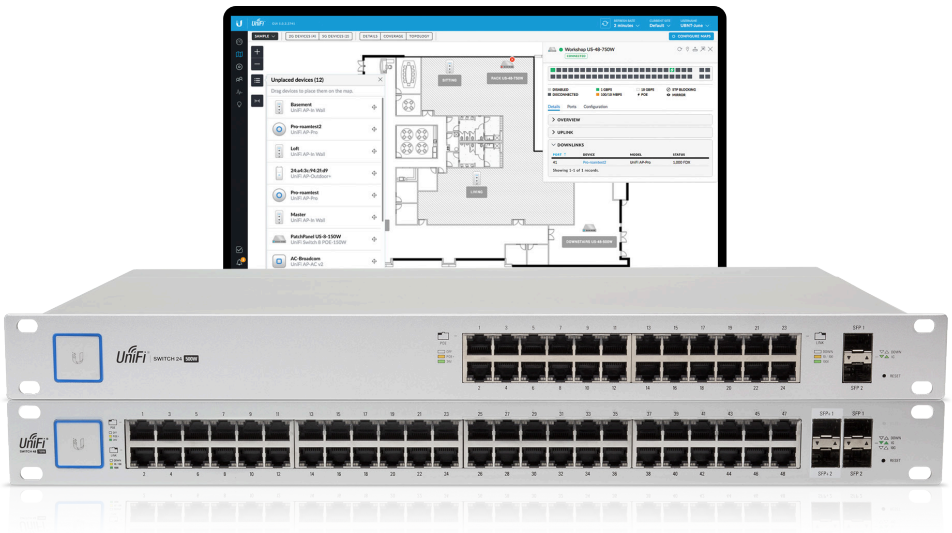


In summary, 802.11 wireless networks are based on listen first, then talk design. “Wi-Fi” radios like UniFi Access Points are half-duplex, meaning they can either transmit or receive, but neither communicate simultaneously. Compared to switches, wireless radios feature a single collision domain shared among stations competing for channel usage.

Network Equipment

Regardless of the requirements for your enterprise deployment, Ubiquiti UniFi products feature all the necessary features to manage networks at competitive hardware pricing, without costs due to software licensing. Besides the popular UniFi Access Points, Ubiquiti makes Enterprise grade switches, routers, and other equipment for every type of network scenario.

Switches are the building blocks of every local area network. Not only are switches useful for expanding the Layer-2 broadcast domain, but managed switches provide features that are crucial for monitoring the LAN. Managed switches like Ubiquiti UniFi Switches grant network admins total control over switch-based functions, such as Power-over-Ethernet (POE), Port Operation mode (switching, mirroring, or aggregate), Network/VLAN configuration, Jumbo frame and flow control services, Port Storm Controls, Spanning Tree Configuration, and more. UniFi Switches feature a friendly graphic user interface for making quick changes to switch operation.



Routers move packets between networks, and therefore lie at the core and edge of every enterprise network. Gateways are routers that link to the Internet, and therefore move packets between devices on the Local Area Network (LAN) and the Wide Area Network (WAN). The UniFi Security Gateway combines reliable security features with high-performance routing technology in a cost-effective unit, including DHCP, DNS Forwarding, VPN services, powerful firewalls, QoS for Enterprise VoIP/Video, as well as Deep Packet Inspection (DPI). Ubiquiti EdgeRouters are also popular for their low hardware costs, routing protocol support (Static, ECMP, OSPF, BGP, MPLS) as well as WAN load-balancing capabilities.

Powered by 48V PoE (802.3af/at & Passive), the UniFi Cloud Key (UC-CK) securely runs a local instance of the controller software and features cloud SSO for remote access on unifi.ubnt.com. The free UniFi controller software can also be installed on standalone servers, for cloud-based hosting, or even local machines like your laptop.

III. WLAN Planning

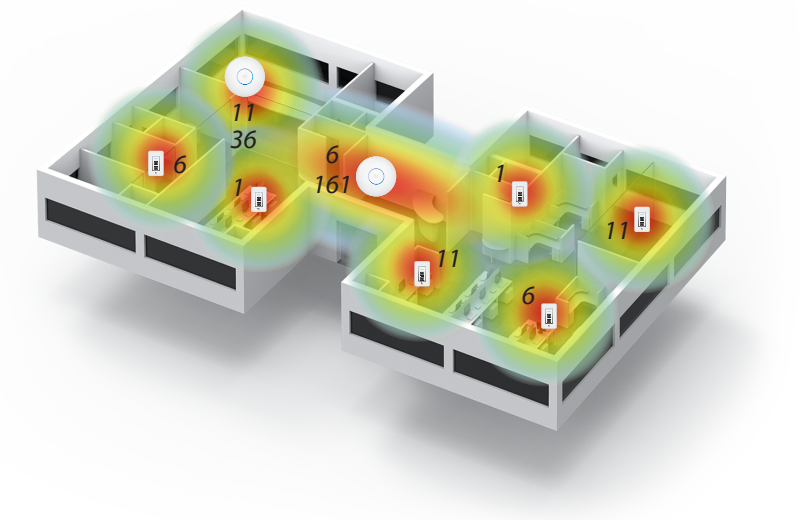
Application Overview

With a basic understanding of wireless physics and the access methods for WLANs, admins can embrace the fundamentally important task of planning the wireless network. A complete consideration of both present and future needs of the network clients is the first step to planning the WLAN. Such knowledge is crucial in estimating the capacity and density of the wireless network and will ultimately help in planning more abstract parts of the WLAN such as signals, coverage and overlap.

Initial planning should seek to answer the following questions:

- Total number of users and density (corporate/guests? 10/100/1000+?)
- Bandwidth requirements of users (file sharing/browsing? 1/2/5/10 Mbps?)
- Application needs of clients (browser/video/VoIP?)
- Growth of WLAN (area/bandwidth/number of users? 1/3/5+ years?)
- Security (open/personal/enterprise? password/hotspot? SSL certificates?)
- Coverage areas (room/building/field/city?)
- Density (sparse/crowded? AP/stations? Number of devices per user?)
- Roaming (fixed or mobile users? amount of cell overlap?)
- Types of UAPs (regular/long-range? single/dual-band?)
- Types of antennas (internal/external? low/hi-gain?)
- Physical location (urban/rural? indoor/outdoor?)
- Band steering (Legacy on 2.4 GHz? N/AC on 5 GHz? 2.4 GHz voice? 5 GHz data?)
- Obstacles (desks/people/trees/signs/doors/walls/windows?)

The wireless concepts explored in this manual will prepare you to plan and develop functional, high-performance UAP networks, regardless of application. Site surveys are very helpful in planning WLANs for the information they provide about the WLAN environment and will be covered in the next chapter: Deployment.

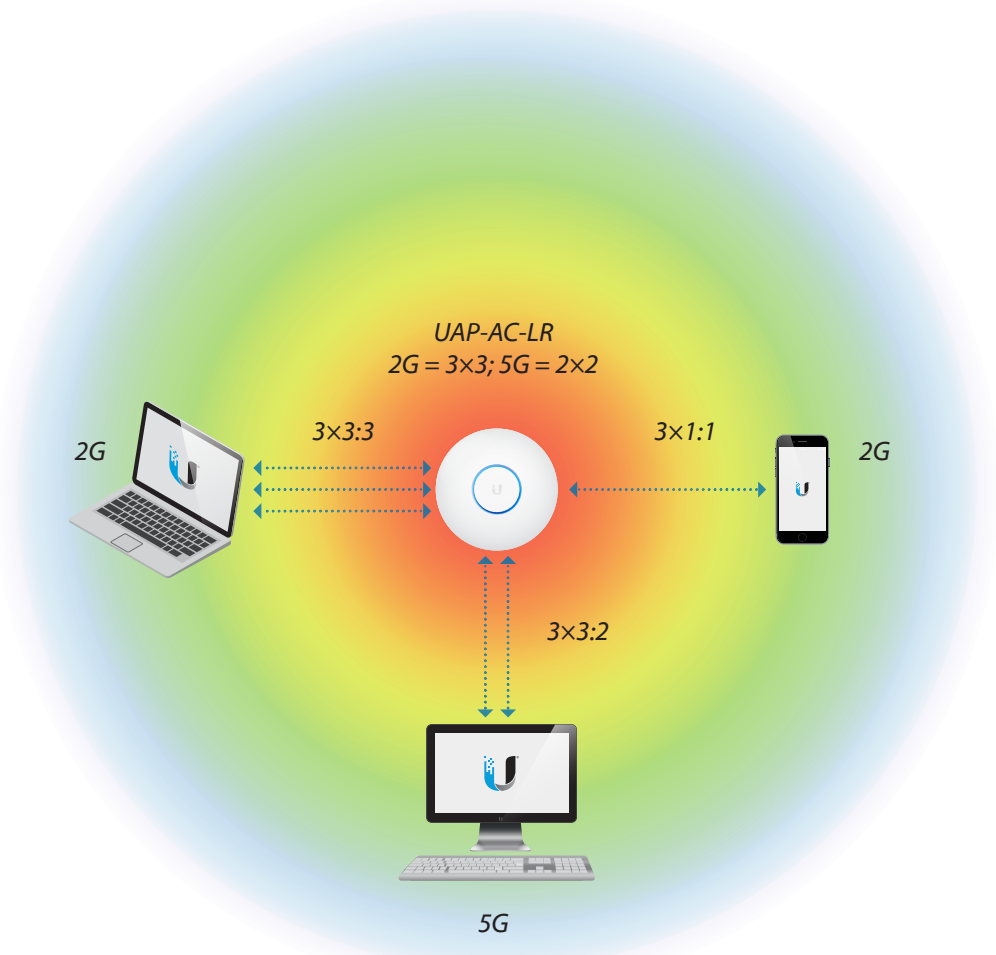


Wireless Technology

Ubiquiti Networks manufactures different UniFi AP models with unique characteristics to match the needs of any enterprise network. Indoor UAP models are ideal for hotels, schools, and hospitals while outdoor UAP models are more suitable for campgrounds, marinas or campuses. Due to its advanced filter technology, the UAP-Outdoor+ is especially well suited for high-density settings such as concerts, trade shows, sporting events, etc.

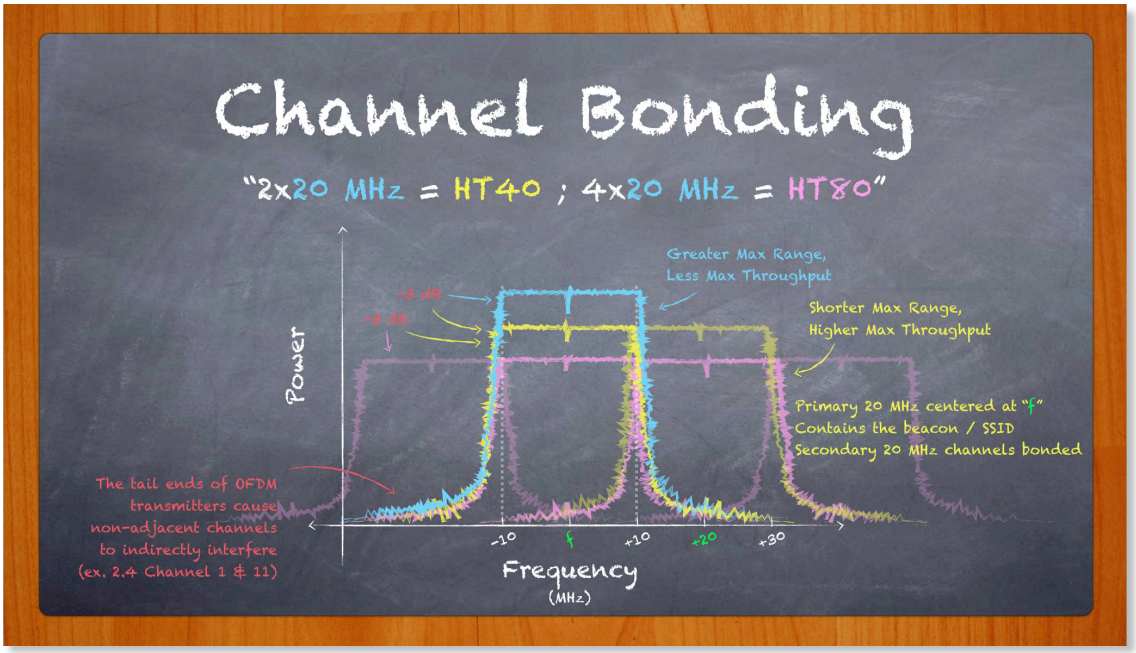
Among the most important, defining characteristics of the UniFi AP family are their MIMO capabilities and supported 802.11 standards. MIMO (multiple-input, multiple-output) relates the number of transmitter and receiver antennas, followed by the maximum supported data streams. The formula TxR:s describes the MIMO operation of a wireless station, where:

- "T" = Number of transmit antennas
- "R" = Number of receive antennas
- "s" = Number of spatial data stream



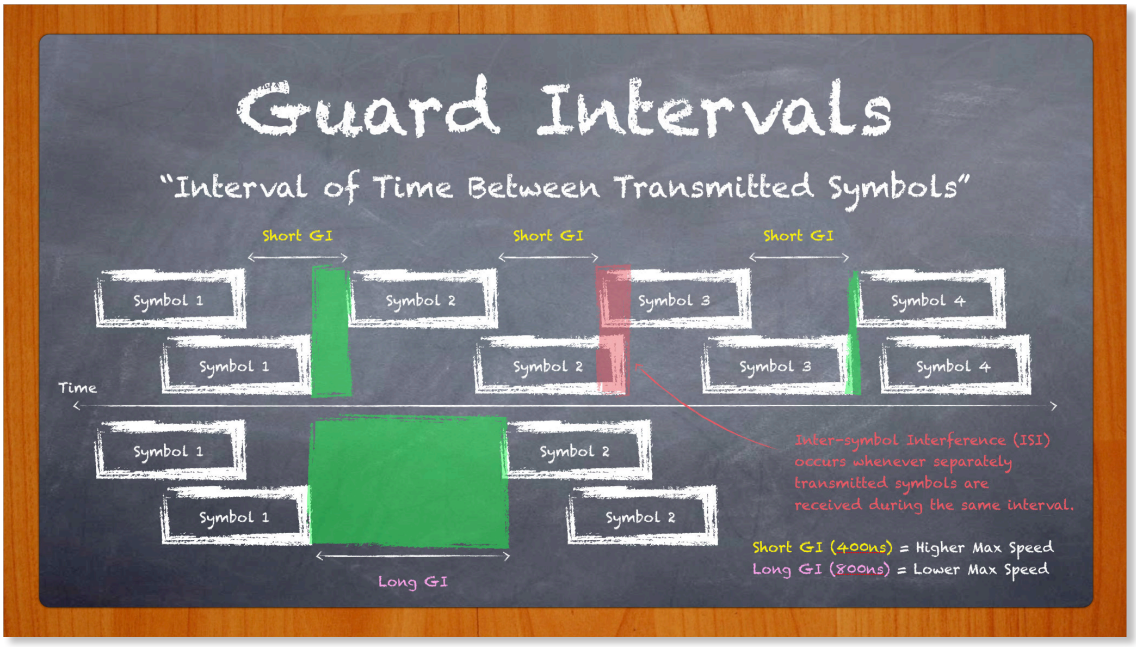
Ubiquiti UAPs use the latest MIMO and 802.11-specific technologies to achieve high performance wireless communication, being backwards-compatible with previous 802.11 versions. They also make use of Ubiquiti proprietary technologies that empower wireless networks unlike ever before:

- **Channel Bonding** – 802.11n/ac hardware supports 'Channel Bonding,' a Physical-Layer enhancement that permits wireless stations to use larger channel bandwidths for potentially higher throughput. HT40, HT80 and HT160 call for High Throughput operation with bonded 40 MHz, 80 MHz and 160 MHz, respectively. However, larger bandwidths mean more spectrum is used, so fewer channels are available for reuse patterns. Also, the peak power density is spread across a wider channel, resulting in shorter range.



- **Spatial Multiplexing** – Multiple transmitters send space and/or time differentiated signals to multiple receivers for multiplexed data within the same frequency band. As an example, the UAP-PRO supports MIMO 3x3:3 operation on its 2.4 GHz radio, meaning it transmits or receives up to three multiplexed data streams across three antennas, reaching speeds as high as 450 Mbps.
- **Diversity and Maximal Ratio Combining (MRC)** – Multiple, identical receive signals across antennas are independently processed and combined, resulting in an increase in desired signal and a reduction in out-of-phase signals. More antennas mean greater potential to boost the receive signal. In this way, a 3x3 AP has inherent advantages over 2x2 APs, even when communicating with stations using two or fewer spatial streams.

- **Guard Interval** – 802.11n/ac drafts specify optional, shorter time intervals between transmitted symbols. Longer Guard Intervals (800ns) result in lower data rates but are less likely to incur intersymbol interference. This differs from interframe spacing (IFS) which is the time between transmitted packets. Guard Intervals are a dynamic setting that UniFi APs and clients will automatically manage. Long and short Guard Intervals are represented in the Data Rate tables in the indices of this student manual.



The latest MIMO and 802.11 features combined with Ubiquiti's proprietary technologies maximize the potential for the best signals and highest data rates across the entire wireless network. Ubiquiti's 802.11ac access points finally make possible Gigabit speeds over-the-air through a culmination of high-performance standards including larger channel bandwidths, support for more spatial streams and more advanced modulation. Compared to Ubiquiti's advanced enterprise wireless access points, other vendor APs can create bottlenecks and limit the network from reaching its full potential.

In reality, the performance of a wireless network is two-fold dependent on access points as well as client devices. The collective characteristics of 802.11 WLANs and their environment determine the ability of these APs and clients to communicate at high speeds, with low latency, and without connectivity issues.

Signals & Coverage

Decibels (dB) are ratios comparing a real-world value to an order of magnitude. In this way, a very large or very small value can be represented by a simple decibel value. “Decibels over milliWatts” (“dBm,” for short) represent the energy intensity of a wireless signal. The data signal generated by a transmitter reaches an intensity called Transmit (TX) Power level. For example, a UAP-AC-Mesh can transmit up to 20dBm (on either 2G or 5G) while client devices typically transmit at lower power levels (~10dBm).

Note to Student: Using an online Decibel calculator, you can quickly discover the milliWatt value represented by the dBm ratio. For example, 20dBm = 100mW.

Before leaving a station and passing through space, the TX Signal passes through an antenna, whose gain passively amplifies the signal. Gain (synonymous with directivity) is represented in units called “decibels over isotropic radiator” (“dBi,” for short). For example, a UAP-AC-Mesh has a combined antenna gain of 3dBi and 4dBi on 2G and 5G, respectively.

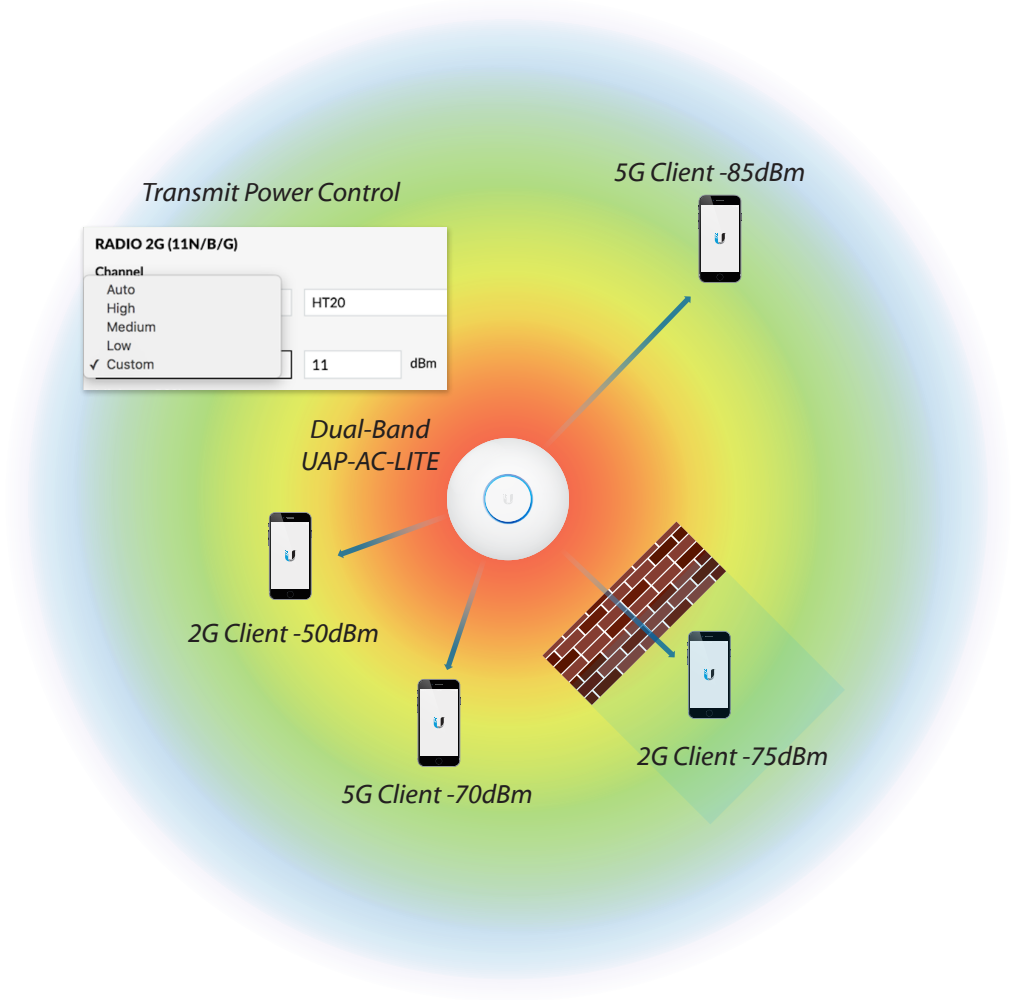
Note to Student: With a gain of 0dBi, an isotropic radiator is a theoretical radiator that emits energy equally across all planes of space. Increased antenna gain ‘focuses’ the direction in which a signal radiates. Conceptually, an isotropic radiator is like a light bulb (shines light in all directions equally) while a high gain antenna (30dBi) is like a laser (shines light in one direction with much higher intensity).

Known as EIRP (explored later), the combined decibel value of TX power and antenna gain relates the intensity of the wireless signal leaving the transmitter. For example, a UAP-AC-Mesh has a maximum 2G EIRP of 23 dBm (20dBm TX power + 3dBi TX gain).

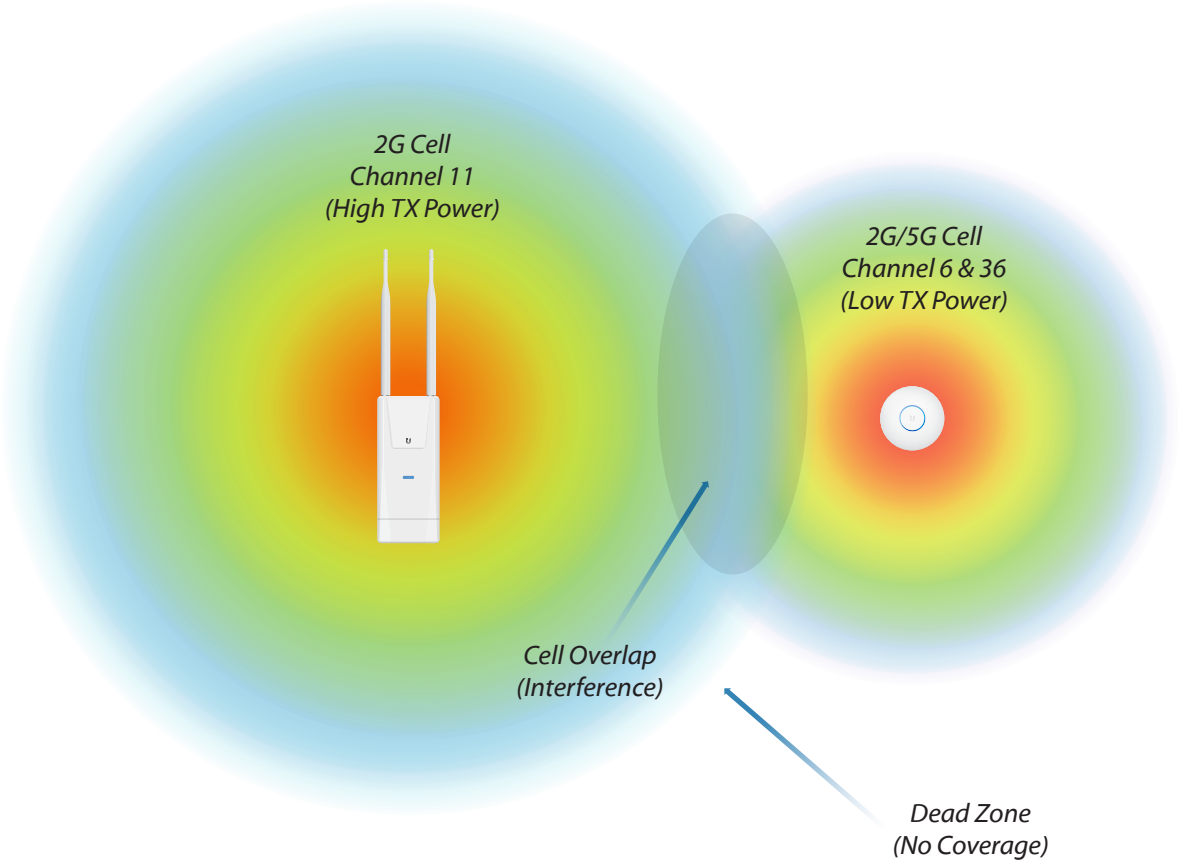
As previously mentioned, Free Space Path Loss (FSPL for short) causes a wireless signal to rapidly decrease in energy intensity as it moves through space. For example, at 1 meter distance, the combined +23 dBm 2G TX signal leaving the UAP-AC-Mesh drops to -17 dBm (because 2.4GHz FPSL at 1 meter distance = 40dB); at 10 meter distance, the signal drops to -37 dBm.

Note to Student: The - sign in front of the transmitted signal (ex. -17 dBm) does not represent a ‘negative’ value, instead, a decimal value. For example, -17 dBm = .02mW; -37dBm = .00002mW.

In general, signals around -50 dBm are considered excellent, while signals lower than -75 dBm are considered weak. However, more important than a strong signal is the actual difference in signal & noise levels—called signal-to-noise ratio (SNR) that determines wireless speeds and user performance. Although some amount of cell overlap is necessary between neighbor WLAN cells to allow clients to roam without extended disconnectivity, too much overlap can severely hinder the performance of WLANs and limit the scalability.



The purpose of any access point is to provide wireless coverage to clients over a given area known as a cell. As a WLAN station moves away from the AP, its receive signal gradually weakens. This also occurs as obstacles prevent direct line-of-sight between AP and station. As signals decrease, wireless performance drops before eventually, the station becomes disconnected from the AP. This is due to the Free Space Path Loss (FSPL) relationship as mentioned previously.



In the past, greater emphasis was placed on producing a large wireless coverage area over creating a high performance network. As a result of bringing on more distant clients with low signals, WLANs became crippled beneath increased latency, poor speeds and diminished scalability. However, present-day wireless LANs are most concerned with providing the best possible performance. To do so, WLANs target close-range clients with the best signals, since signal strength is a key indicator of network performance. When connected stations have strong signals, the WLAN works faster, more reliably and can scale to add more clients.

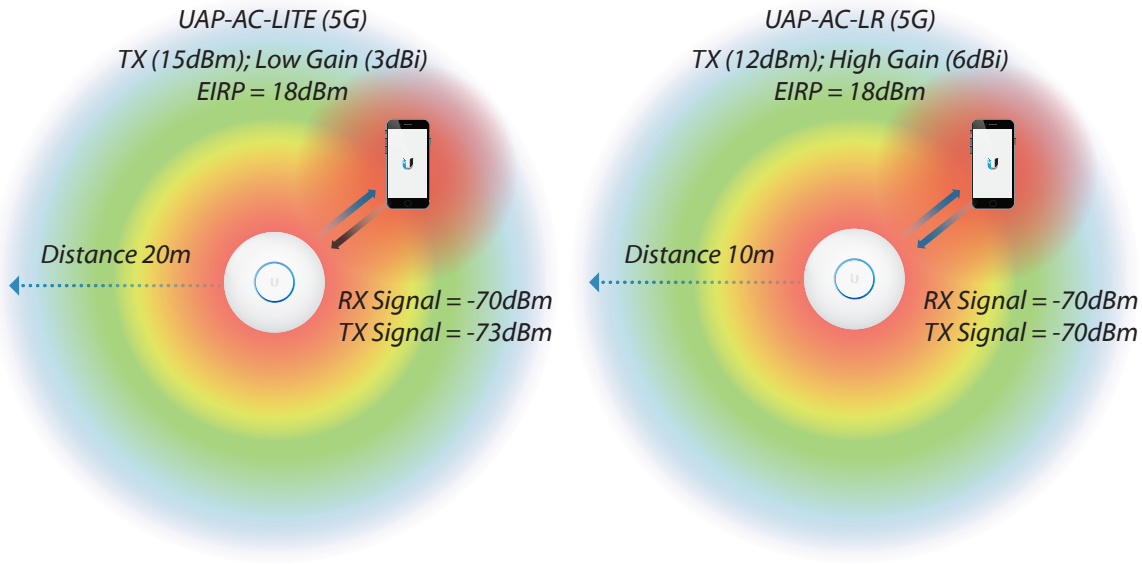
Characteristics	Large Cell	Small Cell
Objective	Coverage	Density
Transmit Power	High	Low
Best Frequency	2G	5G
Avg. Signal	Mid-Weak	Strong
Avg. Speeds	Lower	Higher
Deployment Complexity	Low	High
Hardware Recommendation	UAP-AC-PRO UAP-AC-M-PRO	UAP-AC-HD UAP-AC-M with 5G airMAX sector (disable 2G radio)

Coverage and capacity have a dichotomous relationship. Smaller cells are more likely to encounter close-range wireless clients with higher signals, while larger cells are designed to pick up long-range clients with lower signals. The application needs of the network should ultimately determine how and where APs should be deployed across the WLAN environment.

Three characteristics of access points that affect propagation/cell size include radio frequency, TX power and antenna gain.

1. **Frequency**- As previously discussed, lower frequency signals propagate better than high frequency signals. For this reason, 5 GHz networks are ideally-suited for high-density deployments, while 2.4 GHz networks are better in scenarios where greater coverage is desired. Depending on the type of deployment, walls and barriers can either help or hinder the WLAN. By strategically placing co-located UAPs between and around obstacles, administrators can create coverage areas to meet expectations for the wireless LAN deployment.
2. **TX Power**- TX power works similarly to the volume setting on a stereo. By adjusting the TX power of a UAP, WLAN administrators can increase/decrease cell size accordingly. As high-powered devices, UAPs can transmit at notably high-power levels to reach distant clients. However, wireless communication is bi-directional, meaning both the AP and client must hear each other at reasonable signal levels to maintain reliable connectivity. For this reason, low-power clients such as laptops, tablets and smartphones can often limit the maximum size of a wireless cell.

   To ensure that APs and clients can hear each other at similar signal levels, the UAP's TX power level may need to be decreased. By default, UAPs are set to Auto. Choose between high/medium/low or custom TX settings.
3. **Antenna Gain**- Gain measures an antenna's ability to radiate (focus) power into a particular direction. Compared to TX Power, which only increases the signal in one direction, antenna gain increases the signal in both directions. Rather than overextend cell size, reduce TX power to client levels & increase antenna gain. Pairing a UAP-AC-M with an external, hi-gain antenna is a very efficient way to improve signals across the WLAN.



The antenna gain diagrams represent a three-dimensional area over which wireless signals propagate. Indoor as well as outdoor UniFi access points feature 'omnidirectional' antennas that produce a radiation pattern similar to a 'donut' shape.

The left figure represents the horizontal plane (azimuth plot) of a UAP-AC-PRO's 2.4 GHz antennas. The right figure represents the vertical plane (elevation plot) of the same. The two plots together reveal the three-dimensional radiation area of the 2.4 GHz antennas on the UAP-AC-PRO. Imagine a donut shape that reaches 360° on the horizontal plane but has short height lobes on the vertical plane.

EIRP represents the combined transmit power level and antenna gain for the AP. When setting TX power high/medium/low, the actual TX power level (in dBm) can be found by subtracting the UAP's antenna gain from the reported EIRP. Maximum EIRP is dependent on frequency and cannot exceed the threshold established by regional governments. Make sure that the correct country code is selected for each UniFi site. The below image expresses the EIRP of the UniFi AP based on the TX Power and antenna gain. Find the TX Power (20 dBm) by subtracting the antenna gain of UAP-Regular (3 dBi) from the EIRP total (23 dBm).

Due to their lower power levels, client devices often limit cell size. A common symptom of a cell with overextended coverage is when the high-power AP's SSID is visible but the low-power client cannot connect. And if the client connects, the low RX signal at the AP causes a mismatch in upstream vs. downstream speeds.

Cell Channel Assignments

After determining the cell sizes, wireless admins can begin to assign channel assignments to cells across the coverage area. When choosing channels, not only should operators know which channels are legally available, but also which channels have the lowest noise floor. Ubiquiti's compliance team regularly updates its products to operate within the legal boundaries where the equipment may be used. Therefore, it's always recommended to select the correct country code when first installing the UniFi software. Measuring noise floors will be explored further in the Deployment chapter under Site Surveys.

To reduce neighbor cells from self-interfering, whether via Adjacent Channel Interference, or due to Co-Channel Interference, apply a channel reuse pattern throughout the WLAN. The unlicensed, 2.4 GHz band features just 83 MHz of available spectrum for approximately three separate 20 MHz channels. Comparatively, the unlicensed 5 GHz band features as much as 300 MHz of available spectrum (depending on region) for many separate 20 MHz channels. It is only recommended you use bonded channels (40 MHz) in the 5 GHz spectrum, since no reuse pattern can be effectively used with 40 MHz channels in the 2.4 GHz spectrum.

Noise

As a principle of building WLANs, place equal emphasis on keeping noise levels low as well as keeping receive signals high. After all, the key to a high performance WLAN is high SNR across all clients. In order to not overload receiver radios, avoid positioning stations under a few centimeters distance from the access point since this can cause performance-related problems and degrade the radios over time (receive signals should never exceed -10 dBm).

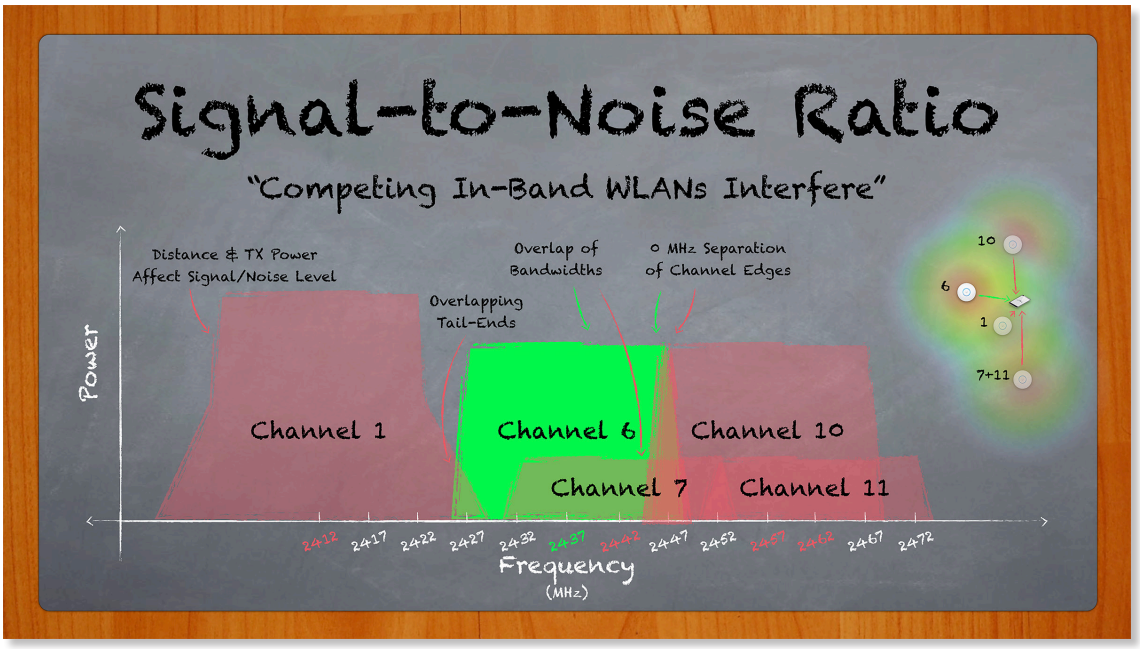
In order to maintain a low noise floor, operators must first understand what are the sources of noise. The true noise floor of a wireless network is the sum of four factors including:

- Thermal noise
- In-band interference
- Receiver noise
- Electromagnetic interference (EMI)

Noise Source	Cause	Recommendations
Thermal Noise	Inherent physical noise related to size of WLAN channel.	Use HT20 in high noise environments. Where noise is lowest, deploy HT40/80 WLANs.
Competing In-Band WLANs	Noise from nearby, same and/or adjacent channel WLANs.	Use non-overlapping channel re-use patterns. Provide sufficient spacing between neighboring cells sizes. Client devices also raise noise floor.
RX Noise	Noise generated by receiver radio during normal operation.	Use Ubiquiti UAPs for high quality radio performance.
Electromagnetic Interference (EMI)	Energy from sources of EMI (ex. microwave oven, wireless IP cameras).	More common to 2.4 GHz band. Limit proximity to EMI sources around the WLAN. Mount UAPs in strategic locations.

WLAN operators are responsible for controlling these noise factors and should conduct site surveys to measure noise levels long before deployment. Site surveys will be thoroughly discussed in the Deployment chapter. If signals and noise floor are overlooked, stations will experience poor SNR, resulting in higher latency, lower throughput and packet loss.

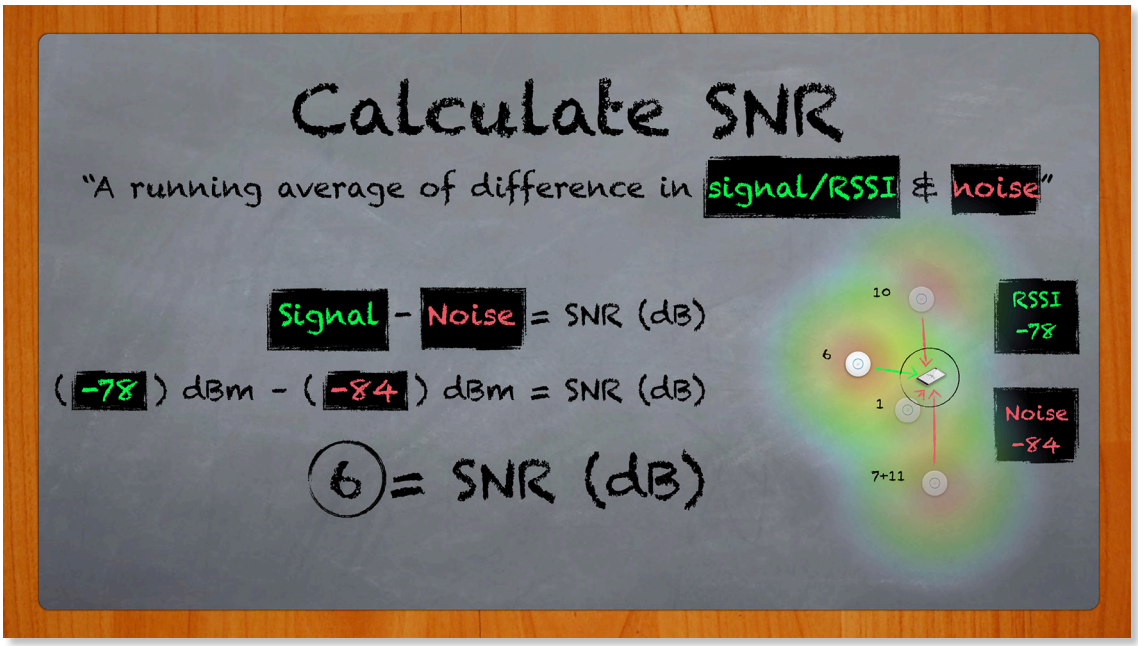
Signal-to-Noise Ratio (SNR)



The signal arriving at the intended wireless station is known as the receive signal (energy from transmitter). Due to path loss and propagation characteristics, signals incur greater loss as the distance and/or number of obstructions increases between transmitter and receiver. Although signals play an important part in the performance of a Wireless LAN, it is actually the Signal-to-Noise Ratio (SNR, dB) that determines what data rates are achievable. That is, the difference in Receive Signal (dBm) and Noise Level (dBm).

SNR is a dynamic value. In the presence of competing wireless signals, APs and client stations may encounter difficulty 'hearing' the intended receive signal due to the 'noisy' background. In order to achieve the best possible data rates, the SNR ratio be sufficiently high, through either a reduction in noise floor level, an increase in receive signal, or any combination of the two. The WLAN performs best when APs are deployed on uncrowded channels, and when APs/clients have sufficiently strong signals.

To calculate SNR, simply subtract the Noise Floor value from the Receive Signal, as illustrated in the following graphic:



UniFi relates SNR as a percentage value to help new WLAN admins troubleshoot the connected stations in their network. Just like SNR, which is a dynamically changing value, the Signal % of a client device may increase or decrease accordingly and in real-time. To derive the SNR reported by the Signal % value, the following formula may be used:

SNR = x

If x ≥ 45, then x = 45

If 5 ≤ x ≤ 45, then x = x

If x ≤ 5, then x = 5

Return ((x-5) / 40) * 99.toPrecision(2) + '%' = Signal %

Example: When RSSI is 29 dB, what is Signal %?

x = 29 since 5 < x < 45

Return ((29 - 5) / 40) * 99.toPrecision(2) + '%'

Signal = 59% (from 59.4%)

Example: When Signal % is 75%, what is RSSI?

75 = ((x - 5) / 40) * 99

30 = x - 5

35 = x (from 35.303)

As previously mentioned, SNR is the difference in receive signal and noise floor, and can vary at both AP and client station. SNR and speed are positively correlated, where the highest physical wireless data rates (PHY, for short) require strong receive signals and lower noise floor. As SNR decreases, so too do the PHY rates. When the SNR is too low, clients may even face connectivity problems. The Modulation and Coding Schemes (MCS for short) table represents the achievable PHY rates based on SNR (in the column MCS Index) and a few other important characteristics, including:

- 802.11 Version
- Channel Width
- Guard Interval
- Spatial Streams

HT MCS Index	Spatial Streams	Modulation & Coding	20MHz		40MHz		80MHz		160MHz		VHT MCS Index
			Data Rate GI=800ns	Data Rate SGI=400ns	Data Rate GI=800ns	Data Rate SGI=400ns	Data Rate GI=800ns	Data Rate SGI=400ns	Data Rate GI=800ns	Data Rate SGI=400ns	
0	1	BPSK 1/2	6.5	7.2	13.5	15	29.3	32.5	58.5	65	0
1	1	QPSK 1/2	13	14.4	27	30	58.5	65	117	130	1
2	1	QPSK 3/4	19.5	21.7	40.5	45	87.8	97.5	175.5	195	2
3	1	16-QAM 1/2	26	28.9	54	60	117	130	234	260	3
4	1	16-QAM 3/4	39	43.3	81	90	175.5	195	351	390	4
5	1	64-QAM 2/3	52	57.8	108	120	234	260	468	520	5
6	1	64-QAM 3/4	58.5	65	121.5	135	263.3	292.5	526.5	585	6
7	1	64-QAM 5/6	65	72.2	135	150	292.5	325	585	650	7
	1	256-QAM 3/4	78	86.7	162	180	351	390	702	780	8
	1	256-QAM 5/6	n/a	n/a	180	200	390	433.3	780	866.7	9
8	2	BPSK 1/2	13	14.4	27	30	58.5	65	117	130	0
9	2	QPSK 1/2	26	28.9	54	60	117	130	234	260	1
10	2	QPSK 3/4	39	43.3	81	90	175.5	195	351	390	2
11	2	16-QAM 1/2	52	57.8	108	120	234	260	468	520	3
12	2	16-QAM 3/4	78	86.7	162	180	351	390	702	780	4
13	2	64-QAM 2/3	104	115.6	216	240	468	520	936	1040	5
14	2	64-QAM 3/4	117	130.3	243	270	526.5	585	1053	1170	6
15	2	64-QAM 5/6	130	144.4	270	300	585	650	1170	1300	7
	2	256-QAM 3/4	156	173.3	324	360	702	780	1404	1560	8
	2	256-QAM 5/6	n/a	n/a	360	400	780	866.7	1560	1733.3	9
16	3	BPSK 1/2	19.5	21.7	40.5	45	87.8	97.5	175.5	195	0
17	3	QPSK 1/2	39	43.3	81	90	175.5	195	351	390	1
18	3	QPSK 3/4	58.5	65	121.5	135	263.3	292.5	526.5	585	2
19	3	16-QAM 1/2	78	86.7	162	180	351	390	702	780	3
20	3	16-QAM 3/4	117	130	243	270	526.5	585	1053	1170	4
21	3	64-QAM 2/3	156	173.3	324	360	702	780	1404	1560	5
22	3	64-QAM 3/4	175.5	195	364.5	405	n/a	n/a	1579.5	1755	6
23	3	64-QAM 5/6	195	216.7	405	450	877.5	975	1755	1950	7
	3	256-QAM 3/4	234	260	486	540	1053	1170	2106	2340	8
	3	256-QAM 5/6	260	288.9	540	600	1170	1300	n/a	n/a	9

Airtime, Capacity and Density

Airtime

Airtime defines the shared access to the wireless medium split among stations that actively send/receive traffic on the network. Airtime deals directly with the data rates of individual wireless stations. A WLAN whose clients send/receive traffic at the highest possible data rates is said to have high airtime efficiency. Furthermore, a WLAN without packet loss and high data rates means airtime is not wasted unnecessarily.

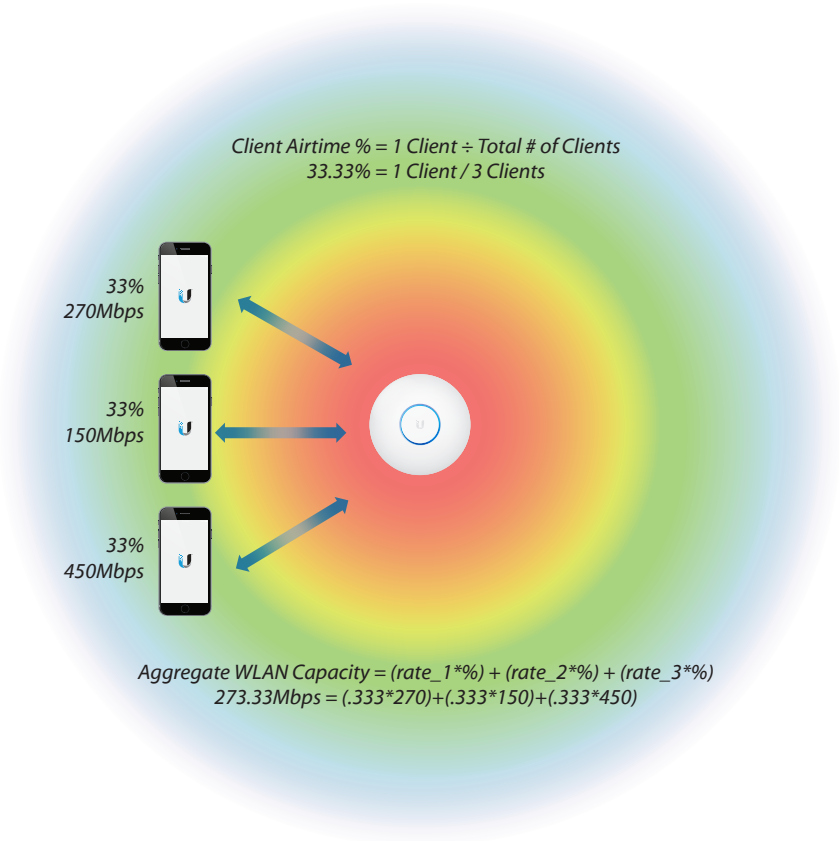
Stations use airtime on an as-needed basis. Given the shared access nature of the wireless medium, each individual station contributes to the overall airtime efficiency of the WLAN. For this reason, stations with poor data rates can jeopardize the performance of the entire WLAN. To maximize airtime efficiency, keep station signals high and whenever possible, use 802.11n/ac client equipment instead of legacy.

Due to data overhead associated with wireless protocols, actual throughput is limited to about half of a station's negotiated data rates. So a 2x2 laptop communicating with a radio at 300 Mbps data rates will reach actual TCP throughput around 150 Mbps aggregate. Due to the overhead, airtime efficiency becomes even more important to ensuring a high performance wireless network.

A simple formula for calculating each station's allocated airtime % is to divide the single AP radio by the total number of active clients.

Example: 3 active stations pass traffic on the 5GHz WLAN.

1/3 = 33%, so each of the 3 active clients receives 33% airtime.



Because the WLAN channel is shared among all clients on the WLAN, airtime is a shared concept. The airtime efficiency of every client is therefore important, affecting the aggregate capacity of the entire WLAN. Clients with low data rates need more time to transmit/receive data, leaving less time for other clients to use the WLAN channel and transmit/receive data.

Capacity

Capacity/throughput measures the total bandwidth available to stations on the wireless network. Rightly so, administrators introduce to the WLAN access points that use the latest technology. To reach the full data capacity of a UniFi WLAN, clients' devices should match the UAP's MIMO operation and 802.11n/ac protocol. Compared to the early 802.11 networks of 1997, WLANs are far more capable of meeting the data needs of today's networks. Addressing these needs is especially important as more and more users turn to wireless to support high bandwidth applications such as HD video streaming, file sharing and cloud-based storage.

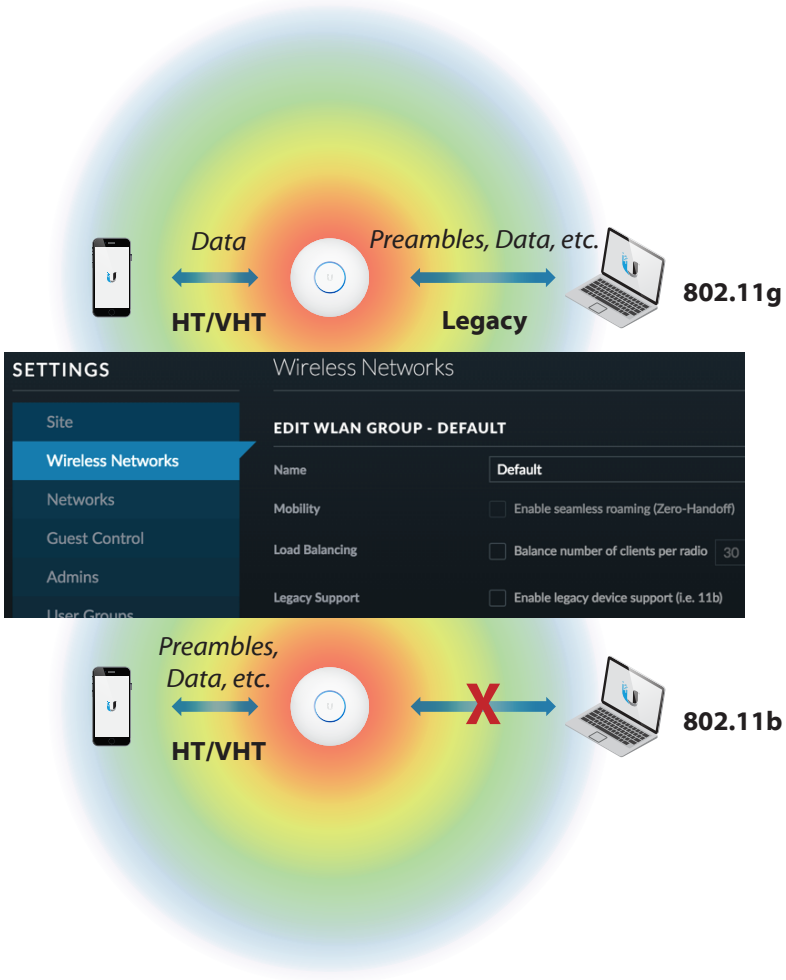
Once the allocated airtime percentage for each client is known, the approximate throughput can be calculated for each station. Recall that actual wireless throughput is about half of the advertised data rate.

Mixed vs. Greenfield Networks

As demonstrated in the previous section, the best performing wireless networks feature APs and stations that use the latest hardware and technology. For ultra-high throughput, be sure to use UAP-AC and 802.11ac-ready clients with high MIMO operation (3x3 preferred). In the absence of legacy (802.11a/b/g) devices & networks, 802.11n/ac-capable WLANs operate in Greenfield mode to achieve High Throughput (HT) or Very High Throughput (VHT) rates. As legacy devices join, WLANs operate in mixed mode, requiring protection mechanisms (ex. preamble, RTS/CTS) at slower, legacy rates to avoid collisions at the cost of throughput.

The 802.11n draft redefined the wireless protocol, introducing a Greenfield mode of operation for HT communication. However, this transmission method made HT networks unrecognizable to legacy clients, resulting in increased probability of collisions. To account for this potential problem, 802.11n networks can operate in a Mixed operation mode. While in this mode, Physical and MAC Layer protection mechanisms are applied to allow legacy and HT clients to coexist on the same wireless channel at a significant cost of throughput.

Guaranteeing a network comprised of only 802.11n/ac devices is a difficult, often unrealistic expectation for some enterprise networks. This is especially true in a bring your own device (BYOD) setting like a public hotspot where guests may introduce legacy (802.11a/b/g) equipment to the WLAN. By default, 802.11b 'legacy' devices are blocked (at time of WLAN Group creation). Legacy support for 802.11b can be enabled/disabled across select UAPs under the WLAN Group settings page.



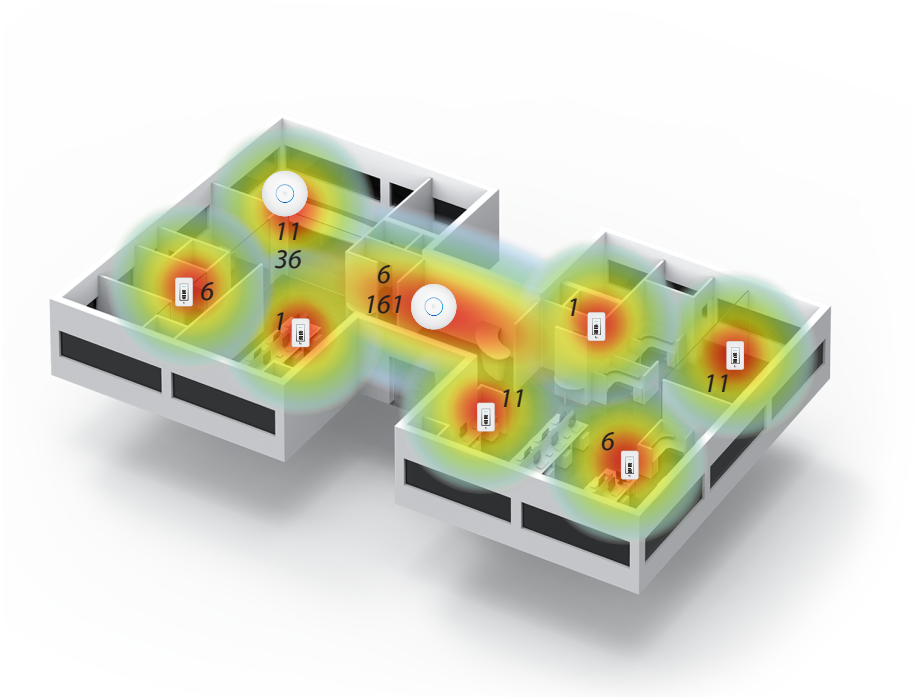
Airtime Fairness

Fortunately, UniFi APs feature proprietary enhancements to give HT clients favored airtime over legacy clients to balance airtime efficiency and increase data rates for the overall network. This also applies in situations where lower rate or poorly performing clients would normally consume unequal amounts of airtime. The enhancement also allows 802.11g legacy stations to perform better in mixed networks when 802.11b clients are absent.

Another way to ensure the highest possible performance and still allow legacy devices on the network is to segregate HT and legacy users. In some enterprise networks, a viable option is to manually steer clients to a particular UAP/WLAN. Wireless admins can help clients choose the right WLAN by identifying the frequency band in the SSID. As an example, HT clients would join the 5G WLAN while any legacy clients would join the 2G WLAN.

Airtime Fairness minimizes the effect of slower and/or problematic clients on aggregate WLAN performance by allocating equal airtime access to all clients. Under the UniFi Airtime Fairness algorithm, 2nd Gen. UAPs monitor channel utilization to determine the % of time the channel is busy with same WLAN traffic vs. competing same/adjacent channel WLAN traffic. The remaining % of time is available for UAPs to equally allocate time slots to stations based on the remaining available airtime.

Density



Density characterizes the number of users across the entire WLAN environment. High-density deployments like sporting events or concerts are marked by a high volume of users in a small area. Low-density deployments seen in rural areas or residences typically encounter much lower amounts of users across the same area. Compared to low-density deployment, which may consist of just a few sparsely placed UAPs, high-density scenarios require more planning and attention. With more users in a denser area, the wireless network faces more potential problems that can deter high performance.

However, the foremost problem faced by a high-density WLAN is in-band interference. As the WLAN scales to larger sizes, the potential for interference increases with increased wireless activity in a dense area. In a high-density scenario, two or more UAPs may be placed in close proximity to support a large amount of users. Often as the WLAN scales to larger sizes, in-band interference increases unnecessarily as a result of poor planning on the part of the wireless administrator. In-band interference stems from a number sources:

Causes of In-Band Interference in High-Density, Co-Located WLAN Settings

Cause	Description	Recommendations
Poor channel assignments	Two or more stations on neighboring channels are likely to interfere since they compete for the same channel causing higher noise floor and reduced performance.	• Follow a channel re-use plan (e.g., 20 MHz channels on 1, 6, 11 with 2.4 GHz) • UAPs on same channel (e.g., 36 and 36) should never overlap with strong signals reaching center of neighbor cell. • Use UAP+ for their highly selective radio filters.
Inappropriate distance between wireless cells	Closely-spaced cells can increase the overall noise floor when channel re-use patterns aren't used since both networks compete in the same proximity for use of same channels.	• Place UAPs on adjacent channels with appropriate distance to avoid self-interference. • Adjust cell size or create specific coverage area (e.g., external antennas, barriers).
Increased client loads	Stations like UAPs transmit and can cause interference for other stations/APs within the vicinity.	• Enable load-balancing. • Keep associated stations close to center of cell through minimum RSSI threshold. • Use dual-band UAPs whenever possible.

To account for all of these problems, be sure to plan and estimate the expected signals, noise floor, coverage area, capacity load and density of the wireless LAN. Once the first phase of planning is finished, administrators can begin to deploy UAPs and measure the signals, noise, coverage, capacity and density.

IV. Deployment

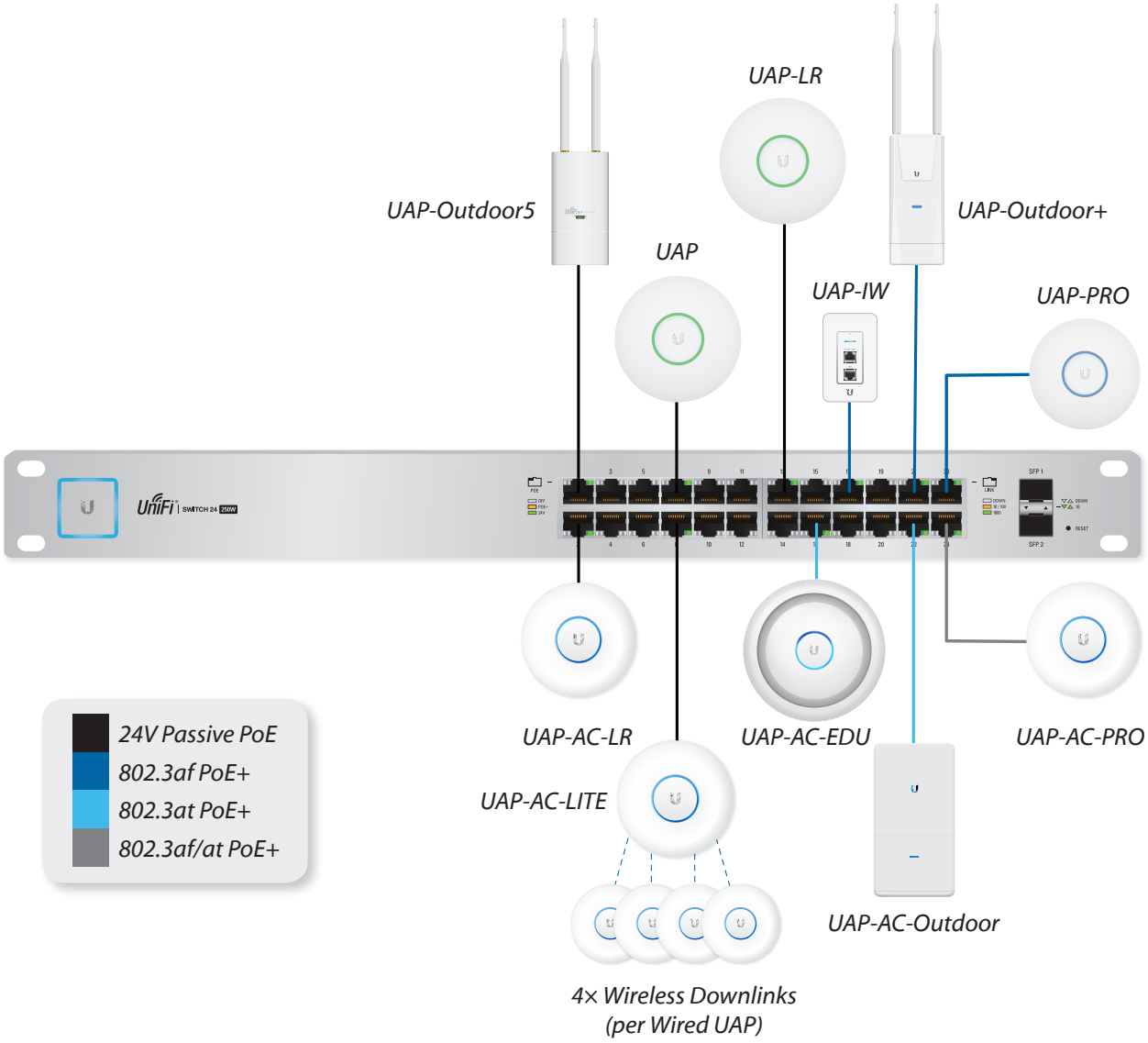
Site surveys, that is, detailed inspections of the deployment site, are pivotal in deploying the wireless network. The results of a site survey help determine some of the most important decisions in deployment, such as frequency selection, mounting location and channel assignments. During and after equipment installation, administrators should make software and hardware adjustments based on the results of benchmarks and real-world tests until the desired WLAN performance is achieved. The physical construction of the WLAN environment greatly affects deployment since what is 'possible' in one location may not be in a different setting. In general, wireless admins should consider the following details when deploying access points:

- Pre-install site surveys (blueprints/maps? mounting locations? construction materials?)
- Spectrum analysis (noise sources? dead zones? co-channel interference?)
- Attenuation (desks/people/trees/signs/doors/walls/windows? path loss?)
- Channel assignments (2.4/5 GHz? 1/6/11? 36/44? 36/40/44? 20/40/80 MHz?)
- Mounting UAPs (ceiling/wall/post/seats? obstacles/open?)
- Wiring (switches/PoE injectors? CAT5e/CAT6? UTP/STP? ferrite beads?)
- Post-install site surveys (SNR? overlap? co-channel interference?)
- Benchmarking (range/latency/jitter/speeds? roaming? applications work?)

Site Surveys

Before, during and after deployment, wireless admins should perform site surveys of the WLAN area. Surveying an area requires one visit to the premises to identify possible mounting locations for UAPs as well as barriers in building design or construction materials that could attenuate signals. Obtain copies of building floor plans to make note of objects not appearing on the blueprints (e.g., humans, computers) and consult them when designing the WLAN architecture. Later, upload these maps into the UniFi Controller to measure UAP coverage areas.

Power-over-Ethernet (POE) & Wiring



Despite its name, "wireless" networks still rely on cables and wires to connect access points to switches and routers. It's imperative that Ethernet connections function properly in full duplex and at advertised data rates (100/1000 Mbps), otherwise bottlenecks will occur. These problems can occur when line and EMI interference is present. Whenever possible, use outdoor-rated, shielded-twisted pair (STP) Ethernet cables like EdgeSwitch to protect against harsh weather and RF environments.

Ethernet cables are also responsible for supplying power to the wireless access points through Power over Ethernet (PoE). UAPs, IP cameras and other PoE-ready equipment are called powered devices (PDs) since they receive power from power sourcing equipment (PSEs) like EdgeSwitch. All UAPs come with a voltage-specific PoE (Power over Ethernet) adapter, however admins can consolidate power outlets by using a single UniFi Switch to power as many as 24 separate UAPs. Make sure that proper voltage is specified on each port since a misconfiguration could damage hardware.

802.3af and 802.3at define two of today's PoE standards. Some UAP models including PRO and AC are compliant with these standards since they require more power (48V) to support advanced features like dual radios and 3x3 MIMO. Other UAPs use passive PoE due to their lower power consumption (24V) but can be paired with adapters to use CAT5e or later Ethernet cables; operators can run cable up to 100m+ distance to provide PoE at the end of the UAP. However, this distance is subject to decrease in situations where more power is needed (e.g., 48V, Gigabit Ethernet).

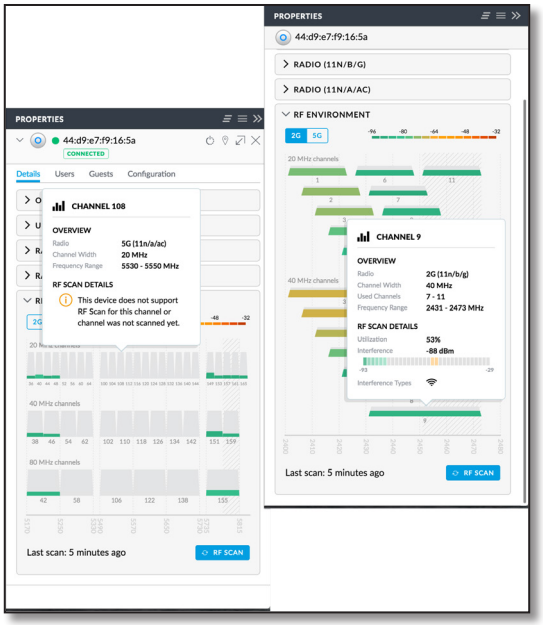
Select UAP models feature a secondary Ethernet port for bridging network connections without the use of a switch. This is particularly useful when an extra wired connection is needed to connect another network node. While the secondary Ethernet port itself does not provide PoE passthrough, it does act as a simple bridge port and can extend the reach of the wired LAN in a wireless uplink scenario

Device Forecasting

Besides estimating the minimum number of access points based on total number of clients and their bandwidth requirements, forecasting the number of required network devices can take on several pieces of evidences. For example, the sum of the used Wattage for each POE device in the proposed network can help estimate the minimum number of UniFi Switches needed to supply POE throughout the LAN.

As a network consultant, you are often required to submit equipment costs and estimates to governments and other organizations in order to win project bids. The Ubiquiti UniFi Network Planner tool gathers admin information about the planned site to generate a Bill of Materials, which you can use to secure project bids.

Spectrum Analysis

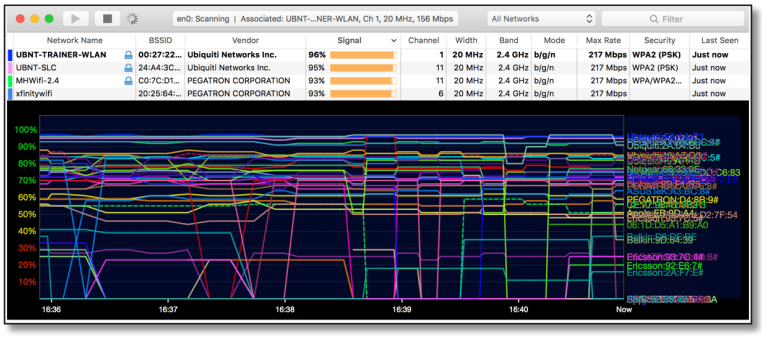


Site planning also requires wireless administrators visit the site to measure the noise and receive signal levels. Wireless devices transmit signals that are invisible to the human eye, so spectrum analyzers are used to read energy levels across the spectrum. If any noise sources exist in the WLAN environment, installers must know prior to deployment. Spectrum analysis data helps administrators choose wireless channels for deployment, as well as anticipate the client signals, SNR, and data rates throughout the WLAN.

Commonly, urban and densely populated areas face wireless saturation, that is, overcrowded channels. This is especially true in the 2.4 GHz band. In such cases, smaller channel widths (20 MHz especially) are important as they ensure the best possible SNR. After deploying UAPs, perform signal and speed tests throughout the WLAN using real-world client devices.

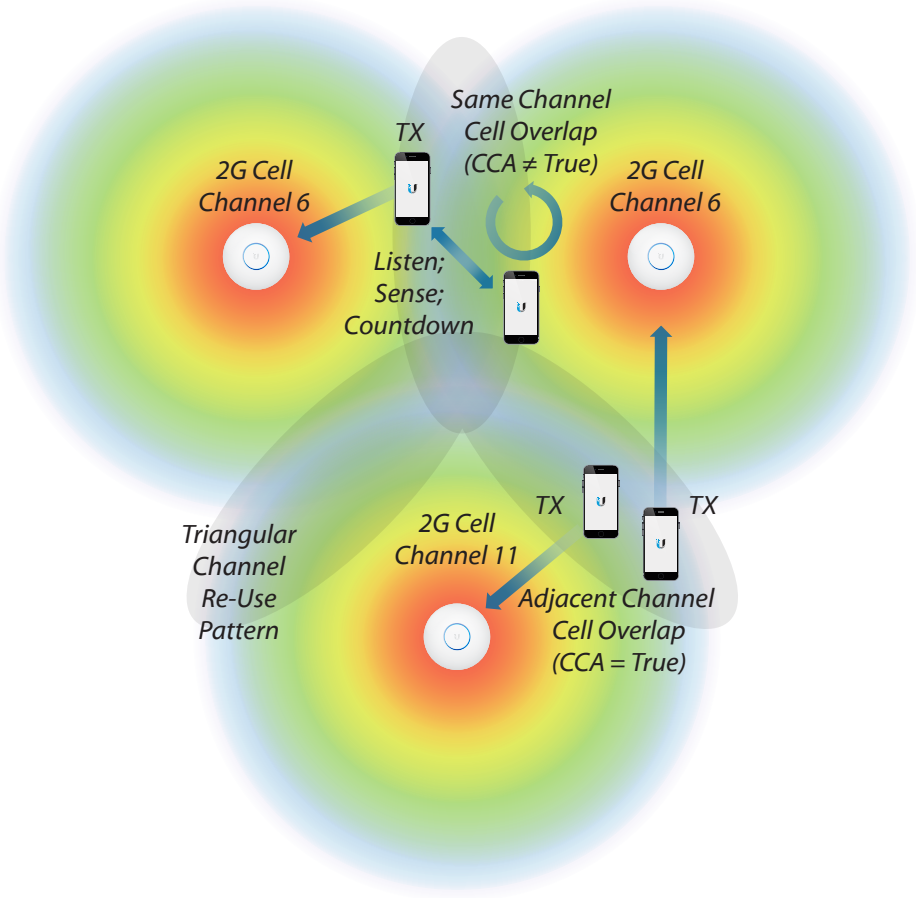
Second Generation UAP-AC devices allow administrators to scan the RF environment using a built-in spectrum analyzer tool. During the RF Scan, UniFi 2G/5G radios stop transmitting (i.e., stop broadcasting WLANs) to "listen" to the RF environment. All wireless clients using the UAP are disconnected, until after approximately five minutes, when the Controller presents the reported data from the UAP under scan.

Client WLAN Scanning



On client devices, use software like inSSIDer to measure the receive signal levels and noise floor based on nearby networks. At the very least, client spectrum analysis software should identify RSSI, channel, SSID and MAC addresses, to differentiate between neighbor APs and competing wireless networks. Where client signals are weaker than expected, consider introducing a new UAP on an adjacent or non-adjacent channel to decrease the probability of co-channel interference. This will help keep SNR at high levels across the WLAN and ensure smooth performance as the WLAN scales larger. Recall also that smaller channel bandwidths can achieve better signals and greater wireless range due to greater power density.

Overlap

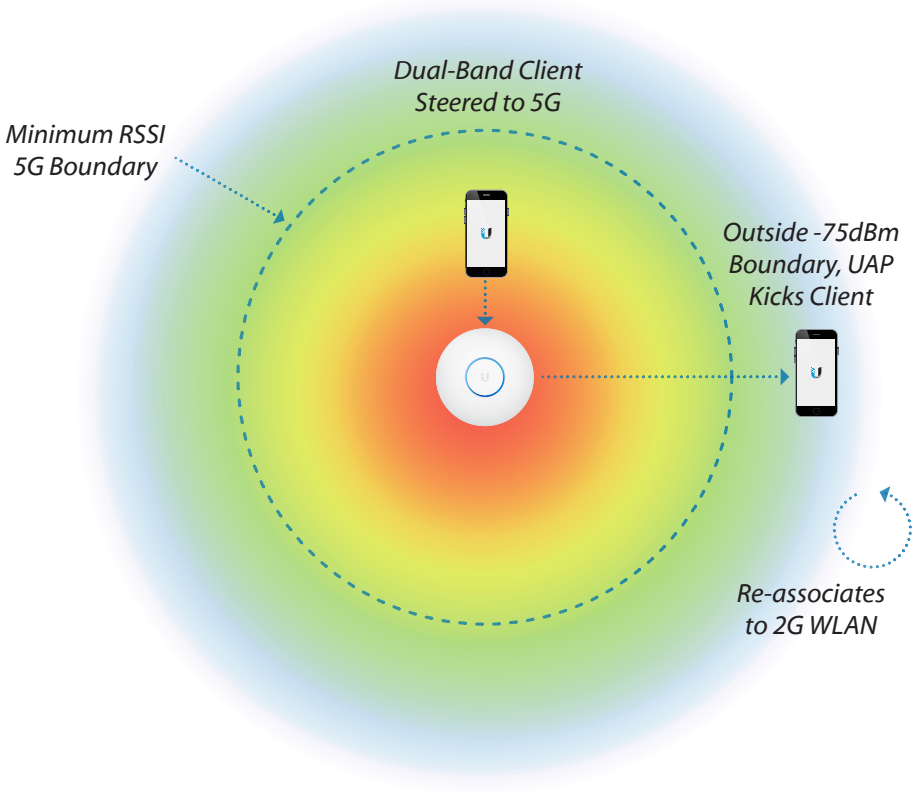


Make sure that UAP cells overlap enough for the application by always testing client applications and tweaking cell areas. If cells overlap too much, then co-located networks which compete for access to the same channel, may hear each other at similar levels to the clients. This would likely result in greater abundance of interference for both networks. If on the other hand, cells don't overlap enough, clients may experience poor performance or AP-assisted roaming could fail altogether. In the case of roaming, cells must overlap but since they use the same channel assignment, the potential for collisions and co-channel interference is increased.

Estimating overlap can be tricky and will ultimately depend on the application needs of the WLAN. It's generally a good idea to identify a minimum SNR or receive signal desired among clients across the entire wireless network (e.g., 24 dB, -70 dBm). Then adjust neighboring AP cells that use the same channels so that their signals do not arrive at each other's cell edges beyond what is necessary. Although signals will propagate beyond this point, the signal arriving from a neighbor cell on the same channel shouldn't exceed this threshold. For example, if UAP A can be 'heard' at -85 dBm by UAP B's clients, who hear UAP B at -70 dBm, then the SNR is only 15 dB every time UAP A talks. In this way, administrators can plan for coverage across the entire network while making sure that unwanted signals from overlap never exceed those desired signals.

Minimum RSSI

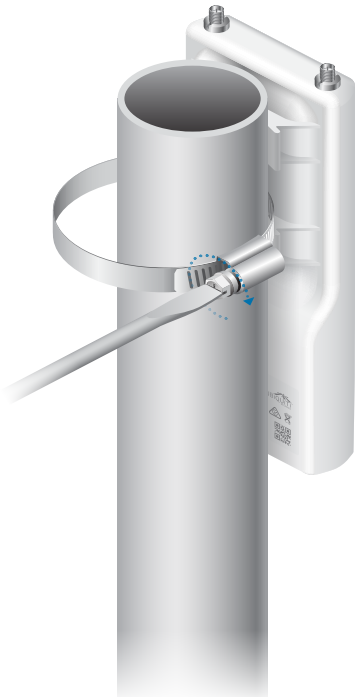
Minimum RSSI is an important part of managing an enterprise network. Its main purpose is to help client devices during roaming, ensuring that clients remain connected to the appropriate UAP. Often a single low-signal client can drag down the performance of the entire wireless network through wasted airtime, slow data rates and unstable activity. Currently, UniFi allows users to set minimum RSSI on individual UAPs by radio bands (2G and 5G). Minimum RSSI relies on de-authentication packet requests sent to the station (similar to the reconnect button found in the Controller UI). As a soft-kick technique, the final decision of whether to de-authenticate and look for another UAP is ultimately the decision of the Client device. From the perspective of the Client device, if only a single clear UAP is within 'good' range, it is possible that the station will connect, then reconnect over and over, causing frustration to the end-user. Therefore, configure Minimum RSSI with caution, and only in a properly-design WLAN.



Mounting UAPs

Mounting and orienting UAPs is a simple yet often overlooked part of managing wireless coverage areas. To create the most effective coverage area possible, wireless admins should always consult the antenna radiation diagrams of the access points being deployed. These diagrams provide detailed knowledge of antenna gain levels to maximize receive signal levels arriving at wireless stations.

UniFi APs come with mounting kits to be easily mounted on walls, ceilings or poles. Although mounting UAPs in visible locations is aesthetically pleasing, it also can serve to help users identify the UAP cell so they can move closer to improve their signal. In some scenarios, it may be necessary to place the UAP in a concealed location (e.g., underneath seats, on poles), like in large open space (e.g., concert hall) where walls/ceiling are distant from the center of the room.



AMO-5G10
AMO-5G13

RP-SMA Connectors for External Antennas

UniFi-Outdoor5
UniFi-Outdoor+

airMAX Antennas		
Omni	Sector	Titanium Sector
AMO-2G10	AM-2G15-120	AM-M-V5G-Ti
AMO-2G13	AM-2G16-90	AM-V2G-Ti
AMO-5G10	AM-5G16-120	AM-V5G-Ti
AMO-5G13	AM-5G17-90	
	AM-5G19-120	
	AM-5G20-90	

Regardless of how and where the UAP is mounted, wireless administrators must be conscious of how signals propagate and undergo loss. As seen with distance and free space path loss, higher frequency signals attenuate more when passing through obstacles. Compared to less dense materials like glass or wood, materials like metal attenuate signals greater. A great deal of data has been published that details specific attenuation levels for different materials of varying thickness. Be careful when placing UAPs in environments with many obstacles, especially metal surfaces, since reflections can create a degree of unpredictability for WLANs.

In large-scale deployments, several hundreds or thousands of UAPs may be adopted in a short period. It therefore becomes necessary to identify UAPs not only in the real-world (with markers or label makers) but in the Controller as well. The UniFi Controller features a handy locate tool for identifying each individual UAP as well as an Alias tag for specific, name-based identification within the Controller.

The UniFi Discovery Tool is a standalone software program that also allows admins to locate UniFi APs on the local network, without any need to log into a Controller at the site. Although the Discovery Tool will be studied in greater detail in Chapter 7, this software is useful in identifying the model/firmware and resetting the UAP to factory defaults (when the Device Username and Password are known).

Wireless Uplink is a proprietary technique for extending the range of the WLAN without the use of cables. Comparable to mesh and WDS repeater topologies, Wireless Uplink requires one UAP establish downlinks (up to four) to nearby UAPs. Although downlinked UAPs cannot themselves participate as uplink UAPs to another UAP, all UAPs (uplink and downlink alike) act as servicing access points to client stations. Wireless Uplink will be discussed later in the student manual.

Benchmarking

After the entire UniFi AP network is deployed, wireless admins should run benchmark software to measure the total data capacity of the network. Benchmarking measures the activity of wireless users and guests across each access point based on signals and test simulations. Try and anticipate real-world usage when benchmarking by using the same applications and devices that regular clients would use.

Among the numerous amounts of benchmarking software that exist, one common, widespread example known for its open source availability is iperf. As a cross-platform benchmarking tool, iperf is useful for testing UDP and TCP data streams from clients, APs and servers alike. UAPs already have iperf pre-installed and can host end-to-end tests. While it's okay to run benchmarks from end-to-end, running tests across individual links is the best way to find 'bottlenecks' in network communication. Consider the following parameters when running benchmarks:

- Client devices (tablets, smartphones, laptops? 1x1, 2x2, 3x3?)
- Applications (web browsing? video streaming? VoIP? UDP vs. TCP?)
- Position/location (range from UAP/neighbors? sitting/standing? obstacles in path?)
- Time (work/non-work hours? holidays? mass events? weekends?)

The main purpose for benchmarking is to model and test real-world applications through live simulations to estimate network performance. In a guest network where it's difficult to simulate before going live, it's absolutely crucial to perform tests and monitor the wireless network as soon as guests begin to associate to the access points. Pay particular attention to which UAPs receive the most wireless users to make quick hardware and software changes as needed. This may mean adding an extra UAP on a non-adjacent channel or enabling Load Balancing on select UAPs.

Regardless, the following benchmarks should be measured and analyzed:

Benchmark	Description	Indicator
Throughput	Measure of actual station's data capacity (e.g., to UAP)	• High throughput means good SNR and high airtime efficiency • Low throughput means poor SNR, low airtime efficiency and network saturation
Latency	Measure of time delay of packets (end-to-end)	• High latency is caused by poor SNR, high interference and network saturation • Low latency indicates good network performance
Jitter	Deviation in time delay of packets	• High jitter indicates interference and instable noise floor • Low jitter indicates good SNR and stable noise floor

Benchmarking gives WLAN operators an expectation of the overall performance of the wireless network. Be sure to run multiple tests to measure the signals, speed, latency and other network characteristics during and after deployment. This also includes running application-specific tests like video streaming or voice calls across the entire WLAN. While results should be close to estimates made during planning, actual throughput and performance may differ in the real world. After evaluating results, make specific decisions to improve the existing WLAN until desired capacity, density and coverage is achieved.

Characteristic	Ways to Improve
• Poor Signals • High Noise/Low SNR • Low Speed/Throughput • High Latency/Jitter • Poor Coverage • Poor Density	• Use more directive antennas • Deploy extra UAPs • Introduce or remove barriers in environment • Create traffic shaping rules • Enable Load-Balancing • Upgrade AP/client hardware • Alter channel bandwidths • Adjust radio settings

V. Basic Adoption and Setup

The UniFi Controller server software installs on any OS, network-capable server machine, whether virtualized, cloud-based, or local (ex. UC-CK, your laptop). In the UniFi directory, you can override the default ports specified in the "system.properties" file. UniFi hosts an Apache web server on default port 8443, so if you have L3 connectivity to your Controller, you can access the UniFi software anywhere from your web browser.

The UniFi Controller is designed to assist network administrators rapidly configure and deploy UniFi hardware. Multi-site controls, fast adoption schemes, and customizable WLAN Groups allow admins to configure hundreds, even thousands of UAPs across multiple networks.

UniFi stores site information, including statistics on user traffic and adopted devices in a database called 'MongoDB.'

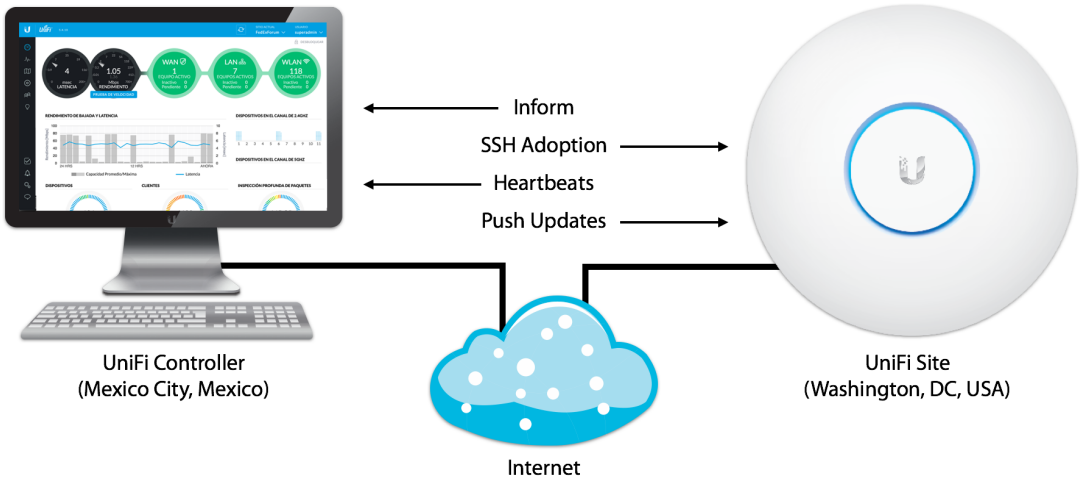
Multi-Site

Site A *Single Controller* *Site B*

With UniFi, a single Controller can be used to manage multiple deployment areas. Following first-time installation, the Controller creates a single, default site on which all new UAPs are automatically adopted. Creating a new site preserves existing sites and launches a completely separate interface in the UniFi Controller. One or more maps can be uploaded to visualize different floor space and deployment areas within each site.

For Advanced Adoption scenarios (Layer-3 or already managed UAPs), the site on which UAPs will be managed must be specified. Otherwise, UniFi Devices will appear under the default site to be managed. Later, UniFi Devices can be moved to another site from the *Configuration* tab, under *Forget this AP*.

Device Discovery & Adoption



Adoption is the binding between the UniFi Controller and UniFi Device. Once adopted, admins manage and push updates to hardware via software changes, called Provisioning. Before Adoption can proceed, a UniFi Device must be first Discovered in the UniFi Controller. Discovery occurs as UniFi Devices send out beacon messages to find and announce to the UniFi Controller to which it will be adopted. Inside these beacon messages, the UniFi Device includes routine status updates, as well as a network IP address to which the Controller can reach the UniFi Device.

By default, UniFi Devices in their Factory Default State announce their presence on the local network via Layer-2 Broadcast messages. In this way, local Device Discovery and Adoption is simply 'plug & play'. As long as there is end-to-end connectivity between the UniFi Device and Controller, admins can also adopt and manage devices anywhere in the world. Through a number of different "Layer-3 Adoption" techniques, admins can update 'en-masse' any number of UniFi Devices' "Inform URL", that is, the IP, hostname, or FQDN of the UniFi Controller.

Once discoverable to the UniFi Controller, the Status of the UniFi Device is listed, whether "Managed by Other [Controller]," or "Unmanaged" (Factory Default State). Following adoption, UniFi Devices periodically 'call home' to the Controller in short, 'heartbeat intervals.' This is a simple two-way process where the UniFi Device informs the Controller of current network location and the Controller provisions the UAP if any new configuration changes have been made. Communication between the UAP and the Controller uses a scalable, proprietary based protocol. All management traffic between the UniFi Device and the Controller goes untagged and encrypted.

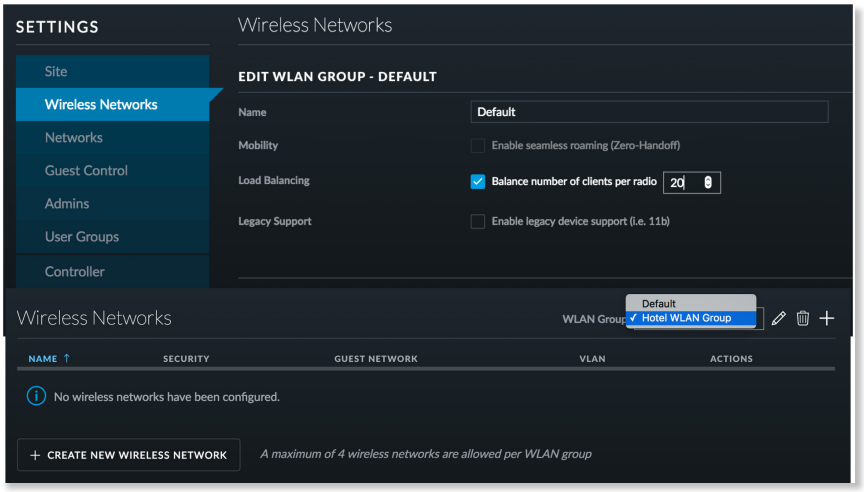
If a UniFi Device cannot reach the Controller to inform it during a scheduled heartbeat interval, the Controller will report that a heartbeat was missed. If more heartbeat intervals are missed, eventually, the Controller will report that the UniFi Device is "Disconnected." By default, UniFi APs will appear as isolated whenever they cannot reach their gateway but are in close proximity to other nearby, connected UAPs (who can hear their wireless beacons).

The Statuses for UniFi devices are listed in the "Appendices" of your Student Manual.

WLAN Groups

UniFi features fast, convenient methods for adopting many UAPs across multiple sites. By configuring WLAN Groups specific to the site and UAP clusters, access points will automatically provision with the correct WLAN information following adoption. Each WLAN Group supports up to four different WLANs. However, using UniFi overrides, the UniFi Controller supports an unlimited number of different WLAN configurations. Each WLAN can be configured with unique parameters, including:

- SSID
- Security & Encryption
- VLAN Controls
- User Bandwidth Groups
- Radio Load-Balancing (Chapter 3)
- Legacy Support (Chapter 3)
- Guest Policies (Chapter 8)



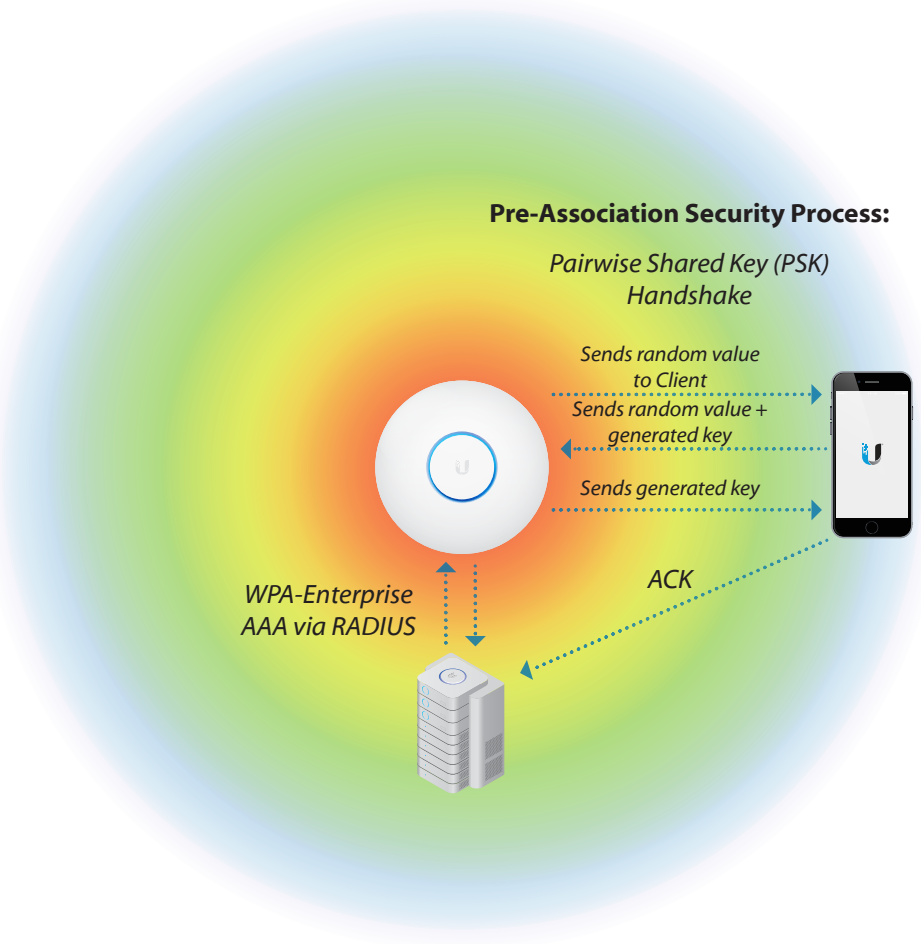
Service Set Identifiers

Service Set Identifiers (SSIDs) are the unique names given to WLANs that are broadcast by wireless access points. The BSSID (Basic Service Set Identifier) represents the MAC address of a particular access point. The ESSID (Extended Service Set Identifier) represents an SSID being broadcast by multiple APs. Multiple SSIDs being broadcast by a single AP are commonly called 'Virtual APs.' In addition to broadcasting the SSID of the WLAN, wireless access points also announce supported rates, encryption details and other relevant information in beacon frames that can be 'heard' by nearby stations. When Hidden SSIDs are enabled, connecting users must stipulate the name of the wireless network they wish to join. Although UniFi allows for up to four WLANs to be advertised simultaneously, administrators can override the WLAN group assignment for an endless number of supported SSIDs.

Security

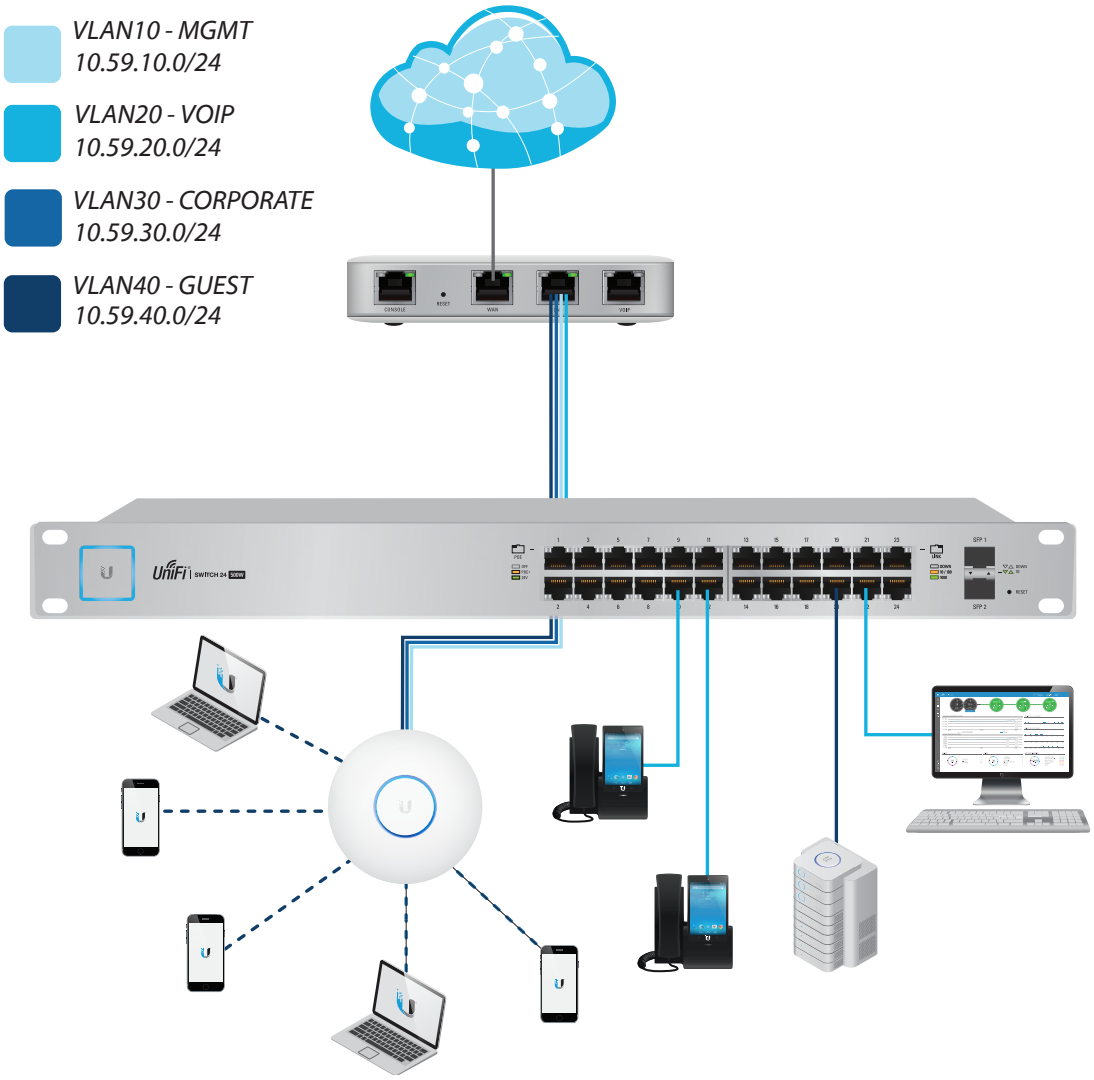
UniFi supports a broad range of security for a variety of different applications. Open security is useful on guest networks since stations can connect without prior, shared knowledge needed to authenticate. To control these open-access networks, be sure to enable UniFi's Guest Portal for restricted subnets, landing pages, walled gardens and voucher-based authentication. WEP is a very weak security protocol used in early 802.11 legacy networks and should be avoided unless absolutely necessary, like when legacy clients don't support later security protocols. However, WPA-Personal (also known as pre-shared key or PSK) is a simple, yet powerful security method that relies on a shared, preset password known to connecting wireless clients.

Perhaps the most secure and manageable security method for UniFi wireless enterprise networks is WPA-Enterprise. Also known as 802.1X or the extensible authentication protocol (EAP), WPA-Enterprise requires a RADIUS server in order to authenticate individual WLAN clients. A number of different RADIUS servers can be paired seamlessly with UniFi APs for standard-based authentication, authorization and accounting (AAA). At the RADIUS server, specify the location from which RADIUS requests may originate, like the IP addresses or subnet range belonging to the UniFi APs and clients. If necessary, set up wireless clients and specify certificates, like if EAP-TLS (Transport Layer Security) is configured. Because UAPs simply forward requests and are not actually responsible for performing the RADIUS authentication, UniFi can be paired with a number of different EAP types.



UniFi WLAN Groups allow administrators to choose between security types (e.g., WPA, WPA2) and encryption modes (e.g., AES, TKIP) to achieve the best possible performance while still servicing all 802.11 clients. The most advanced security method is WPA2, but may not be supported by older clients. When selecting WPA security, UniFi administrators can choose between AES- or TKIP-based encryption. AES encryption is 128-bit and occurs at the radio itself for the least possible overhead. AES should be used whenever possible over TKIP since it allows for the highest possible data rates. Keep in mind that unless WPA2-AES is used, WLANs face serious privacy issues since data can be intercepted and used maliciously.

Virtual LANs



Scalability and security are two important objectives when deploying an enterprise network. Through VLAN (virtual LAN) technology, networks can achieve both without great costs in time or resources. Fortunately, UniFi supports 802.1Q, an industry standard that supports VLAN information in packet (frame) headers.

Whenever new devices are added to the network, the broadcast domain increases. More traffic passing on the local network means higher chances that performance problems will occur. Traditionally, routers are used to break up broadcast domains. However, VLAN-aware switches and access points can also be used to break up broadcast domains. By principal, broadcast traffic from one VLAN will not reach another VLAN. In addition to providing better performance, VLANs also offer security benefits. Broadcast traffic from two WLAN clients connected to the same UAP will not reach each other, assuming they are assigned to two separate VLANs (e.g., VLAN100 and VLAN200). With 802.1Q, a VLAN-aware device such as a UniFi AP or Switch will 'tag' and 'untag' packets according to the Layer-2 network in which they remain.

In the UniFi Controller, admins can assign a VLAN to each WLAN much like a switch assigns VLANs by port. This means that connecting clients across different VLANs can both access the same Layer-2 AP but still pass traffic freely independent of one another. However, this does not change the fact they still compete for the same wireless medium since there is still just one collision domain per radio. VLAN assignments are made at the time of WLAN creation. Like with SSIDs however, admins can also override the VLAN setting for every WLAN.

In summary, wireless networks like UniFi are based on a 'listen first, then talk' design. Despite supporting multiple WLANs, a wireless access point like UniFi has a single collision domain for connecting stations. Wi-Fi products use half-duplex communication to compete for access to the wireless channel.

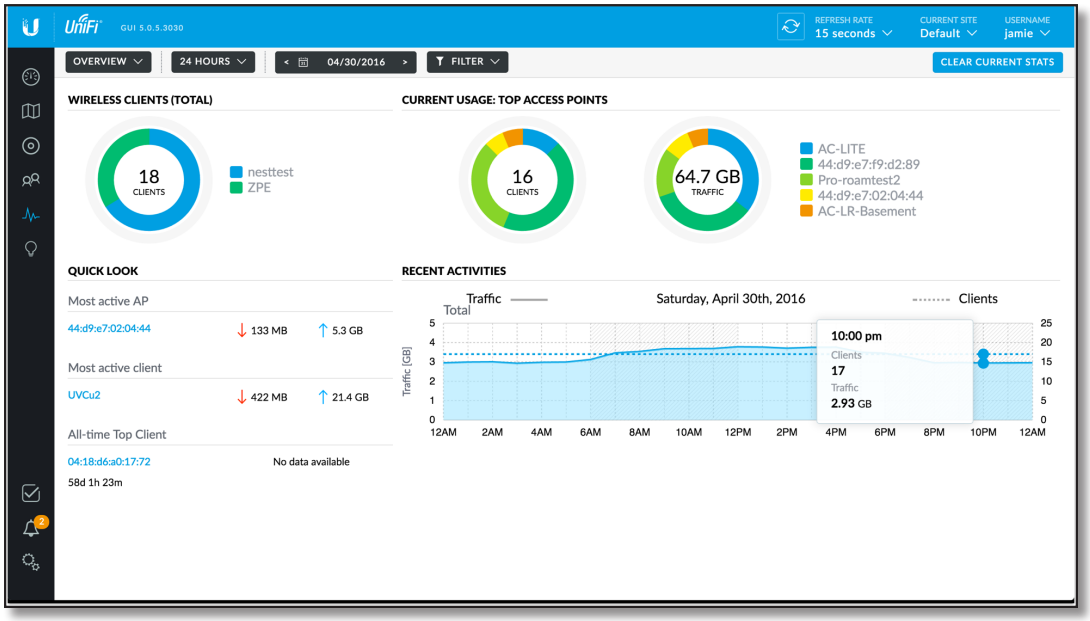
User Bandwidth Groups

User Groups are another important access control that UniFi allows administrators to set for both regular and guest WLANs. Creating User Groups is a fast, efficient way to assign maximum bandwidth controls to connecting users or guests. User Groups are applied to a WLAN at time of configuration so that any newly connected user will automatically be capped at the preset traffic limits for upload/download. Like with WLAN settings per UAP, User Groups can be overridden for each user/guest at the Controller.

VI. Analytics

The UniFi dashboard summarizes the most important statistics about traffic collected by UniFi devices and reported back to the UniFi controller. The Deep Packet Inspection engine is a free, powerful function that can be enabled for any UniFi site with a UniFi Security Gateway. To enable the DPI function, visit the Site settings page in your UniFi Controller.

Statistics



Enterprise networks often require that statistics be gathered to monitor traffic and establish controls on network activity. UniFi provides flexibility in monitoring wireless traffic and presents the data in an intuitive manner during user-defined intervals. The Controller makes setting user controls simple and straightforward. Among the data collected and displayed on the *Statistics* tab, UniFi tracks:

- Bandwidth of most active clients
- Bandwidth of most active UAPs
- Top all-time client bandwidth
- Aggregate bandwidth across UAPs
- Number of clients across UAPs
- Chronology of bandwidth activity
- Chronology of client total

Note: The Controller must be running for in-controller statistics to be gathered. If the Controller is not running, UAPs can still report data via SNMP.

Furthermore, the *Devices, Users,* and *Clients* tabs give a breakdown of activity, configurations and performance for all UAPs and WLAN clients across the UniFi managed network. Also from the *Devices* tab, admins can quickly view and visit any of the UniFi Devices discoverable to the Controller, including Devices currently managed by other, existing Controllers.

On the *Clients* tab, wireless clients can be blocked, forced to 'reconnect' or, when viewing individual Client/Guests Properties, forced to join a specific WLAN. Clients can be sorted by *Users* and *Guests* tabs which show relevant information about uptime, signal and bandwidth activity for connected guests on the UniFi network. However, the *Guests* tab allows admins to block, authorize or un-authorize guests on the WLAN.

The *Insight* tab provides unique information to help administrators keep the wireless LAN functioning smoothly. The first Insight shows data history for all Known Wireless Clients, past and present. Here, both online and offline Users/Guests can be blocked or unblocked at will. The second Insight displays Neighboring Access Points, which are simply access points not being managed by the UniFi Controller and in range of managed UAPs. The third and fourth Insights track Past Connections and Past Guest Authorizations. All of this information is important in monitoring user access and helps ensure a secure network.

Besides WLAN statistics, the UniFi Controller provides other useful information about the Enterprise network & UniFi devices under the *Insight* tab, including:

- Port Forward Stats
- Dynamic DNS
- Remote User VPN
- AC-EDU Streams

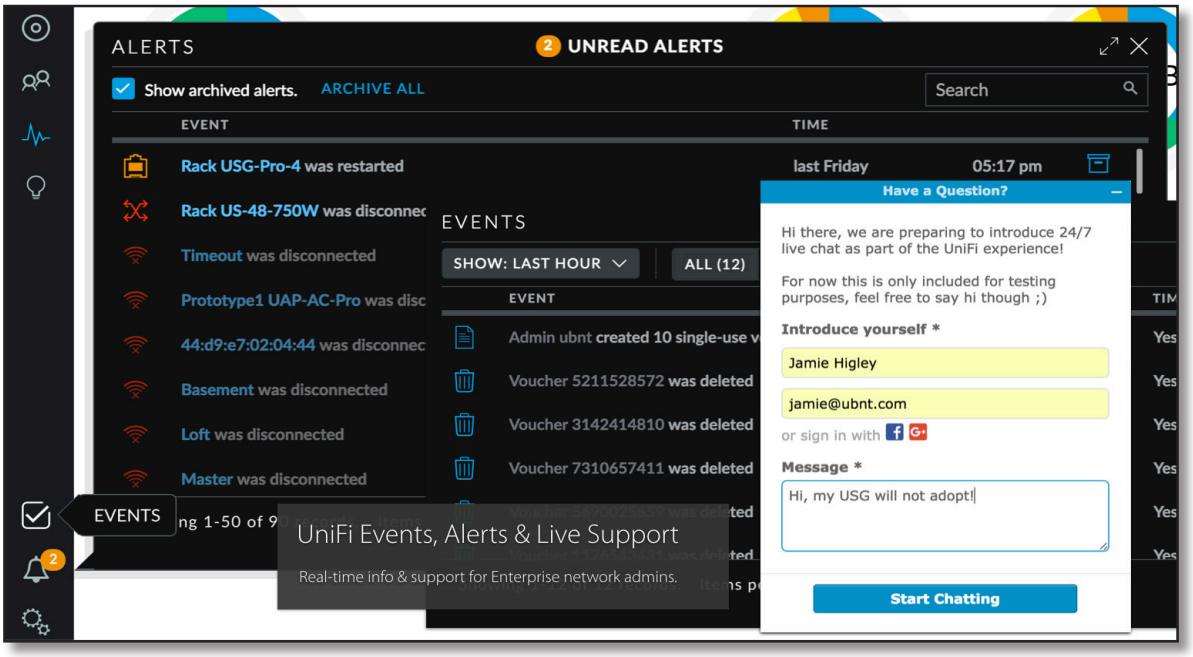
Events, Alerts & Support

At the bottom of the Controller, the *Alerts* tab displays important events as they occur in real-time. Whenever UAPs become disconnected or appear as pending adoption, the *Alerts* tab flashes red to call the attention of the UniFi administrator. Events can also be searched or archived accordingly.

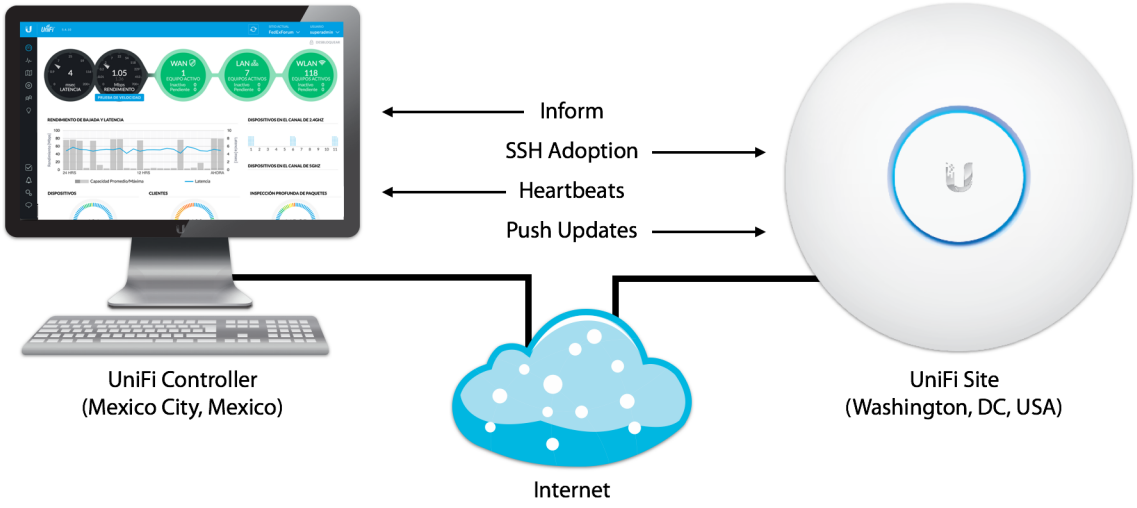
The UniFi Controller can also be configured to send automated alerts via Simple Mail Transfer Protocol (SMTP). Under the *Settings* tab, under Controller settings, admins can specify the mail server address, port as well as username and password used to authenticate the mail server. Optionally, users can enable use of Secure Sockets Layer (SSL) communication for added security encryption, although the port will automatically change from its default TCP 25 to 465. Verify that the SMTP server is working by sending a test e-mail to a target e-mail address.

When collecting server logs, UniFi can automatically back up logs to a remote syslog server, as specified at the *Settings* tab, under Site page. The server.log file can be found under <unifi_base>/logs directory.

Ubiquiti Networks has a dedicated support team that works 24 hours a day, 7 days a week to serve the end user at no extra cost. At any time, UniFi users can speak with the UniFi support staff, via Live Chat (in-Controller), or via e-mail (support@ubnt.com) for assistance with product setup, installation and recommendations for best practices.



VII. Advanced Management



Layer-3 Adoption

UniFi was specifically designed for scenarios where the Controller may be located away from the deployment site. In such cases, a variety of Layer-3 Adoption techniques can be used to remotely manage UniFi APs from virtually anywhere in the world provided there is connectivity between remote networks. The basic premise to Layer-3 Adoption is that UAPs located in different subnets can inform the UniFi Controller of their network location and pending adoption state. Admins should ping to test end-to-end connectivity between remote UAPs and the UniFi Controller, then ensure that Ports are open for UniFi Device & Controller communication.

L3 Adoption via UniFi Discovery Tool

Ubiquiti's proprietary software Discovery Utility makes UniFi AP adoption quick and easy. By default, UAPs will populate the Discovery Utility list when placed on the same Layer-2 network, since broadcast traffic initiates discovery. Inside the Discovery Utility, useful information related to each UAP is displayed including MAC address, IP address, model, version and status.

Wireless admins also have the choice of locating, managing or resetting the UAP through the UniFi Discovery Tool. Under *Manage*, unadopted UAPs can be prepared for Layer-3 adoption by setting the inform URL to the UniFi Controller IP on its inform port (default is 8080). Don't forget to include forward-slash, inform, after the IP address and port. Moments later at the UniFi Controller, the UAP will appear under pending devices, ready to be adopted.

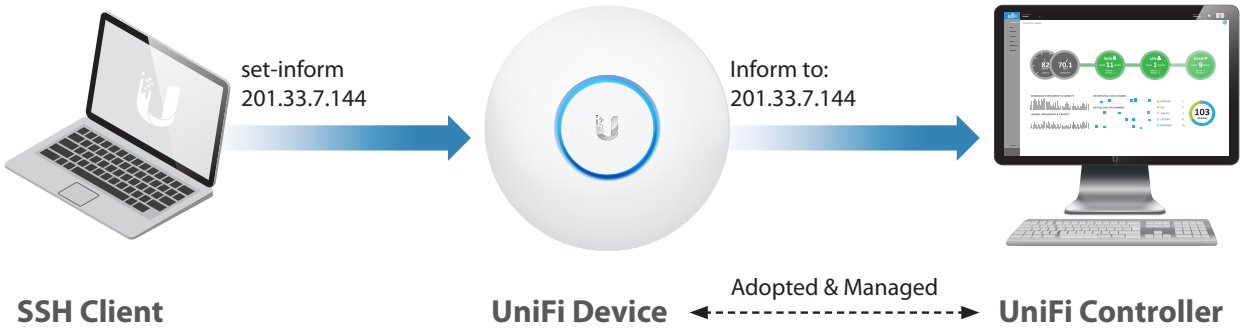
L3 Adoption via Secure Shell

Secure Shell (SSH) is used to establish remote client connections to SSH hosts over a secure, encrypted protocol. Using SSH, the wireless admin can point the UAP to the logical inform address of the UniFi Controller, after which the UAP will appear as pending in the Controller. In order to begin an SSH session, the device username and password for the UAP should be known. After opening an SSH session, admins can begin using the UniFi CLI to run specific commands for adoption, debugging, etc.

On Mac/Linux, network admins can open terminal to begin an SSH session by typing **ssh ubnt@192.168.1.20**. On Windows, users can download a free terminal emulator like PuTTY to begin an SSH session. In either case, you must know the device username and password before connecting over SSH to a UniFi Device. Once connected, the following commands offer insight into managing your UniFi hardware:

- help – Shows a list of UniFi-specific commands from the CLI.
- info – Displays information about the UniFi AP.
- set-default – Resets the UAP back to default factory settings
- set-inform http://<ip-of-controller>:8080/inform – Prepares the UAP for Layer-3 adoption.

```
Jamies-Macbook-Pro-2:~ QTiP$ ssh ubnt@10.1.0.7
ubnt@10.1.0.7's password:

BusyBox v1.19.4 (2016-05-29 23:56:59 PDT) built-in shell (ash)
Enter 'help' for a list of built-in commands.

BZ.v3.7.5# set-inform://ip.of.unifi.controller:8080/inform

Adoption request sent to 'http://ip.of.unifi.controller:8080/inform'.

1. please adopt it on the controller
2. issue the set-inform command again
3. <inform_url> will be saved after device is successfully managed

BZ.v3.7.5#
```



Secure Shell Connection

SSH is a secure protocol whereby a host connects to another host running an SSH server- all data is encrypted. Open an SSH Session via an SSH client (terminal, PuTTy/WinSCP)

ssh<username>@<ip_of_ssh_server>.

After issuing 'Set Inform' command to L3 controller inform address, the device will appear as pending. Proceed to 'Adopt' then re-issue inform URL.

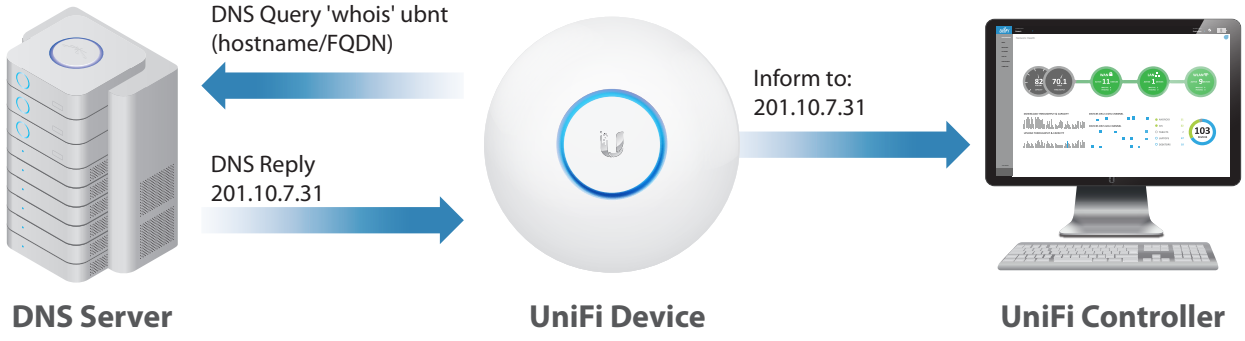
L3 Adoption via DNS

Domain Name System (DNS) is a broadly used naming system for computers and servers across the World Wide Web. DNS servers are distributed throughout the world and act like Internet phonebooks to resolve easy-to-remember domain names (www.ubnt.com) to logical IP addresses (23.21.93.68). Although DNS servers are prominently used across the World Wide Web, they are often deployed on private enterprise networks for purposes of redirecting web traffic, like in the case of UniFi Device Layer-3 Adoption.

In order for UniFi Devices to reach the UniFi Controller using DNS and DHCP on a private network, the network administrator needs to resolve unifi to the Controller's IP address on the DNS server. Make sure that the domain is reachable by pinging from the local network of the remote UAP to the Controller. For example, if the inform URL of the Controller is http:// XYZ:8080/inform, try pinging the domain XYZ.

Note to Student: When configuring the UAP to use a static IP address in the Controller UI, make sure that the IP of the configured DNS server is specified since the UAP still needs to resolve the Controller domain name.

```
##Set up distribution packages BIND

##configure /etc/dnsmasq.conf

## /etc/hosts
127.0.0.1                 localhost
201.10.7.31             unifi      ### UniFi Controller IP ###
```



Domain Name Service

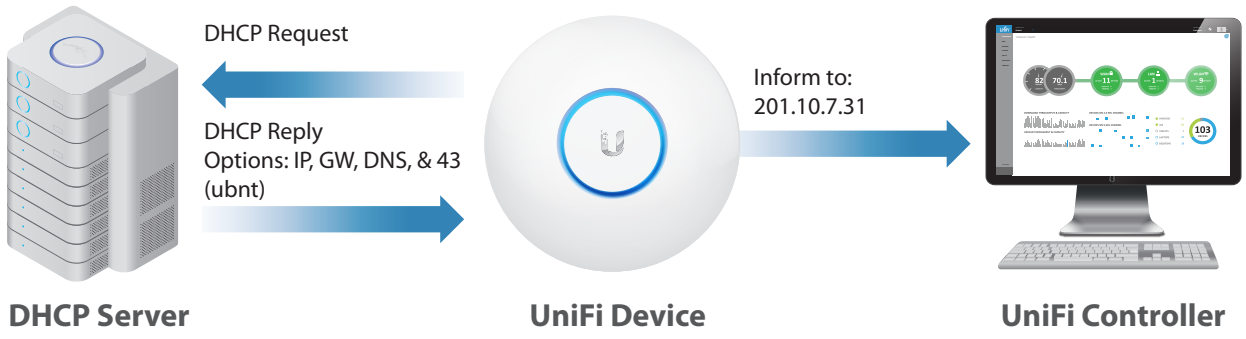
Using Linux DNS methods, (server files **dnsmasq.conf** & **/etc/hosts)**, point UniFi devices to the UniFi Controller. Simply assign an IP address to the hostname 'unifi,' referenced in the default inform URL: http://unifi:8080/inform

L3 Adoption via DHCP Option 43

Dynamic Host Configuration Protocol (DHCP) uses the client-server model for assigning IP information in IPv4 and IPv6 networks including network address, DNS servers and gateway. DHCP servers are typically configured to lease a range of IP addresses to host devices upon request, but can be configured with a variety of parameters (such as MAC reservation/filtering) to help accordingly. Furthermore, an Option 43 parameter can be inserted in lease information from DHCP servers to match the Controller IP address.

The following illustration shows a Linux DHCP Server configured with Option 43.

```
# ...
option space ubnt;
option ubnt.unifi-address code 1 = ip-address;

class "ubnt" {
      match if substring (option vendor-class-identifier, 0,
      option vendor-class-identifier "ubnt";
      vendor-option-space ubnt;
}
subnet 10.10.10.0 netmask 255.255.255.0 {
      range 10.10.10.100 10.10.10.160;
      option ubnt.unifi-address 201.10.7.31; ### Unifi Controller IP ###
      option routers 10.10.10.2;
      option broadcast-address 10.10.10.255;
      option domain-name-servers 168.95.1.1, 8.8.8.8; #
}
```



Dynamic Host Configuration Protocol

Using Linux DHCP server methods, (server files **dhcpd.conf**), point UniFi devices to the UniFi Controller. Assign an IP address to the vendor class identifier 'ubnt', which is simply another option contained in the DHCP lease requested by certain managed network devices.

UniFi Hybrid Cloud Controller Management

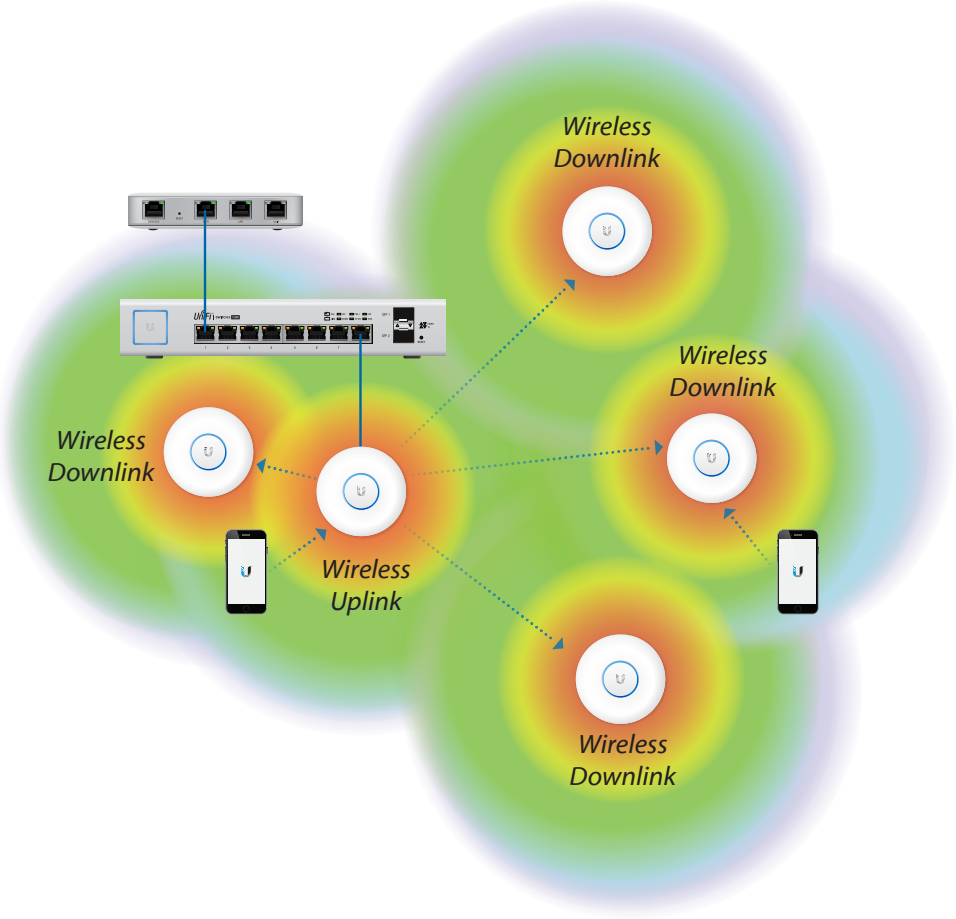
Since version 2 of the UniFi software, the Controller has supported Layer-3 device management & machine virtualization for remote, 'Cloud-based' server deployments, such as Amazon Web Services. However, the lightweight, low-cost UniFi Cloud-Key (UC-CK) provides an excellent alternative for localized device management, reducing overhead, bandwidth and points of failure for enterprise networks. To support an array of many physical sites with unique Cloud-Key (and PC-based) UniFi Controller deployments, Ubiquiti provides a free Cloud platform for central management of each UniFi Controller.

The Cloud platform relies on WebRTC protocol to establish end-to-end connectivity across firewalls/NAT, for web applications and their clients. This includes popular P2P software like Google Hangouts & Skype. Admins accessing the UniFi Cloud Portal can access any online, Internet-ready Ubiquiti Controller despite a dynamic WAN IP address.

Wireless Uplink

Wireless Uplink is Ubiquiti's proprietary method for extending UniFi networks without the use of cables. Compared to wireless distribution system (WDS) repeaters, ad-hoc networks and wireless mesh methods offered by other vendors, Wireless Uplink is a simple, secure and reliable technology used to extend the network without the use of wires. Once a UAP is adopted, it can serve as either an uplink or downlink UAP. Wired UAPs can perform wireless downlinks to as many as four island UAPs simultaneously. Both uplink and downlink UAPs can service WLAN clients, although downlink UAPs cannot themselves perform downlinks to other island UAPs. As seen in other repeater-type topologies, each wireless downlink introduces a 50% reduction in available throughput.

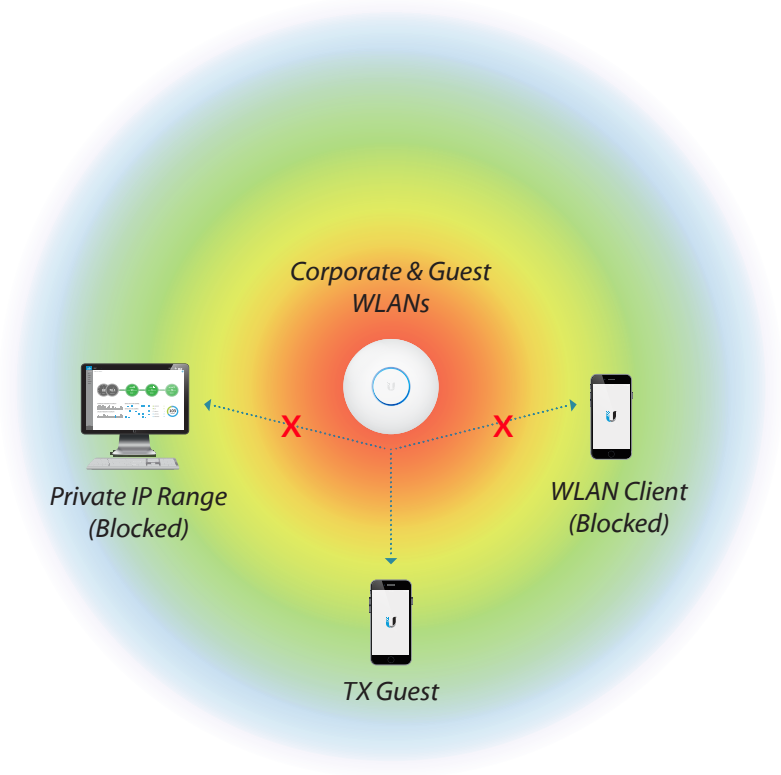
To initiate a wireless link, disconnect the intended island UAP. Once disconnected, the UAP will no longer be able to heartbeat into the Controller. Soon after, the Controller will report that the UAP has missed its heartbeat interval. Some time later, the UAP will appear as Disconnected in the Controller. Anytime a Disconnected UAP is unable to reach the gateway, an Isolated state is triggered. While in the Isolated state, the island UAP will search for nearby UAPs to perform a wireless uplink. After encountering a potential uplink UAP, the Controller will update the Disconnected UAP to an Isolated status and the wireless admin can perform a wireless downlink from the wired UAP to the island UAP.


Wireless
Downlink
Wireless
Downlink
Wireless
Downlink
Wireless
Uplink
Wireless
Downlink

VIII. Guest Networks, Portal & Hotspot

Even without making use of the Portal and Hotspot features, UniFi allows admins to create Guest Networks that differ slightly from Standard Networks in terms of User Policies and Access Controls. The function of the Guest Portal is to enable an authentication/ authorization mechanism, after the guest device has already associated to the Guest WLAN.

Guest Policies and Access Controls



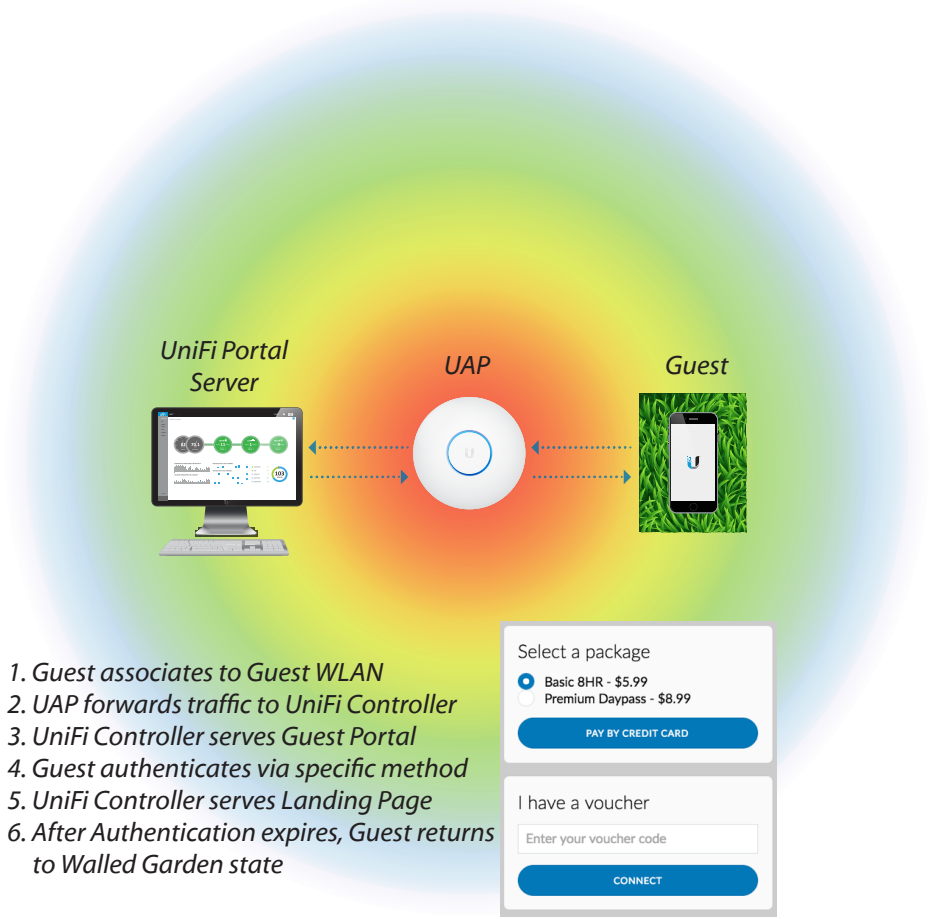
Wireless Networks that have the “Guest Policy” enabled are immediately subject to the following settings:

- L2/L3 Traffic Isolation - by default, guest stations are unable to send traffic to other guests, such as L2 broadcasts for discovery.
- Access Controls - by default, guests cannot send traffic to hosts in the private network ranges RFC1918—only to the gateway for purposes of communicating on the Internet. These private network ranges can be overridden in case a desired pool of hosts should be reached by the guests.
- User Groups - by default, guest users have traffic shaping settings applied for bandwidth limits. User Groups are applied to a Guest WLAN at time of configuration so that any newly joined guest will automatically be capped at the preset traffic limits for upload/download. Inside the Controller, User Groups can be overridden for each user/guest at the Controller.

Guest Portal

When enabled, UniFi's Guest Portal acts as a complete system for authenticating new guests to the WLAN. Compared to regular users that associate and authenticate on non-guest networks, guest users connecting through the Guest Portal are placed in a Walled Garden or limbo state until they are authorized by the UniFi system. While in this Walled Garden, guests receive an IP address and perform DNS lookup, but all other traffic is blocked. HTTP/HTTPS traffic is automatically redirected to the Controller running the portal.

Note to Student: Once authorized, guests have access limited to the Restricted/Allowed Subnets as specified on the *Guest Portal* settings page.

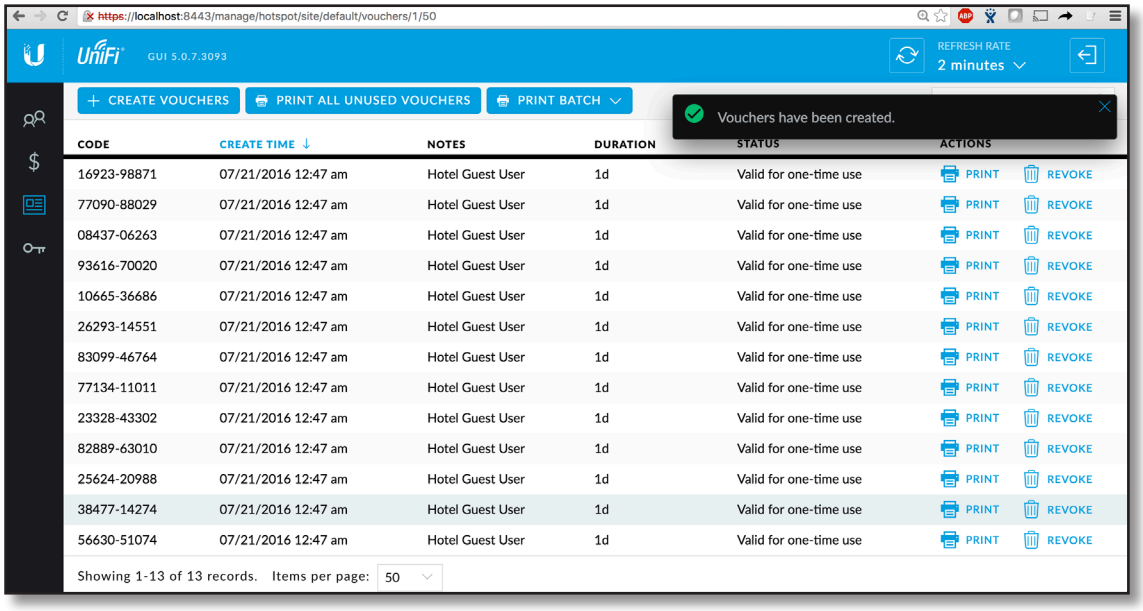


Authorization is dependent on the authentication methods and other parameters configured under the Guest Portal for a particular site. Each authentication method is uniquely prepared to handle a specific scenario:

- **Open**: Without authentication, users can be forwarded to a promotional URL (Free Internet brought to you by. . . or simply Accept Terms of Use) or be redirected to the original URL, for discrete guest services. Most common in completely free-to-use scenarios.

- **Simple Password**: While in the Walled Garden state, guests are redirected to a Landing Page where they must enter a simple password, defined by the administrator at the Controller. While similar to PSK-based authentication on normal WLANs, guests enter this password at the Landing Page.
- **Hotspot**: UniFi's built-in Hotspot function allows wireless operators to customize portal login pages and bill customers using major credit cards or other supported methods. With voucher-based authentication, the Hotspot Manager can create and manage vouchers for authorized use. UniFi also supports a variety of payment sites including PayPal, Stripe, QuickPay and many more.
- **External Portal Server**: The UniFi AP system can also be integrated with existing businesses/individuals' web servers. When External Portal Server is selected, UniFi applies Guest Policies to connecting guests while authentication is redirected to the specified server. From a port perspective, HTTP 80 and HTTPS 443 are forwarded. An API is also provided to better integrate the External Portal with the Controller to perform actions like authorize guest [00:15:34:93:e3:f2] for 4 hours.

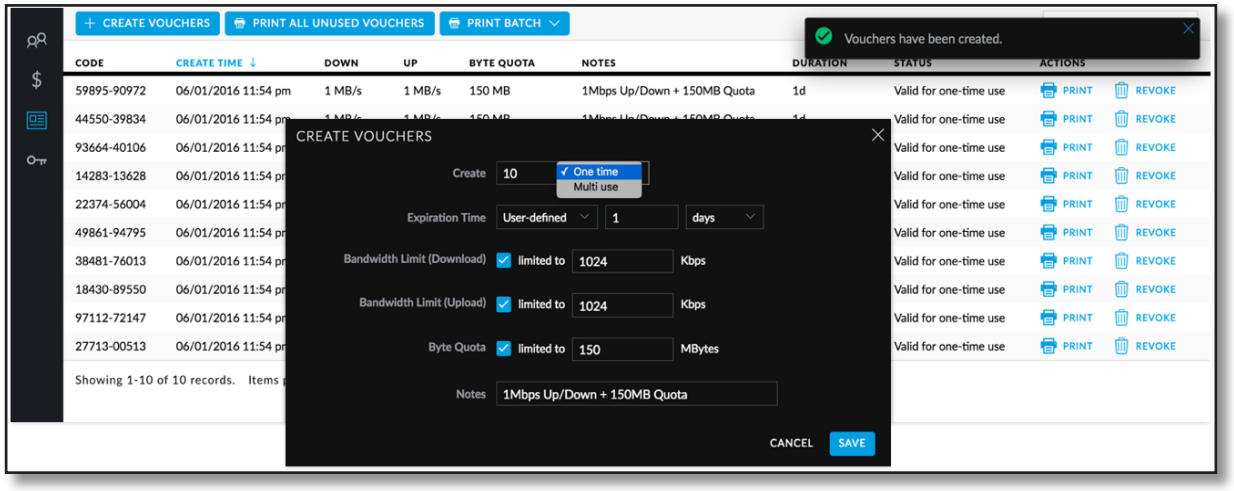
Hotspot Manager & Vouchers



Unlike other wireless network management systems, UniFi comes bundled with an intuitive Hotspot Manager for authorization and monitoring of guest users at no extra charge to the operator. Built-in hotspot authentication methods for guests include voucher distribution and online payment gateways. Before leaving the Walled Garden, guests must authenticate using a selected authentication method and accept the Terms of Use.

The Hotspot Manager can be found on the default address https://<IP_of_controller_ PC>:8443/hotspot/s/<site_name>. In this way, each site can be configured with unique Hotspot Operator accounts to separate management among employees within every organization. Hotspot Operator accounts are suitable for employees that do not need administrative access for configuring the UAPs themselves.

Hotspot Operators have permission to create, revoke and print vouchers. Furthermore, Hotspot Operators can perform special actions on the wireless guests in cases where access needs to be blocked, extended or if the guest wants to be refunded payment.



Payment Integration

Using UniFi, businesses and individuals can integrate PayPal and other online payment software with their hotspot portal. Such payment software will vary in price and features. PayPal Standard accounts are free of charge, but do not support APIs, so an external web server is required to leverage the PayPal Instant Payment Notification service. However, using PayPal Pro accounts, operators can quickly incorporate APIs to set up the PayPal service in the UniFi Controller. This service requires a small monthly charge.

In the case of PayPal Pro users simply prepare the PayPal account, update the Controller with PayPal settings and customize the portal files with wireless packages before guests can begin choosing packages offered by the Hotspot. Compared to Pro accounts, PayPal Standard requires an extra step for setting up the external portal server, since APIs are not supported. The authentication method therefore would be the External Portal Server. Once a user is validated, the Package, Payment Amount and Authorization Method will appear on the Payments/Transactions page.

Portal Customization

With Portal Customization, the UniFi Controller software allows complete branding of a portal implementation, allowing admins to white label the wireless Internet service as if it were developed completely by the business. In order to provide the greatest degree of flexibility in branding the company/individual, the UniFi Controller software provides total access to the portal directory on the system in which it is installed. This open architecture allows administrators to include unlimited content while keeping development simple through the use of plain .html (hand code or use any text editor).

After enabling Portal Customization under the Guest Portal settings, the Controller creates a file structure that can be easily accessed and navigated, found at /<unifi_base>/data/sites/<site_name>/portal.

Among the files contained in the portal directory, the most important ones are outlined below:

- index.html – Main landing page that displays pricing, authentication information and Terms of Use to the guest.
- payment.html – Used to submit credit card information. It requires HTTPS and also serves as an example of an additional .html page.
- fail.html – Displayed when there is an error handling a guest login.
- reset-min.css – Standardizes the rendering of HTML elements across browsers.
- styles.css – Controls the style of HTML elements.

Located in the bundle folder are the following files:

- bundle/messages.properties – This file defines package costs, duration of access, package titles, and how the charge will appear on a customer's credit card account. Error messages are also defined by this file and can be edited in most text editors.
- bundle/vouchers.css – Standardizes the rendering of HTML elements across browsers.
- vouchers.html – The default appearance of vouchers belonging to a site.

Testing is simple and immediate; simply save code on the Controller PC, reload the guest browser and see changes reflected on Guest Portal pages. All HTML pages are rendered and can be the target of a form's POST action. None of the supporting files are required (e.g., styles, css), although using the files provided by Ubiquiti, network administrators have complete control to customize the Guest Portal experience for the end-user. Moreover, multiple hotspot packages can be configured for different payment types, names, duration of use, bandwidth limits, etc.

III. High-Density WLAN Design Guide

Overview

What is High-Density Wireless?

By definition, High-Density (HD) wireless scenarios refer to WLANs whose coverage area contains a relatively high concentration of APs and connected client devices. As mobile networking trends toward scenarios where users carry multiple client devices, HD WLANs become increasingly more commonplace. Therefore, WLAN administrators tasked with designing a successful HD network can do so using Ubiquiti's UniFi platform, provided they carefully consider and account for all of the unique design variables surrounding the enterprise project.

UniFi Demo Simulator - FedEx Forum Site

Throughout the HD WLAN Design Guide, we'll reference the "FedEx Forum" Site, inside the UniFi Demo Simulator. The "FedEx Forum" Site mimics a real-world HD deployment that supports more than 7,000 simultaneous Wi-Fi users today.

Why HD WLANs Generally Fail?

Ubiquiti identifies three major areas that impact the performance of every HD WLAN deployment:

Most Impactful Aspects of High Density Deployments		
Problem Area	**Description**	**Solution**
Broadcast/Multicast Domain Control	Uncontrolled network traffic jeopardizes airtime, resulting in decreased speed, increased latency, and potential connectivity problems.	Besides assigning VLANs to WLANs, configure Port Isolation at the switch layer to limit unnecessary traffic and conserve precious airtime available to stations in the HD WLAN.
WLAN Planning & Design	Inadequate and improper planning/design physically inhibits wireless performance and cripples user activity on the network.	Carefully anticipate and plan for network capacity parallel to the user requirements for the HD WLAN prior to methodically designing the coverage area with proper channel reuse patterns.
Site Survey, Analysis, & System Characterization	Lackadaisical attention of the RF environment results in careless placement and inept configuration of APs for poor wireless performance.	Before, during, and after deployment, consciously track, measure, and evaluate signals, noise, traffic, and other metrics to optimize the HD WLAN accordingly.

Four Part HD WLAN Design Guide

This four-part guide presents and explains, from start-to-finish, the implementation of an HD WLAN using the Ubiquiti UniFi platform:

Part 1 - Planning

Part 2 - Design

Part 3 - Deployment

Part 4 - Config

Part 1a - Planning - Application Requirements

The Purpose of the HD WLAN

Regardless of user density, the purpose of every WLAN is to support the wireless users' application requirements. Therefore, the very first step when planning for the WLAN is to understand the user applications and behavior. Typical projects involving HD WLANs include stadiums, auditoriums, concerts, and other events where a high volume of users gather across the coverage area. The most common applications for these HD scenarios range from social media to live video/VoIP streams to simple web browsing. Consequently, use of these applications may see varied levels of activity due to the nature of the event, such as with spontaneous traffic bursts (e.g., everyone posts to social media during breaks) or as more constant streams of data (e.g., students taking notes in a lecture hall).

Core Applications Define Planning & Design

Recognizing the core applications and types of users on the network, begin to plan and design the HD WLAN with regards for the unique limitations and requirements of the planned project. For example, the performance of latency-sensitive applications like VoIP can degrade as WLAN usage reaches peak levels. Why? Because the wireless channel is shared among all nearby, active stations; an 802.11 station (i.e., the VoIP user) must 'wait' to transmit until the channel is free of activity. Fundamentally speaking, the principal applications and services on the network dictate the architecture and design of the WLAN—especially in HD scenarios.

Realistic WLAN Planning/Design

Can a WLAN simultaneously support latency-sensitive applications, as well as high bandwidth users? With total control over all of the variables affecting the WLAN, including client devices and the physical environment for deployment, the realization of both objectives in a single, culminating project becomes more realistic. When faced however with "bring your own device" (BYOD) scenarios, as HD WLANs often are, limited control over environmental variables often at time of planning forces the network to choose between supporting high throughput or low latency applications.

Part 1b - Planning - User Bandwidth

Client Traffic Analysis via UniFi DPI

Following deployment, enterprise network administrators can take advantage of the Deep-Packet Inspection (DPI) engine running on the UniFi Security Gateway (USG) to review the applications in use by client devices on the network. The UniFi Controller summarizes the total bandwidth consumed by the user applications, as well as the individual activity of users, so WLAN administrators can make firewall and other configuration changes to improve the performance of the network.

What is "Service Level Assurance"?

Prior to deployment however, anticipate which applications will be serviced by the HD WLAN to develop a plan for "Service Level Assurance" (SLA) ahead of estimating the "Per-Client Bandwidth". A clearly-defined SLA identifies the primary applications and services to be supported on the intended network (such as VoIP or YouTube), and therefore, guides the early stages of planning and designing the WLAN architecture. Keep in mind that although low-end VoIP and video calls require minimal bandwidth, their tolerance for latency is also much lower, and therefore are designed uniquely. Although UniFi APs give "Quality of Service" (QoS) priority to such traffic (per WMM standards), initial planning/design for the HD WLAN should cater to the specific needs of the applications.

Create an SLA for the HD WLAN

To help formulate the SLA for the users on our unique HD WLAN, let's reference the client device "current-e58ba353" as a baseline example. A quick analysis of the DPI section under the UniFi Client Properties tab reveals its top three applications to be:

1. Web Browsing
2. Social Media
3. Video Download

"Application Requirements" Data Table

The following "Application Requirements" table relates info about the speed and connection required to service some of the most popular applications used in today's WLANs.

Application Requirements				
Type	**Example**	**Bandwidth (Mbps)**	**Latency Tolerance**	**Packet Flux**
Email & Instant Messenger	Gmail, Messages	0.1	High	Bursty
VoIP	Skype Audio Call	0.1	Low	Constant
Podcast/Radio Download	Pandora, Spotify	0.2	Medium	Bursty
Social Media	Instagram, Facebook	0.25	High	Bursty
Video Call	Skype Video (Low)	0.3	Low	Constant
	Skype Video (High)	0.5	Low	
	Skype Video (HD)	1.5	Low	
Web Browsing	Wikipedia, Google Web Results	0.5	High	Bursty
	Reddit, Google Image Results	1		
Video Download	YouTube 240p	0.4	Medium	Bursty
	YouTube 360p	0.75		
	YouTube 480p	1		
	YouTube 720p	2.5		
	YouTube 1080p	4.5		
Online Gaming	League of Legends	2	Low	Constant
Internet TV	Netflix 720p	4	Low	Bursty
	Netflix 1080p	5		
File Sharing	Bittorrent	10	High	Bursty
File Backups	Dropbox	10	High	Bursty

SLA for Multitasking & Multiple Users Types

In some WLAN scenarios, the SLA may seek to support a variety of user types, or even multiple applications per client device (i.e., network multitasking, background services), and should therefore sum together the total Bandwidth required for each application.

"Application A Bandwidth + Application B Bandwidth + Application C Bandwidth + … "

"Per-Client Bandwidth"

For purposes of our HD WLAN example, our SLA assumes that the user (guest) is single-tasking, and therefore, seeks to support the most bandwidth intensive application used by client "current-e58ba353": Video Download (0.3-4.5Mbps, with 1Mbps assumed for mobile resolution playback). This means that the "Per-Client Bandwidth" (that is, the HD WLAN's SLA) is approximate 1Mbps.

"Maximum Aggregate Throughput Requirement"

To discover the "Maximum Aggregate Throughput Requirement," that is, the total amount of bandwidth needed for the HD WLAN to support ALL client devices simultaneously, multiply the "Per-Client Bandwidth Requirement" (1Mbps) by the "Total Number of Client Devices" (the "FedEx Forum" has a seating of 18,119). While not all 18,119 in attendance will bring one mobile device to the event, planning for future growth is an important consideration for every WLAN.

"Per-Client Bandwidth Requirement" x "Total Number of Client Devices"
= "Aggregate User Throughput Requirement"

(1Mbps) x 18,119 Clients
= 18,119Mbps Aggregate

"Expected Peak Aggregate Throughput"

Therefore, the "Maximum Aggregate Throughput" at the "FedEx Forum" is 18,119Mbps. However, since it is impractical to assume that all 18,119 will ever pass traffic simultaneously, let's multiply the "Expected Peak Usage" (let's estimate 50% of total attendance) by the "Maximum Aggregate Throughput Requirement" to determine the "Expected Aggregate Throughput".

"Maximum Aggregate Throughput Requirement" x "Expected Peak Usage"
="Expected Peak Aggregate Throughput"

(18,119Mbps) x (50%)
= 9059.5Mbps "Expected Peak Aggregate Throughput"

Later on, the "Expected Peak Aggregate Throughput" value will directly help to estimate the minimum number of Access Points required for the HD WLAN deployment.

Upstream Data Links

The ~9Gbps of data passed on the HD WLAN by the guest users is Internet traffic, and therefore, the upstream pipe to the ISP should support the "Expected Peak Aggregate Throughput" to account for the offered SLA at the event. Throughout the HD WLAN, make sure that upstream network infrastructure (e.g., switches) accommodates the traffic bandwidth downstream (i.e., aggregation switches at core, access switches at edge).

Part 1c - Planning - WLAN Capacity

What is Capacity?

In the context of all WLANs, capacity is defined as the data rates supported by an AP and its respective clients. Capacity is therefore, twofold dependent on the characteristics of both client devices and APs (hereafter called "stations"). By anticipating and analyzing the characteristics of stations, we can accurately calculate the capacity of the network in order to estimate the total number of access points required to support the planned HD WLAN.

Choose the Best AP Possible

Although "bring your own device" (BYOD) scenarios mean client devices cannot be consciously chosen, fortunately, WLAN administrators can select access points whose wireless characteristics offer the best performance to match their particular HD WLAN scenarios. This is also important to ensure that the HD WLAN has longevity through down-the-road support for the client devices of today and tomorrow.

Introducing the UAP-AC-HD

The UAP-AC-HD is Ubiquiti's premiere 4x4 MU-MIMO Access Point for HD WLAN deployments. The UAP-AC-HD features the latest, cutting-edge 802.11 technology for breakthrough speeds (2.5Gbps aggregate PHY rates) at a revolutionary price that undercuts all competitors. The unbeatable price/performance advantage entices WLAN administrators tasked with deploying HD-ready APs on a tight budget, since more APs (beneficial in HD WLAN) can be deployed for a fraction of the price. And as Wave-2 802.11ac client devices begin to flood the consumer market, the UAP-AC-HD's MU-MIMO technology especially targets HD WLANs, inasmuch as its synchronous, multi-client data streams push airtime efficiency to new levels in extremely dense coverage areas.

Introducing the UAP-AC-M

Alternatively, the UAP-AC-M unit supports versatile coverage options through external connectors for pairing with directional antennas. For example, by pairing the UAP-AC-M with a 45° airMAX sector antenna, WLAN administrators can produce small, controlled 5GHz cells—ideal in certain HD WLAN scenarios. By comparison, the omnidirectional antennas and mounting capabilities make the UAP-AC-HD well-suited for low-ceiling and wall deployments, while the UAP-AC-M (a Wave 1 "Single User" (SU) MIMO AP) is ideal for high-vaulted ceilings seen in auditoriums, stadiums, and concert halls.

WLAN Capacity Variables

To review, there are five variables that determine the supported data rates of a WLAN, including:

1. **802.11 Protocol** - the hardware standard characterizing the 802.11 stations on the WLAN (a, b, g, n, ac Wave 1, ac Wave 2). As a backward-compatible AP, the UAP-AC-HD immediately serves in HD deployments today, while anticipating growth as WLANs scale to support more client devices for years to come.

2. **Spatial Streams** - the total number of data streams simultaneously transmitted and received by the AP and clients. “Multiple In, Multiple Out” (MIMO) operation traditionally has been limited by the supported data streams of the single client with whom the AP communicates. As a Wave 2 802.11ac access point, the UAP-AC-HD boosts the available airtime through true “Multi-User” MIMO mode, concurrently pushing up to 8 streams of data to clusters of 2G & 5G clients. And since most client devices opt for less antennas (i.e., fewer spatial streams) to conserve battery life, the UAP-AC-HD’s MU-MIMO technology is critically important to ensuring maximum WLAN performance.
3. **Channel Width** - the bandwidth over which an AP and its clients transmit data signals (20/40/80 MHz). While 40/80 MHz channels are tempting, HD WLANs dictate use of 20 MHz channel widths to conserve the number of channels available for reuse during deployment (especially true in extreme HD scenarios). In contrast, larger channel widths in HD scenarios generally create a fundamentally flawed WLAN design where closely-placed AP cells operating on same or nearby channels see degraded SNR performance and increased contention for use of the wireless channel.
4. **Signal-to-Noise Ratio (SNR)** - the difference in receive signal (the desired data signal) and noise (the combined level of in-band interference). From the point-of-view of HD networks, SNR poses the greatest threat to performance since by nature, densely-packed WLANs face greater interference. In order to ensure strong SNR levels for clients, HD WLANs necessitate careful cell planning, including methodical channel assignments, very low, controlled transmit power levels, and precisely deployed AP locations.
5. **Guard Intervals (GI)** - 802.11n/ac WLANs support “long” and “short” waiting periods between transmitted symbols (data). Although a short GI is desirable, UniFi APs automatically toggle between “long” and “short” GI depending on the WLAN performance.

PHY Rates vs. Throughput

Now that we have identified the factors that determine capacity, it’s important to distinguish that these are physical-layer (PHY) data rates. What does this mean? Due to overhead in the 802.11 protocol, the actual amount of real TCP data payload sent over wireless signals is approximately half of the advertised PHY rates. When estimating the capacity of the HD WLAN, we’ll factor a 50% reduction of the calculated PHY rates to align with speed results experienced in the real-world.

Estimate Client Throughput

Returning to “current-e58ba353” as our baseline example, the reported 72.2Mbps PHY rate assumes that a ‘typical’ client device is characterized as:

An 802.11n client device,

With a single (1x1) data stream,

Operating on a 20MHz channel,

With the best SNR,

And short GI.

By halving the PHY rate (72.2Mbps), we estimate that for the planned HD WLAN, the "Achievable Real-World Client Throughput" is 36.1Mbps.

Estimate Minimum Required APs

By dividing the total "Aggregate User Throughput Requirement" (9059.5Mbps) by the "Achievable Real-World Client Throughput" (36.1Mbps), we calculate 251 radios (rounded up from 250.955679) as the minimum number of radios required to service the HD WLAN.

"Aggregate User Throughput Requirement" ÷ "Achievable Real-World Client Throughput"
= "Minimum Required Radios"

(9059.5Mbps) ÷ (36.1Mbps)
= 250.955679 Radios

In some scenarios, 2G and 5G bands can and should be used. Note however, that in many HD WLANs, such as stadiums and arenas, only 5G channels are deployed since propagation characteristics make 2G difficult to control.

Therefore, a "Minimum AP Estimate" of 251 APs could satisfy the capacity requirements for the "FedEx Forum" site, based on the following assumptions:

- Full person attendance at event is 18,119.
- "User-to-Client Device" ratio is 1:1.
- "Total Client Devices" at the event is 18,119.
- "Expected Peak Usage" is 50%.
- "Expected Peak Aggregate Throughput" is 9059.5Mbps.
- 'Typical' client device is 802.11n, 1x1, with strong SNR.
- WLAN operates on 20 MHz channels with short Guard Intervals.
- "Achievable Real-World Client Throughput" is 36.1Mbps.

Capacity Conclusions

The "Minimum AP Estimate" is a function of two capacity variables: "Aggregate User Throughput Requirement" and "Achievable Real-World Client Throughput". In simpler words, a client's speed and bandwidth requirements directly affect the capacity offered by an AP. Increased client speeds (e.g., more spatial streams, improved SNR) means fewer APs are required since each AP reaches greater capacity. Conversely, decreased client speeds means more APs are required. As bandwidth consumption on the network increases, more capacity is needed to support the user applications, thereby requiring more APs.

Theoretical vs. Actual APs Deployed

As a theoretical number, the "Minimum AP Estimate" gives network administrators a starting point as they undertake the important task of designing the HD WLAN. The actual number of APs deployed will depend on a broad range of physical factors noted during site visits, floorplan analysis, as well as site surveys conducted at the intended HD WLAN site.

Part 2a - Design - Channel Patterns & Cell Sizing

Capacity, Coverage & "Cells"

Recall that WLAN capacity is directly dependent on the SNR of stations across the wireless coverage area. The primary design objective of each HD WLAN is to limit the coverage area provided by each AP (hereafter called "cells"), then apply an effective channel reuse pattern to ensure a high SNR for every station. HD WLANs perform poorly when AP cells are overextended or if channel reuse patterns are not respected.

2G/5G Characteristics

Although the 2.4GHz band contains eleven 20MHz channels on which a WLAN can operate, only 3 may be used in a non-overlapping channel pattern: 1, 6, and 11. By contrast, the 5G band supports over 20 non-overlapping 20MHz channels, depending on the region. The availability of more channels gives the 5G band a distinct advantage in limiting the interference of neighbor cells through more flexible channel reuse patterns. And due to propagation characteristics, certain HD WLANs may only deploy on 5G channels in open settings like stadiums and arenas, where controlling the effective size of a 2G cell can be physically challenging.

Cell Characteristics

There are seven fundamental points to consider that can affect a cell's coverage area:

Factors Influencing Cell Size		
Factor	**Description**	**HD WLAN Recommendation**
Frequency	Due to "Free Space Path Loss", 2G signals propagate farther than 5G.	Deploy on 5G—use 2G with extreme discretion.
Channel Width	Increased channel width (e.g., 80MHz) means decreased range for signals.	From the standpoint of channel reuse patterns, only use 20 MHz channels.
Transmit Power	High transmit power increases an AP's coverage area.	Reduce transmit power to "Low" for small, controlled cells.
Antenna	Antenna gain influences the directivity and size.	Consider UAP-AC-M with directional antenna capability in areas with ceilings 25 feet or higher.
Obstacles	Obstacles attenuate signals at different rates and influence the propagation behavior of signals (e.g., reflect, absorb, scatter).	Consider the structural elements at the site when choosing how and where APs will be mounted since walls can help control cell size.
Clients	Like APs, client devices also transmit and generate signals.	Implement strict channel reuse patterns and limit overlap between neighbor cells.

DFS Channels

In the 5G band, Dynamic Frequency Selection (DFS) operation requires APs stop broadcasting if radar signatures are detected. As part of the site survey, WLAN administrators must scan these channels prior to deployment and for planning. Whenever possible, include DFS channels in the HD WLAN design for a more robust channel reuse pattern.

Floorplan Example

The following floorplan shows 118 UAP-AC-M deployed using a strict channel reuse pattern across the entire HD WLAN coverage area. The floorplan illustrates three fundamental characteristics of a properly designed HD WLAN:

Fundamental Characteristics of Proper HD WLAN Design		
Characteristics	**Reason**	**Diagram**
Small, controlled cell sizes	Each coverage area features a distinguishable channel for high SNR	(i.e., channel 1 inside daisy flower of 6 & 11 around perimeter...show client SNR from Channel 1 = SNR Strong, Channel 6/11 weak -80)
Neighbor cells (2G/5G) never use the same channel	Avoid channel contention by two competing stations	(i.e., station 1 & station 2 in overlapping AP cells, both on channel 6)
Neighbor cells (5G) assigned non-adjacent channels	Improve SNR inside cell	(i.e., channel 36 & 165 instead of 36 & 40)

Adjacent vs. Non-Adjacent Channels

Adjacent channels refer to WLAN channels whose bandwidth (channel width) edges touch. By contrast, non-adjacent channels are WLAN channels whose bandwidth edges are spaced with 20 MHz or more. For example, 5G channels 36 and 40 are adjacent channels; 36 and 44, non-adjacent channels. When deployed on neighbor and overlapping cells, non-adjacent channels see better performance, a principle that holds especially true in HD WLANs, where the combined total of competing, in-band signals is much higher. The adjacency of 2G channels 1, 6, and 11 causes SNR to degrade quickly, giving 5G the advantage in HD WLAN scenarios.

Part 2b - Design - Minimize Interference

Interference & HD WLANs

Interference represents the total amount of competing, in-band signals that prevent a station from 'hearing' the intended receive signal with clarity. The extreme proximity of so many client devices on adjacent and non-adjacent channels increases interference levels, and therefore, reduces SNR and performance across the HD WLAN service area. When properly designed, an HD WLAN ensures each connected client device has a strong SNR, while mitigating the potential for collisions and limiting the impact of in-band interference.

What is Co-Channel Interference?

Whenever WLAN administrators deploy two neighbor AP cells on the same channel, the overlapping coverage areas encounter Co-Channel Interference (CCI). With the resulting transmit collisions that occur as a result of CCI, stations must retransmit data, which results in decreased speeds, increased latency, and problems for client device connectivity. This is due to the Clear Channel Assessment (CCA) mechanism, which requires an 802.11 station to listen prior to transmission, and yield the channel in case a station is already transmitting on the wireless channel. An HD WLAN with poor channel design and uncontrolled coverage areas will suffer as CCI plagues the wireless network. Conversely, HD WLANs that deploy AP cells with strict channel reuse patterns and controlled coverage areas can avoid CCI in the wireless network.

What is Adjacent Channel Interference?

Although CCI is largely avoidable in a properly designed, well-controlled wireless network, Adjacent Channel Interference (ACI) presents a significantly greater challenge for HD WLANs, and is not easily countered. ACI describes the overall increase in interfering, in-band wireless signals faced by stations as multiple AP cells are placed in relatively close proximity. By overextending the coverage area in a dense wireless setting, ACI increases aggressively throughout the HD WLAN, thereby reducing SNR levels for client devices, and dropping speeds dramatically. More generally, ACI speaks to the type of interference generated along the 'tail-ends' of an 802.11 transmission, which raise noise levels for other nearby in-band stations. Because adjacent channels (i.e., 36 & 40) suffer greater interference levels than non-adjacent channels (i.e., 36 & 165), the channel design for HD WLANs should position AP cells on adjacent channels as distantly as possible.

Best Practices for HD WLAN

To review, an HD WLAN should follow a series of best design practices:

Fundamental Characteristics of Proper HD WLAN Design		
Characteristic	**Reason**	**Diagram**
Small, controlled cell sizes	Each coverage area features a distinguishable channel for high SNR	(i.e., channel 1 inside daisy flower of 6 & 11 around perimeter...show client SNR from Channel 1 = SNR Strong, Channel 6/11 weak -80)
Neighbor cells (2G/5G) never use the same channel	Avoid channel contention (CCI) by two competing stations	(i.e., station 1 & station 2 in overlapping AP cells, both on channel 6)
Neighbor cells (5G) assigned non-adjacent channels	Control ACI and maintain high SNR inside cell	(i.e., channel 36 & 165 instead of 36 & 40

Part 3a - Deployment - AP Placement

Omnidirectional Antennas

In general, most client devices as well as all UniFi Access Points feature antennas that are omnidirectional. Similar to a light-bulb, an omnidirectional antenna radiates wireless signals in all directions. More specifically however, the coverage area produced by an omnidirectional antenna looks similar to a donut pattern, with peak signal strength nearest to the center of the donut, and weaker signals at the edges of the 'cell'. Recognizing that not only UAPs but client devices radiate signals in all directions is crucially important to understanding signal interference. Therefore, all station types contribute variables that affect SNR across the HD WLAN coverage area.

Ceiling & Wall Mounted APs

Indoor UniFi Access Points like UAP-AC-HD and UAP-AC-PRO feature easy mount fixtures for quick installation into walls and ceiling tiles. The UAP-AC-HD provides excellent wireless coverage in extremely dense indoor with ceilings under 25 feet height. Although the antenna coverage pattern of each indoor UAP is similar, understand that reflective surfaces and multipath effects in crowded, more dense settings can result in unexpected signal readings from distant and/or nearby APs, therefore necessitating careful cell adjustments based on site survey analysis.

Directional Antennas

Alternatively, directional antennas can be paired with select UniFi Access Points like UAP-AC-M to produce distinct, controlled coverage areas, making them very popular in outdoor or open indoor settings. When mounting UAPs in open rooms with high ceilings (25 feet and higher), omnidirectional antennas are incapable of producing distinct coverage areas vital in the design of the HD WLANs. Instead, pair the UAP-AC-M with directional antennas pointed at specific areas of the HD WLAN event to produce controlled areas of coverage with robust SNR. Note that when using 5GHz directional antennas with the UAP-AC-M that the 2G radio should be disabled.

"Under Seat" APs

An increasing more popular AP placement trend in today's HD WLANs, such as seated sporting events, is mounting APs below users in attendance. By securely installing an AP in a locked boxes under seats or within the building foundations itself, this coverage technique seeks to improve the SNR of client devices by placing APs closer to the users themselves. The "under seat" technique however presents new challenges for the HD WLAN, including coverage overextension during low attendance events, since less users means fewer bodies attenuating (controlling) the size of each wireless cell.

Part 3b - Deployment - Site Surveys

Site Visit

While important during the planning phase, visiting the HD WLAN site before and after deployment is totally necessary in order to critically assess the area for design and installation guidelines, as well as to conduct crucial site surveys to gather RF information needed for channel assignment. Although the UniFi Controller supports RF scanning with second-generation UniFi Access Points, be sure to also bring sample client devices with spectrum analysis and WLAN scanning software, as well as cameras to document the key areas involved in deployment, such as installation areas, potentially problematic regions, and cable drops.

Map, Topology & Deployment

After visiting the intended deployment site and making adjustments to the final channel plan, WLAN administrators can begin to install UAPs. In addition to the high capacity requirements at HD wireless events, the same-channel requirement for two neighbor UAPs to perform a Wireless Uplink make this topology inappropriate for HD WLANs. Instead, connect each UAP via wired Ethernet cables back to UniFi Switches to support the bandwidth requirements at both the access and core layers of the network.

Site Walkthrough

After supplying POE to the UAPs and updating with the intended channel pattern, consider defining simple SSIDs to uniquely identify each UAP as you walk around the HD WLAN coverage area. With any site walkthrough, you should carry a sample client device (anticipated at time of HD WLAN Planning) to measure and track the most important metrics throughout and across the coverage area including signal strength, noise floor, and SNR. Since the purpose of the initial site walkthrough is to establish, define, and adjust the intended wireless coverage area, be sure to also bring a laptop make immediate configuration changes to the deployed UAPs as well.

Controller Tips for Site Surveys

As part of the Site Walkthroughs, consider using the WLAN Override function to temporarily rename the primary SSID broadcast by each AP to uniquely identify each individual cell to the client device performing the Site Survey. To tweak the HD WLAN coverage area between events, create a backup of the Site that contains the "one-SSID-per-AP-radio" naming convention.

Client Benchmarking

The UniFi Mobile App allows WLAN administrators to collect the most important metrics conducted during the Site Survey, including signal strength and noise levels. Following deployment, use the UniFi Speed Test as well as intended applications during live events to ensure that client devices support the SLA requirements for the HD WLAN.

UniFi RF Scanning

In order to make educated decisions regarding channel operation throughout the wireless network, WLAN administrators must study and analyze the RF environment within the HD WLAN. Before and after deployment, use the RF Scan tool to conduct a spectral analysis from the perspective of each UAP. During the RF Scan, the UAP radio will stop broadcasting WLANs for up to 5 minutes in order to 'listen' to the RF environment. Following the RF Scan, the UAP radio reports two important characteristics needed to level of interference as well as utilization percentage. Based on the results of each scan, record, replan, and reassign channels before reevaluating the RF environment of the HD WLAN. Be sure to run the RF Scan tool on all APs individually, but not simultaneously, otherwise the data presented by the spectral analysis will not accurately represent the RF environment in which the HD WLAN operates (furthermore, all clients will experience connectivity issues).

UniFi Statistics & Insights

The UniFi Controller gathers and reports the most important Client and WLAN information in real-time needed to make 'on-the-fly' changes to the wireless network under management. Here are a few of the most important in-Controller Statistics and Insights to review from the perspective of HD WLANs.

Resourceful UniFi Controller Statistics & Insights for HD WLAN		
UniFi Info	**Description**	**Recommendation**
Traffic Statistics	Relates the aggregate network bandwidth consumed on the network.	Ensure that the aggregate traffic statistics match WLAN capacity plans, otherwise add/remove UAPs as needed.
User Activity	Relates the level of activity and bandwidth consumed by individual users.	Enforce stricter traffic shaping policies to high-activity client devices to minimize their negative effect on the HD WLAN.
Deep-Packet Inspection	Relates information about the applications in use on the network.	Create traffic-shaping and/or firewall rules to limit or eliminate the negative effect of select apps on the HD WLAN.

Part 4 - Config - UniFi Controller Settings

Broadcast/Multicast Control

When left unchecked, broadcast and multicast network traffic can severely reduce the available airtime on the HD WLAN, leading to decrease in speed, increase in latency, and potential connectivity problems for clients. Consider segmenting the wired and wireless portions of the network through VLAN assignment at time of WLAN creation. Alternatively, consider Port Isolation at the switch layer to limit unnecessary traffic and conserve precious airtime available to stations in the HD WLAN.

SSIDs

To ensure maximum Access Points make efficient use of airtime, limiting the number of SSIDs announced throughout the HD WLAN is a vital detail. Although UAPs support up to 4 SSIDs per radio band, most scenarios (including HD WLANs) only require two SSIDs to support two types of security: Open for 'Guests' and WPA2-PSK or -EAP for trusted, 'Corporate' users). For client roaming reasons, use the same SSIDs throughout the entire HD WLAN coverage area (e.g., SSID-event) rather than complicated naming schemes (e.g., SSID-11th-floor, SSID-lobby). Any SSID that serves a nominal purpose separate from the capacity objectives of the HD WLAN (e.g., SSID-admins) does not warrant existence.

Traffic Shaping

To limit the impact of data hungry users and applications that jeopardize the availability of bandwidth and airtime on the HD WLAN, define widespread rate limits (in Mbps) via the User Groups feature. Speed limits that are too strict can detrimentally affect the performance of the wireless network, while too high of speed limits the effectiveness of traffic shaping.

Minimum RSSI

Following association and/or when roaming in the HD WLAN coverage area, client devices negotiating at low speeds (due to long distance from the AP) have a negative impact on the aggregate performance of the wireless cell through poor airtime efficiency. Therefore, proper design and architecture of HD WLANs paired with signal threshold levels helps ensure that clients remain connected to the intended AP cell offering them the best performance. When defining the Minimum RSSI setting, WLAN administrators must be careful, since too strict threshold levels can result in severe, widespread connectivity problems that cripple user activity on the network. For HD WLANs, Ubiquiti recommends setting the Minimum RSSI to no greater than -75 dBm, where lower thresholds levels (e.g., -80 dBm) mean clients will remain connected to the AP at greater distances from the center of the cell coverage area. Because UniFi Minimum RSSI uses a 'soft' kick implementation, whether or not the station disassociates from the AP is ultimately determined by the client device itself.

Band Steering

Although an increasing number of client devices today support and even prefer 5G operation, balancing the client activity between wireless bands often fails in large part due to the strong signals and propagation characteristics of the 2G band. In dual-band HD WLAN scenarios therefore, steering capable wireless clients to the 5G band is a particularly vital configuration setting to avoid 2G band congestion. Because UniFi Band Steering uses a 'soft' steering implementation, whether or not the station associates and remain connected to the 5G band is ultimately the decision of the client device itself.

Load-Balancing

The unpredictability introduced by variables like user attendance and roaming can often result in scattered wireless activity through the HD WLAN. While emphasis on proper design, architecture, and AP placement precedes and carries more importance than post-deployment configuration 'tricks', the UniFi load-balancing technique defines a soft user-ceiling whereby APs attempt to kick the clients with the weakest signals until the total number of associated clients returns to the defined threshold. Because UniFi load-balancing uses a 'soft' kick implementation, whether or not the station disassociates from the AP is ultimately determined by the client device itself.

A. Appendices

802.11n/ac Data Rate Matrices

HT MCS Index	Spatial Streams	Modulation & Coding	Data Rate GI=800ns	Data Rate SGI=400ns	Data Rate GI=800ns	Data Rate SGI=400ns	Data Rate GI=800ns	Data Rate SGI=400ns	Data Rate GI=800ns	Data Rate SGI=400ns	VHT MCS Index
			20MHz		40MHz		80MHz		160MHz		
0	1	BPSK 1/2	6.5	7.2	13.5	15	29.3	32.5	58.5	65	0
1	1	QPSK 1/2	13	14.4	27	30	58.5	65	117	130	1
2	1	QPSK 3/4	19.5	21.7	40.5	45	87.8	97.5	175.5	195	2
3	1	16-QAM 1/2	26	28.9	54	60	117	130	234	260	3
4	1	16-QAM 3/4	39	43.3	81	90	175.5	195	351	390	4
5	1	64-QAM 2/3	52	57.8	108	120	234	260	468	520	5
6	1	64-QAM 3/4	58.5	65	121.5	135	263.3	292.5	526.5	585	6
7	1	64-QAM 5/6	65	72.2	135	150	292.5	325	585	650	7
	1	256-QAM 3/4	78	86.7	162	180	351	390	702	780	8
	1	256-QAM 5/6	n/a	n/a	180	200	390	433.3	780	866.7	9
8	2	BPSK 1/2	13	14.4	27	30	58.5	65	117	130	0
9	2	QPSK 1/2	26	28.9	54	60	117	130	234	260	1
10	2	QPSK 3/4	39	43.3	81	90	175.5	195	351	390	2
11	2	16-QAM 1/2	52	57.8	108	120	234	260	468	520	3
12	2	16-QAM 3/4	78	86.7	162	180	351	390	702	780	4
13	2	64-QAM 2/3	104	115.6	216	240	468	520	936	1040	5
14	2	64-QAM 3/4	117	130.3	243	270	526.5	585	1053	1170	6
15	2	64-QAM 5/6	130	144.4	270	300	585	650	1170	1300	7
	2	256-QAM 3/4	156	173.3	324	360	702	780	1404	1560	8
	2	256-QAM 5/6	n/a	n/a	360	400	780	866.7	1560	1733.3	9
16	3	BPSK 1/2	19.5	21.7	40.5	45	87.8	97.5	175.5	195	0
17	3	QPSK 1/2	39	43.3	81	90	175.5	195	351	390	1
18	3	QPSK 3/4	58.5	65	121.5	135	263.3	292.5	526.5	585	2
19	3	16-QAM 1/2	78	86.7	162	180	351	390	702	780	3
20	3	16-QAM 3/4	117	130	243	270	526.5	585	1053	1170	4
21	3	64-QAM 2/3	156	173.3	324	360	702	780	1404	1560	5
22	3	64-QAM 3/4	175.5	195	364.5	405	n/a	n/a	1579.5	1755	6
23	3	64-QAM 5/6	195	216.7	405	450	877.5	975	1755	1950	7
	3	256-QAM 3/4	234	260	486	540	1053	1170	2106	2340	8
	3	256-QAM 5/6	260	288.9	540	600	1170	1300	n/a	n/a	9

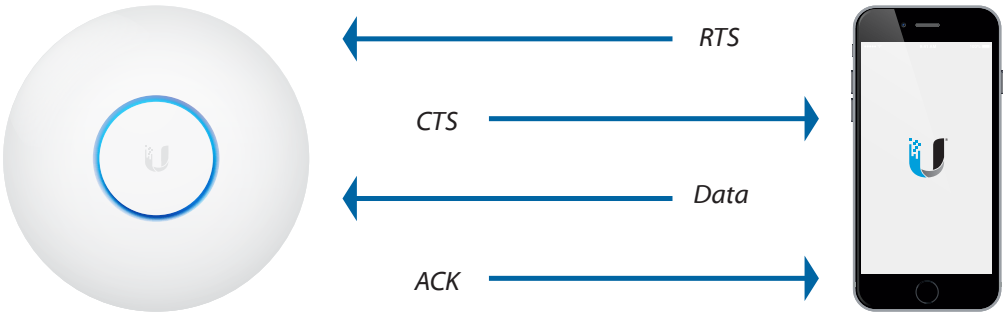
UniFi Device Statuses

- Adopting – The Controller establishes an SSH Connection to the UniFi Device for the purpose of lasting, remote management.
- Connected – The Controller can reach and communicate with the UniFi Device should any configuration updates be required.
  When (wireless) appears next to Connected, the UniFi Access Point is wirelessly connected to an Uplink UniFi AP. When (needs upgrade) appears next to Connected, the UniFi Device is using a firmware version earlier than the UniFi Controller.
- Provisioning – The Controller has issued a setting change that results in Configuration Updates at the UniFi Device. Once applied, the UniFi Device will quickly reboot before returning to its Connected State.
- Pending – The UniFi device is discoverable by the controller and is ready to be adopted.
- Heartbeat Missed – The Controller did not receive a beacon from the UniFi Device at the expected interval.
- Disconnected – Following a period of Missed Heartbeats, the Controller reports that it is unable to manage the UniFi Device. Check cables, network settings, and changes to topology that could disrupt end-to-end Connectivity.
- Isolated – A UniFi AP with power but unable to reach its Internet Gateway will, by default, wirelessly announce to nearby, wired UniFi APs that it is Isolated and seeking Wireless Uplink to re-establish Connectivity to the Controller & service WLAN Clients.
- Managed by Other – The Controller has Discovered the UniFi Device but has previously come under management by another Controller. To adopt the managed UniFi Device to the new Controller, enter the Device Username & Password, listed under the Site Settings for the Controller to which the Device is already adopted.

WMM & DSCP Values

802.1p Class of Service	TOS Range	DSCP Range	WMM Category
0 - Best Effort	0x00-0x1f	0-7	Best Effort
1 - Background	0x20-0x3f	8-15	Background
2 - Spare	0x40-0x5f	16-23	Background
3 - Excellent Effort	0x60-0x7f	24-31	Best Effort
4 - Controlled Load	0x80-0x9f	32-39	Video
5 - Video (<100ms latency)	0xa0-0xbf	40-47	Video
6 - Voice (<10ms latency)	0xc0-0xdf	48-55	Voice
7 - Network Control	0xe0-0xff	56-63	Voice

802.11 - Wireless - CSMA/CA
RTS/CTS Mechanism



Characteristic	Large Cell	Small
Objective	Coverage	Density
Transmit Power	High	Low
Best Frequency	2G	5G
Average Signals	Lower	Strong
Average Speeds	Lower	Higher
Deployment Complexity	Low	High
Hardware Recommendation	UAP-AC-Outdoor	UAP-AC-PRO
	UAP-Outdoor with AMO-2G-13	UAP-Outdoor+ with AM-V2G-Ti

HTTPS & SSL Certificates

URL: < https://help.ubnt.com/hc/en-us/articles/212500127>

Many enterprise networks rely on HTTPS and Secure Socket Layer (SSL) to encrypt sensitive traffic from end-to-end. In this way, SSL certificates can be paired with the UniFi Controller in order for clients to verify from the browser that the UniFi-hosted Hotspot is a trusted party. SSL certificates can be purchased from a number of different web hosting companies, then integrated with the Controller. Once successfully paired, trusted site certificates will appear in the guest browser.

In order to integrate site certificates, follow the steps outlined below:

```
sudo su -

# cd <unifi_base>

# on Windows, "%USERPROFILE%/Ubiquiti Unifi"

cd /usr/lib/unifi


# create new certificate (with csr)

java -jar lib/ace.jar new_cert <hostname> <company> <city> <state>
<country>


# your CSR can be found at /var/lib/unifi

# - unifi_certificate.csr.der

# - unifi_certificate.csr.pem


# have this CSR signed by a CA, you'll get a few certificates back...

# copy the signed certificate(s) to <unifi_base>


# import the signed certificate and other intermediate certificates

java -jar lib/ace.jar import_cert <signed_cert> [<other_intermediate_
root_certs>...]
```

B. Glossary

- **AP** An access point is a network device that allows stations to wirelessly connect to the LAN.
- **Broadcast traffic** Network traffic destined to all nodes on the LAN.
- **CSMA/CA** Carrier Sense Multiple Access / Collision Avoidance is the access protocol for 802.11, whereby APs/stations listen to the wireless medium before transmitting data to the desired node to avoid collisions.
- **CSMA/CD** Carrier Sense Multiple Access / Collision Detection is the access protocol for 802.3, whereby nodes listen to the Ethernet medium before transmitting data to the desired node and can detect collisions.
- **Encryption** The manner by which data is translated to a unique code/language that is understood by the original sender and the intended recipient (those parties holding the encryption keys).
- **Hidden Node Problem** A common problem faced by standard 802.11 networks: Whenever two or more stations are connected to the same AP but cannot hear each others' transmissions, there is increased risk for collisions on the wireless network.
- **HSR** High-Selectivity Receiver technology available on Multi-Lane RF UniFi models to help reject adjacent, co-channel interference.
- **GI** Guard interval represents the time between transmissions to help prevent intersymbol inteference—not to be confused with interframe space (IFS) that represents the time between transmitted packets. Shorter guard intervals are possible with 802.11n/ac and allow for higher throughput.
- **IP Address** The logical address which devices (such as routers) use to forward data to its final destination (IPv4 and IPv6 are layer-3 address assignments).
- **LAN** Local area network; interconnected nodes usually located in the same physical location.
- **Layer-2** The second level of data communications according to the OSI Model (where network switches and most access points communicate based on MAC address assignments).
- **Layer-3** The third level of data communications according to the OSI model (where routers communicate based on logical address assignments).

- **Load-balancing** A characteristic of the UniFi system, which enables shuffling of WLAN clients among UAPs for better distribution of stations per AP.
- **MIMO** Multiple-Input, Multiple-Output. The use of multiple antennas to send multiple streams of data simultaneously between transmitter and receiver, expressed in the format 2x2, 3x3, etc.
- **Multicast** Network traffic destined to specific group of nodes on the LAN.
- **OSI Model** The 7-layer model for data communication whereby software protocols and hardware interact to pass information.
- **QoS** Quality of Service defines prioritization of packets such as video and VoIP in order to guarantee best network performance.
- **Radio Band** The spectrum on which a radio operates, such as 2.4 GHz, 5 GHz, or both simultaneously (dual-band radio).
- **Router** The Layer-3 device that is largely responsible for internetwork communication while switching/filtering packets and path selection.
- **SNMP** The Simple Network Management Protocol is used to monitor and report information as gathered by managed devices on a network.
- **Station** Any wireless node connected to an 802.11 network.
- **Switch** Typically a Layer-2 device that functions similarly to a multi-port bridge.
- **UAP** Ubiquiti's proprietary access point for enterprise networks—combines high performance with disruptive pricing.
- **VLAN** Virtual LANs are a layer-2 technology that allow enterprise networks to create division of networks on the same physical network architecture, while helping to reduce the size of broadcast domains.
- **WLAN Controller** The node responsible for central management of devices on the wireless LAN, including stations and access points.
- **WMM** Wi-Fi Multimedia. QoS standard for 802.11 networks based on DSCP (Differented Services Code Point) header values—higher means more priority.

031317v2.1

For information about future training dates, locations, and courses, visit the official training portal of Ubiquiti Networks: **www.ubnt.com/training**

We'd like to hear your feedback!
Contact us at **training@ubnt.com**

©2012-2017 Ubiquiti Networks, Inc. All rights reserved. Ubiquiti, Ubiquiti Networks, the Ubiquiti U logo, the Ubiquiti beam logo, airFiber, airMAX, airOS, airVision, EdgeMAX, mFi, and UniFi are trademarks or registered trademarks of Ubiquiti Networks, Inc. in the United States and in other countries. All other trademarks are the property of their respective owners.

NB031517v2.1