Why is it so hard to deliver reliable Wi-Fi?

Technology guide

Table of contents

Demand for Wi-Fi

The explosive growth in devices and applications has resulted in an insatiable demand for faster and better
for over a decade. During this time, Wi-Fi has proven to be a cost-effective method for providing devices and users network connectivity.

To keep pace with the explosion of devices and their insatiable appetite for bandwidth, the Wi-Fi industry ratifies a new standard every five to seven years that addresses the shortcomings of previous standards while supporting new uses for Wi-Fi. 802.11ax is the latest iteration in the evolution of Wi-Fi that increases network performance on multiple axes of performance. With each new version of the standards, the development community ensures the inclusion of the latest technology, signal processing, and optimization techniques, such as OFDMA, 1024-QAM and wake-time parameters that improve peak data rates approaching 10 Gbps, deliver more concurrent device connections up to 74, and optimize power usage per device.

Standards and beyond

While 802.11ax improves core Wi-Fi performance, there continues to be an unabated need to deliver great Wi-Fi technology that goes beyond the standards. Delivering great Wi-Fi is hard, and it's only getting harder. The biggest, most endemic problems fall into eight categories.

Problems

- **Mobility:** When a user moves out of the coverage range of an access point (AP)—and must connect to another AP in the same network—the WLAN network must migrate the user's devices gracefully without disruptions.
- **Interference:** Walls and floors, other Wi-Fi networks, and appliances can all interfere with the Wi-Fi network, leading to network congestion and a poor user experience.
- **Security:** Lack of adherence to best practices for securing the network opens hackable attack surfaces for malicious actors looking to steal intellectual property, money and personal identities. The KRACK exploit threatened billions of Wi-Fi devices overnight in 2017 and made headline news.
- **Standards:** With the explosion of IoT devices, a new set of wireless connectivity standards has emerged such as Bluetooth LE, Zigbee, LoRA, NB-IoT and more. The traditional AP is now tasked to support not just Wi-Fi.
- **Infrastructure:** Supporting infrastructure that sits behind the AP is just as important. Technologies such as multi-gigabit Ethernet, 802.3bz and the latest PoE standards like 802.3bt are critical for delivering great Wi-Fi performance.
- **Deployment:** Physical constraints can prevent the deployment of Wi-Fi within street furniture, in vehicles and other space-restricted locations such as light poles. The delivery of Wi-Fi requires defining form factors that are not mandated by the standards body.
- **Density:** Ultra-dense environments with very large numbers of users and devices present in a small area like a stadium or transit hub create unique Wi-Fi challenges that lead to a deterioration in the Wi-Fi network performance.
- **Applications:** 4K video streaming, virtual and augmented reality, and live-stream gaming all consume far greater bandwidth today than 128 Kbps streaming music of times past.

These challenges must be addressed in order to deliver great Wi-Fi.

Technology matrix

At CommScope, we've designed technologies to minimize these problems. Learn about the CommScope Technology Matrix and how each technology addresses the problems with delivering great Wi-Fi that delivers beyond the standard.

Problems	Mobility	Interference	Security	Standards	Infrastructure	Deployment	Density	Applications
Transient client management	X						X	
Airtime decongestion							X	
Adaptive Wi-Fi cell sizing		X					X	
Per-packet adaptive transmit power		X					X	
Network capacity utilization							X	
BeamFlex		X				X	X	
Airtime fairness							X	
Band balancing	X					X	X	
Client load balancing	X						X	
SmartRoam	X							
SmartCast								X
ChannelFly		X				X		
SmartMesh						X		
DPSK			X					
Cloudpath			X					
L3 – L7 traffic control								X
Specialty APs		X				X		
RUCKUS IoT suite				X				
LTE APs				X				
Multi-gigabit Ethernet					X			
Power over Ethernet					X			

Figure 1. CommScope Technology Matrix

Problem: Mobility

In simple terms, a Wi-Fi network consists of a set of fixed, stationary access point radios that serve a large and non-stationary number of user devices (clients). A problem any Wi-Fi network must solve is how best to distribute the client devices across all available radio resources, and adapt to their physical movement. Some typical issues that arise from this problem are:

- **Sub-optimal client:** AP distributions, e.g., one AP may have an excessively high number of clients attached while other APs sit largely idle—the quality of experience that clients on the oversubscribed AP will suffer.
- **Poor use of available spectrum:** A disproportionate number of clients may connect to the Wi-Fi network over the congested 2.4 GHz band while leaving the 5 GHz band under-utilized, again resulting in poor quality of experience for end users.

- **Poor client roaming experiences:** In Wi-Fi, client devices make their own roaming decisions. They must do so based on the limited information they can glean from network scanning—i.e., which APs they can detect and at what signal strength—and their roaming algorithms are typically limited in terms of their ability to robustly handle the vast number of possible scenarios in a Wi-Fi network. This can result in several problems. For example:
  - **Sticky devices:** A client moves away from the AP it is attached to, yet remains connected to it even when there may be another, closer AP available to serve that client at higher capacity.
  - **Ping-ponging:** A client device is able to "see" multiple APs in a given location and bounces back and forth between them because its roaming logic frequently changes its evaluation of which is the best AP to connect to.
  - **Interrupted connectivity due to roaming:** When roaming from one AP to another, a client needs to re-authenticate with the new AP before connectivity can be restored—if re-authentication takes too long, the client will experience periods of no connectivity, which can impact applications adversely and result in a poor quality of experience for the end user.

CommScope technology

Transient client management

In a dense Wi-Fi network, transient clients can degrade the user experience for other connected clients. This problem is typical in train stations, bus terminals and various public hot spot venues where thousands of devices move through an area, sending management frames that an AP will hear but without the need to connect. This overwhelms the network with needless traffic and thus slows or makes the Wi-Fi inoperable.

The RUCKUS® Transient Client Management capability mitigates this degradation in performance using statistical methods to delay the AP's associations with transient clients. Venue administrators and IT administrators can tune configuration parameters based on typical dwell times and received signal strength indicator (RSSI) of the transient clients with accrued heuristics-based techniques that selectively respond to transient clients.

The main benefit of this feature is efficient airtime utilization that maximizes the attention toward connected non-transient clients.

Band balancing

RUCKUS APs balance the client load between the 2.4 GHz and 5 GHz bands on the network, to mitigate the occurrence of one band being over-utilized while the other is under-utilized. Each AP actively monitors the client load per band, as well as client capabilities, and decides on a per-client basis on which band to connect that client. The AP then steers the client to the preferred band using a variety of techniques, including 802.11v BTM messaging.

Client load balancing

Client load balancing seeks to improve WLAN performance by optimally distributing clients between nearby access points, so that one AP does not get overloaded while another sits idle. Each AP scans the air to determine which other APs on the network are physically near it, and then uses this knowledge as well as its own client loading to determine if it should steer clients to alternate APs.

SmartRoam

RUCKUS SmartRoam technology addresses the roaming challenges described above by proactively monitoring client connection strength and facilitating client roaming to mitigate the side effects of poor roaming decisions made by clients alone. For example, if the connection strength (RSSI) of a client device is detected to fall below a roaming threshold, the AP to which it is connected will use technologies such as 802.11v BSS transition management messaging and 802.11k neighbor lists to steer the client to a roaming destination AP. In addition, RUCKUS SmartRoam technology utilizes 802.11r as well as opportunistic key caching (OKC) to minimize roaming time—and therefore ensure seamless connectivity during roaming—by pre-emptively storing authentication credentials for each client on APs, which are roaming candidates.

Problem: Interference

Travel to any country, and Wi-Fi devices work over the same frequencies. However, the downside to Wi-Fi is that it is also unrestricted. Bluetooth devices, legacy cordless phones, microwave ovens and more constantly emit RF signals, especially over 2.4 GHz. All that noise generates interference, preventing APs from maintaining a clear, strong signal with each client.

As Wi-Fi continues to be deployed anywhere and everywhere, interference from other Wi-Fi APs (co-channel interference) becomes a big problem. That applies both to APs broadcasting within the same venue, as well as nearby APs from other organizations broadcasting over the same RF channels as yours. (Think of an office building hosting several different companies on the same few floors.) The Wi-Fi infrastructure needs to recognize sources of interference and employ sophisticated techniques to mitigate them.

CommScope technology

Per-packet adaptive transmit power

APs typically transmit at maximum power to increase coverage and optimize data throughput for distant clients. But this can cause radio interference (co-channel interference) for adjacent APs in the same network. To address this issue, the RUCKUS per-packet adaptive transmit power factors in the client proximity (RSSI) and dynamically lowers transmit power levels while maintaining a constant modulation rate (MCS) on a per-packet basis to maximize performance. This results in reduced co-channel interference and higher average throughput per client.

Adaptive Wi-Fi cell sizing

Optimizing Wi-Fi performance is a challenge due to interfering environmental factors from devices to users. At the time of deployment, APs are placed for optimal performance; but, as users and the environment change, APs may oversaturate coverage in some spaces, while under-saturating coverage in others. CommScope uses periodic co-channel neighbor scans and radio interface estimates to adjust Wi-Fi broadcast patterns and adjusts them in real time based our machine learning algorithms. This technique—in combination with per-packet adaptive transmit power—greatly optimizes performance to each client in under- and over-deployed Wi-Fi networks.

BeamFlex adaptive antennas

When conventional APs are deployed in close physical proximity, each using omnidirectional antennas to send out RF signals everywhere, co-channel interference is a problem. RUCKUS BeamFlex adaptive antennas direct RF signals to the right place—to dramatically minimize the negative effects of interference. See Problem: Density—BeamFlex for more details.

ChannelFly

Most enterprise WLAN APs can migrate a device to a less congested RF channel, but ongoing analysis of changing data traffic is necessary to maintain a healthy network. RUCKUS ChannelFly technology uses machine learning to continually assess all available channels and measure the real-world capacity improvement each one can provide—before it directs the AP to switch channels.

Every country reserves certain RF frequencies for sensitive locations like airports and military installations, and regulates how unlicensed wireless devices operate over those channels using dynamic frequency selection (DFS). If your deployment is near a DFS zone, your AP has fewer channels to choose from when trying to mitigate interference and direct every client to the best-performing option.

ChannelFly was originally developed for Wi-Fi hotspots, where RF channels are highly congested. Even in dense public settings, ChannelFly, working hand-in-hand with BeamFlex, delivers significant improvements in AP and network capacity—automatically. Learn more here.

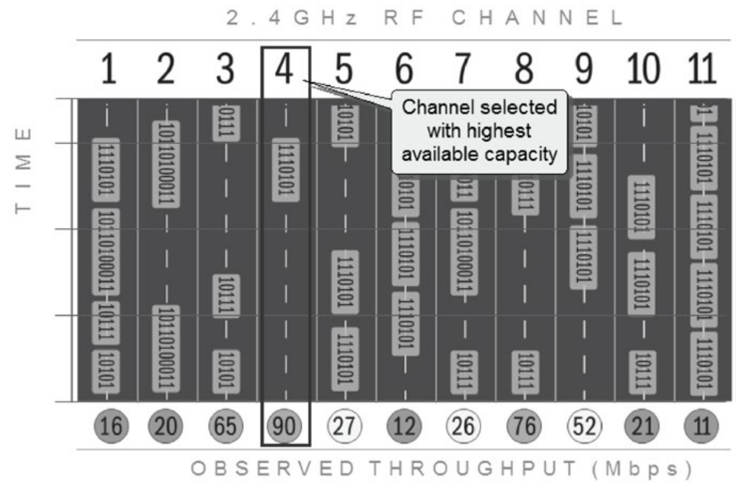

Figure 2. ChannelFly

Problem: Security

Securing Wi-Fi is challenging for enterprises of all sizes due to potential vulnerabilities in both the infrastructure (which can be controlled) and the clients (which often cannot be controlled). Man-in-the-middle breaches, denial-of-service attacks, and zero-day vulnerabilities are not the only sophisticated exploits concerning CSOs and network administrators. There are more prosaic concerns like passwords, which can be forgotten, shared and reused, making them insecure. However, networks that must onboard large numbers of guest users and support bring-your-own-device (BYOD) environments face these challenges daily. Do enterprises use a pre-shared key (PSK)—a single universal password—to onboard visitors and BYOD users? When everybody knows the password, there are limited means to control who is given access without changing the access method for everyone. Administrators are advised to follow security best practices recommended by network vendors and industry experts, and take advantage of the security defenses built into existing equipment.

CommScope technology

DPSK

Unlike conventional pre-shared keys, where the same network password is used by everyone, RUCKUS Dynamic PSK (DPSK) technology builds on the PSK standard to provide every device with a unique PSK credential. Users can still enter a single, shared alphanumeric "password," but RUCKUS SmartZone controllers automatically convert that passphrase to a unique dynamic key just for that device. By provisioning each device uniquely, you get the benefits of per-device or per-user credentials found in 802.1X, with the usability and simplicity of PSK. You can create (and revoke) credentials for any user or device, and set dates for credentials to expire. Each DPSK can also be tied to a unique role or policy, so you can grant different levels of access to different types of users and devices.

Certificates/Cloudpath

These days, organizations that are tired of dealing with insecure, shared or forgotten passwords use certificates instead. RUCKUS Cloudpath Enrollment System makes it easy to implement certificate-based Wi-Fi and build flexible, fine-grained policy control on top of your existing network. Users can onboard their devices in seconds and gain access to the resources allowed for their role and device type, based on policy. From then on, the device will automatically, securely connect until the certificate expires—without users re-entering credentials, and without IT intervention. Find out more here.

WIDS/WIPS

Rogue access points, man-in-the-middle attacks, misconfigured access points, zero-day attacks or WPA2 loopholes are just a few ways hackers can breach network defenses and expose networks to malicious threats. RUCKUS APs feature built-in wireless intrusion detection system and wireless intrusion prevention system (WIDS/WIPS) technology to combat risks to the network. Administrators can aggressively root out unauthorized APs—without creating issues for legitimate APs from neighboring organizations.

RUCKUS APs are able to detect three types of threats: SSID-spoofing, MAC-spoofing and LAN-spoofing. The rogue APs, thus detected, are marked as “malicious” and are effectively quarantined from the network. A legitimate RUCKUS AP will send out broadcast deauthentication frames to alert clients to disconnect from the malicious AP.

CommScope also provides a user-configurable “rogue classification” option for IT administrators to customize their rogue AP detection policy. Based on these policy decisions, the entire list of known APs is scrutinized and all APs are re-classified as malicious or not. RSSI threshold-based decisions allow for benign, non-malicious APs to co-exist on the periphery of a CommScope-based Wi-Fi deployment.

Problem: Standards

With the rise of the internet of things (IoT), the industry is seeing an explosion in the number of devices connecting wirelessly—and not necessarily over Wi-Fi. Different devices and applications in an organization may connect over Bluetooth Low Energy (BLE), Zigbee, RFID, Near Field Communications (NFC), LTE and more. Without careful planning (and capable technology), the result will be a large number of overlay networks and standards to manage and operate.

Ideally, all of these new networks and standards should be able to run over a single, converged network. Instead of trying to juggle a dozen different new infrastructures, enterprises should be able to use the same management and security architectures in place for Wi-Fi, and extend them to every other wireless-connected device, regardless of the radios used.

The growth in IoT devices and the need for an IoT-enabled LAN is driving the concept of an IoT access network. As more and more IoT devices enter the network, the traditional WLAN or LAN will be augmented or replaced by the need for an all-purpose access network that interconnects all IoT devices within a limited area such as a residence, school laboratory, university campus or office building.

CommScope technology

RUCKUS IoT suite

Organizations seeking to deploy IoT solutions face a complex, fragmented ecosystem of standards, devices and services. This complexity often slows or stalls enterprise IoT deployments, due to uncertain return on investment. An IoT access network addresses these issues by consolidating multiple physical-layer networks into a single converged network. This common network simplifies IoT endpoint onboarding, establishes uniform security protocols and converges IoT endpoint management and policy setting. The RUCKUS IoT suite simplifies the creation of IoT access networks through the reuse of LAN and WLAN infrastructure, thus shortening deployment duration and reducing the cost to support multiple IoT solutions. Learn more here.

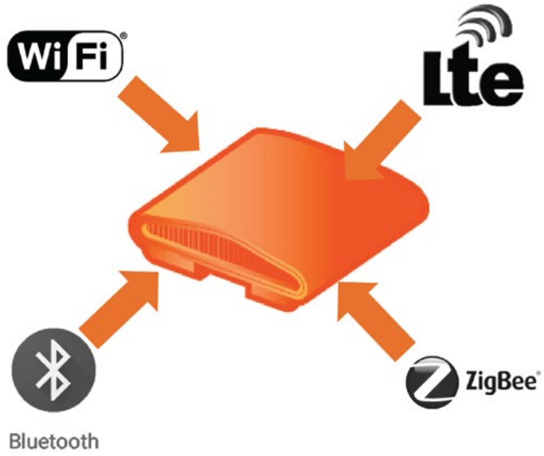

Figure 3. Consolidated wireless standards

CBRS LTE

Operators of Wi-Fi networks have no control over the experience users receive when connecting over Wi-Fi. If an important conference call disconnects, or students cannot receive texts from within the residence hall, users inevitably blame the service provider. The recently launched Citizens Broadband Radio Service (CBRS) initiative allows venue operators to extend cellular coverage deep inside buildings over an unlicensed radio spectrum. RUCKUS CBRS technology offers the industry's first CBRS cellular solution in a real-world product. Using the CBRS band, operators can support the deployment of private LTE networks for enterprises as easily as deploying Wi-Fi, using the same AP form factor. This vastly improves the mobile coverage and the capacity of the LTE networks. Learn more here.

Problem: Infrastructure

Reliable Wi-Fi requires a well-matched wired infrastructure that provides high performance and high reliability, is easily managed, and can scale to meet ever-increasing Wi-Fi demands.

To have high-performance Wi-Fi, it's essential to have sufficient performance in the switching underlay. If the underlying network can't keep up with the data from access points, then you won't get the full value from them. The wired infrastructure needs to provide adequate speed for connections to the switch (e.g., from the access point), as well as the uplinks to aggregation and core switches.

Other factors in the switching infrastructure necessary for great Wi-Fi include the ability to deliver sufficient power over Ethernet (PoE), resiliency to maintain connectivity, simplified management and the ability to meet requirements now and for the life of the network.

CommScope technology

Multi-gigabit connectivity

802.11ax and future wireless technologies can exceed the connection performance of Gigabit Ethernet (GbE) switch ports. CommScope offers 2.5 GbE multi-gigabit connections in an entry-level switch, which includes all the performance as required by an 802.11ac Wave 2 AP. Additional switches with 1/2.5/5/10 GbE ports support 802.11ax and future generations of the Wi-Fi standards. Additionally, CommScope switches offer up to 100 GbE uplinks with entry-level switches upgradable to 10 GbE and high-end switches upgradable from 40 GbE to 100 GbE uplinks with a simple CLI command.

Power over Ethernet (PoE)

Power over Ethernet (PoE) is the primary method of providing power to wireless access points. The latest generation of 802.11ac Wave 2 access points and new 802.11ax access points can operate on 30 watts of power (PoE+). However, additional power is required to deliver full power to all radios and to provide power to the USB port on the AP for optional devices. The new IEEE 802.3bt standard establishes protocols for higher PoE levels.

SmartZone™ network controller

CommScope enables IT to deploy a single network element—the network controller—to simultaneously and directly control and manage both wired and wireless networks. RUCKUS SmartZone network controllers simplify the complexity of scaling and managing wired switches and wireless access points through a common interface to support private-cloud network-as-a-service offerings in addition to general enterprise networks. SmartZone support for multi-tenancy, domain segmentation and containerization enables secure delivery of managed networking services with complex, multi-tiered service levels.

Problem: Deployment

Access point deployment is a complex subject that requires extensive design guidelines and field site surveys to help optimize network performance. For example, can using wider channel sizes boost network capacity in densely populated environments? How does the use of wider channels balance against the need for more channels for use with more APs? Having fewer APs operating on the same channel decreases the likelihood of noise, co-channel and adjacent channel interference, which will increase the expected performance gains. These decisions are only a few of the considerations among many. The technology that automates and simplifies deployment complexity matters. APs must also ease physical deployments—making the deployment of Wi-Fi in harsh or hard-to-reach environments easier.

CommScope technology

ChannelFly

RUCKUS ChannelFly intelligence selects the optimal channel among all available options. Devices are automatically pushed to the best-performing channel, avoiding DFS channels, without users (or WLAN operators) needing to manually intervene. See Problem: Interference—ChannelFly for more details.

SmartMesh

Deploying an AP in an area where there is no easy way to run cable is a challenge. RUCKUS SmartMesh eliminates Ethernet cabling to every Wi-Fi access point, while also reducing cumbersome RF planning. SmartMesh simplifies the cost of a WLAN deployment. The SmartMesh allows APs to be connected by Ethernet as well to form new trees in the middle of the mesh and thus take advantage of spectrum reuse to increase system capacity while expanding the mesh. APs automatically determine their role in the mesh, and automatically react to topology changes. Additionally, the technology automatically directs Wi-Fi signals over the best-performing paths between nodes. And intelligent BeamFlex antennas extend signal range, minimizing the number of mesh hops and reducing the number of APs you need to deploy. SmartMesh is enabled with a simple check box within the administrative interface.

Specialty APs

Every deployment has its own unique requirements. Providing Wi-Fi in every room of a hotel or residence hall, for example, requires a different type of platform than serving an enterprise office. Deploying Wi-Fi outdoors, or in a large stadium, demands still other considerations. CommScope offers a large portfolio of indoor and outdoor AP options to suit any type of deployment. This includes wall-mounted Wi-Fi + Ethernet switch platforms for hospitality and multi-dwelling unit environments, and solutions that run over a building's existing coaxial cabling.

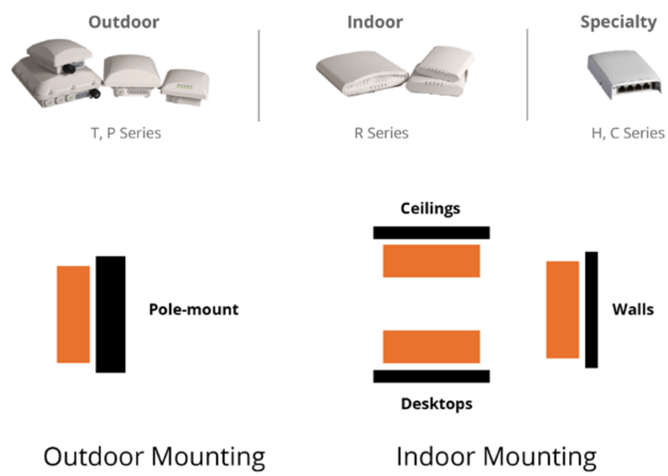

Figure 3. Multiple AP types

Problem: Density

Convention centers, stadiums and other crowded venues are the toughest Wi-Fi environments, for obvious reasons. When tens of thousands of devices are fighting over Wi-Fi resources in the same space, the performance of each device can deteriorate quickly. One AP may be required to service hundreds of devices at the same time, which can lead to a poor user experience. An AP needs to solve common problems at the physical layer that can thwart a great user experience:

- **Ping-ponging devices:** An inability for devices to find the "right" AP to connect with when it sits between two equally reasonable APs.
- **Sticky devices:** Mobile devices can stay connected to one AP too long while roaming instead of switching to a closer AP that could provide a better connection.
- **Dominant devices:** Some older devices, or those with poorly written device drivers, occupy a disproportionate amount of the AP's air-time resources—to everyone else's detriment.
- **Chatty devices:** Modern wireless devices use self-discovery and self-provisioning protocols that are "chatty" with management traffic and clog airways in device-heavy environments.

Additionally, APs must optimize for the best modulation scheme, encoding rate, guard interval and other Wi-Fi parameters in real time for each device. APs are constantly evaluating the appropriate channel bandwidth, spatial streams and transmit antenna pattern to utilize. Each represents an AP decision that can lead to an optimal or sub-optimal user experience. The CommScope ultra-high density suite addresses these challenges and provides exceptional end-user experience within stadiums, large public venues, convention centers and school auditoriums.

CommScope technology

BeamFlex adaptive antennas

Traditional APs use “omnidirectional” antennas that radiate signals in all directions. Conversely, RUCKUS BeamFlex adaptive antennas allow RUCKUS APs to dynamically choose among a host of antenna patterns (over 4,000 possible combinations) in real time to establish the best possible connection with every device. BeamFlex works on a per-packet basis to optimize the user experience. In addition, BeamFlex uniquely supports mobile devices by adapting antenna transmissions to a device’s orientation in both vertical and horizontal axes through our PD-MRC technology.

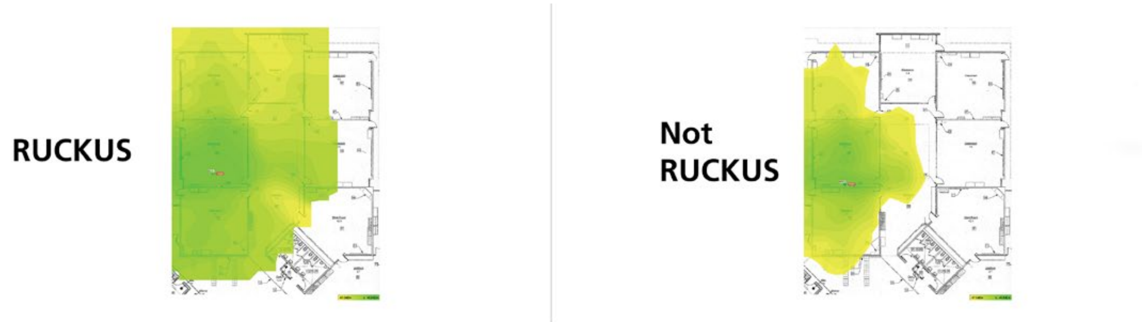

Figure 4. BeamFlex adaptive antennas

Airtime fairness

Like having too many cars on a freeway, too many wireless devices fighting for access to the same APs can cause network congestion and poor network performance. To keep traffic flowing, APs need to balance data traffic so each device receives sufficient airtime. CommScope’s airtime fairness algorithms provide each device an appropriate amount of “airtime” to transmit and receive data. The algorithm balances the needs of slower legacy devices with that of faster devices so older or more distant clients do not slow everyone else down, or that faster devices do not take all the bandwidth in the air.

Band balancing

A CommScope network monitors all clients in the environment to track whether they’re single- or dual-band, and which types of APs are in their proximity. If there’s a lot of traffic on the 2.4 GHz frequency, for example, and a dual-band client tries to connect, the AP steers that device to the cleaner, higher-capacity 5 GHz band instead. Users on each band benefit, because they’re now sharing that spectrum with fewer devices. In ultra-dense venues, the combination of band balancing and airtime fairness delivers a significant performance boost.

Client load balancing

Certain APs are more likely to get congested initially in device-dense environments—like the first AP near a convention center or stadium door, which everyone connects with first when entering the venue. The key is to make sure these devices migrate seamlessly to another AP that can provide equally good performance (solving the sticky client problem). RUCKUS APs communicate with each other and use client load-balancing algorithms to monitor client load across all APs in the venue and drive new clients to less congested APs. Factors that influence channel management include device per-band allocation, channel throughput utilization, and device count per AP along with other metrics. The CommScope network controls how and where each client connects to distribute the load more evenly—automatically.

SmartCast

As more people use live-streaming applications in public spaces, they need high-definition broadcast-quality video. RUCKUS SmartCast technology maximizes the reliability and performance of delay-sensitive applications (such as IP-based voice and video) over 802.11 networks. Utilizing the basic framework of 802.11e/WMM to categorize traffic, SmartCast extends this standard and delivers a collection of unique capabilities, including packet inspection, automatic traffic classification, and advanced queuing and scheduling to ensure bandwidth-intensive applications get the performance they need, without drowning out everything else.

SmartCast algorithms automatically schedule and pre-queue traffic on a per-client, per-packet basis. This allows for more fine-grained classification and scheduling than global network-layer QoS policies, which can't account for device and environmental differences in real time. Our patented multicast traffic technology further enhances high-definition video streaming over Wi-Fi.

Transient client management

In a dense Wi-Fi network, transient clients can degrade the user experience for other connected clients. This problem is typical in train stations, bus terminals and various public hot spot venues where thousands of devices move through an area sending management frames that an AP will hear but without the need to connect. This overwhelms the network with needless traffic and thus slows or makes the Wi-Fi inoperable.

The RUCKUS transient client management capability mitigates this degradation in performance using statistical methods to delay the AP's associations with transient clients. Venue administrators and IT administrators can tune configuration parameters based on typical dwell times and RSSI of the transient clients with accrued heuristics-based techniques that selectively respond to transient clients.

The main benefit of this feature is efficient airtime utilization that maximizes the attention toward connected non-transient clients.

Airtime decongestion

In an ultra-high-density Wi-Fi environment, excessive management frame traffic saturates the available Wi-Fi spectrum, resulting in poor connectivity and low per-client throughput. This ultimately results in a poor client experience. RUCKUS airtime decongestion proprietary techniques limit management frame exchanges between APs and clients in these environments. This allows APs to selectively respond to clients, dramatically increasing overall network efficiency for higher airtime utilization.

Per-packet adaptive transmit power

Access points typically transmit at maximum power to increase coverage and optimize data throughput for distant clients. But this can cause radio interference (co-channel interference) for adjacent APs in the same network. To address this issue, RUCKUS per-packet adaptive power factors in the client proximity (RSSI) and dynamically lowers transmit power levels while maintaining a constant modulation rate (MCS) on a per-packet basis to maximize performance. This results in reduced co-channel interference and higher average throughput per client.

Adaptive Wi-Fi cell sizing

Optimizing Wi-Fi performance is a challenge due to interfering environmental factors from devices to users. At the time of deployment APs are placed for optimal performance, but, as users and the environment change, APs may oversaturate coverage in some spaces, while undersaturating coverage in other locations. CommScope uses periodic co-channel neighbor scans and radio interface estimates to adjust Wi-Fi cell sizes in real time. This technique, in combination with per-packet adaptive transmit power, greatly optimizes performance to each client in under- and over-deployed Wi-Fi networks.

Network capacity utilization

In dense networks, APs suffer uneven client load distribution, leading to low utilization of network capacity. This leads to a sub-optimal client-to-AP link quality, resulting in a lower throughput for the clients. CommScope's solution provides adaptive client management techniques to evenly spread client load across APs and across bands to maintain optimal AP-to-client links in ultra-high-dense environments. This feature employs real-time learning techniques to associate clients to APs with higher link quality and capacity in response to dynamic network loads, resulting in higher overall network capacity and higher per-client throughput.

Problem: Applications

New applications are being rolled out at an unprecedented pace—but not all applications are the same. Some require a significant amount of bandwidth; others not so much. Some are highly dependent upon receiving a high priority for the traffic to provide a high level of user satisfaction. The bottom line is that not all applications are the same. If your Wi-Fi network isn't able to account and adjust for the differing requirements of the applications crossing the network, then users will be unhappy and IT will be frustrated.

CommScope technology

SmartCast® is a sophisticated quality of service (QoS) engine specifically developed to maximize the reliability and performance of delay-sensitive applications, such as IP-based voice and video over 802.11 networks.

Based on patented technology, SmartCast delivers a collection of unique capabilities—such as packet inspection, automatic traffic classification, advanced queuing and scheduling. Unlike any other 802.11 system, RUCKUS SmartCast algorithms automatically schedule and pre-queue traffic in software on a per-client basis. This enables more advanced classification and scheduling that can be applied for each client on a per-traffic class basis. SmartCast is a superset of the IEEE 802.11e/WMM hardware-based queuing standard, ensuring uncompromised performance while remaining standards-compliant.

Application visibility and control

The SmartCast QoS engine inspects each packet and automatically classifies it into one of four queues—voice, video, best effort, and background. SmartCast can inspect a variety of headers, including those of Ethernet frames (both TCP and UDP), VLAN tags, and IPv4 and IPv6 packets.

With per-client queuing, SmartCast is ideal for video and voice over Wi-Fi applications because it ensures disruptive clients don't negatively affect the performance of other clients on the network (no head-of-line blocking). In addition, SmartCast employs sophisticated load balancing and band steering techniques to enable clients to efficiently use the AP and spectrum resources.

Deliver consistently great Wi-Fi

Users and network operators want the same thing: secure, reliable, high-performance Wi-Fi, for every device, every time. However, delivering this is far from easy—but can be accomplished with the right technologies.

CommScope draws on years of innovation in the industry to develop technology that tackles the densest environments, mitigates interference, enables better mobility, secures network access and more. This is why CommScope continually outperforms the competition year after year, especially within the harshest environments. When organizations want to provide their users a Wi-Fi experience that is consistently great, they turn to CommScope.

To learn more, contact your local CommScope account representative or visit www.commscope.com.

About RUCKUS Networks

RUCKUS Networks builds and delivers purpose-driven networks that perform in the demanding environments of the industries we serve. Together with our network of trusted go-to-market partners, we empower our customers to deliver exceptional experiences to the guests, students, residents, citizens and employees who count on them.

CO-114092.3-EN (12/23)