COMMSCOPE®

RUCKUS®
SYSTIMAX®

Best Practice Design Guide

Wired and Wireless Networks for Education
October 2020

Table of Contents

Intended Audience

This document provides an overview of how to configure RUCKUS® products to support K-12 deployments. Outline procedures for configuration and testing are demonstrated. Some knowledge of the RUCKUS Networks equipment and wireless site survey software is recommended.

This document is written for and intended for use by technical engineers with some background in Wi-Fi design and 802.11/wireless engineering principles.

For more information on how to configure CommScope products, please refer to the appropriate CommScope® user guide available on the CommScope support site. https://www.commscope.com/SupportCenter/

Overview

This guide's intent is focused on explaining how to plan for, design, and configure RUCKUS Networks products within the K-12 education environments. The scope of the deployment encompasses a school district office and three types of schools—elementary schools, middle schools, and high schools based on the RUCKUS Unleashed, RUCKUS Cloud, and RUCKUS SmartZone management systems.

It is important to understand that large projects rely on a process that is re-iterative; that is to say that during each part of the process, things may change to support the requirements or to mitigate issues that arise during the process.

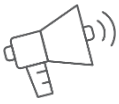
During the planning phase requirements will be defined and any existing infrastructure will be identified. During the design phase these requirements will shape the proposed design for both the wired and wireless networks. Hardware will be selected and locations for installation will be identified. During configuration best practices for additional services will be discussed. During all of these steps, issues may arise that require going back and changing what had already been defined; this is normal and to be expected.

Before the actual design of a K-12 network can start, there are some issues that should be considered. These can dramatically impact the final design, deployment plan and network performance. Items to keep in mind during this process are client counts, the type of network traffic, and the infrastructure type (AP's, controller platforms, management systems) that the administrators are comfortable with. Designing a system that uses the only the latest and greatest hardware and system methodology might be great for locations that have the funding and resources to support this type of network but for others with limited budget and skill sets (think of the janitor being responsible for the network) it's best to recommend something that capability.

Fortunately, with the right Wi-Fi technology and careful planning, most if not all of these problems can be avoided. This document discusses these best practices for planning and deploying networks for K-12.

RUCKUS Top Tips

Throughout the document look for "Top Tips" that summarizes key points for that section. Look for the top tip symbol to read those tips.



RUCKUS TOP TIP!

While this is a Best Practice Design Guide, it is understood that best practices don't always translate to real world scenarios. At times like these it is up to the designer to be able to adapt the best practices to what is presented with the project.

Designing networks as well as maintaining networks is a re-iterative process. As one part of the design changes, go back to ensure that all facets of the requirements are still met. Some designs will require multiple changes to everything, while others won't require any additional rework.

The "Best Practice" is to ensure that the requirements are defined, and the design meets those requirements, no matter how many times adjustments need to be made.

Network Planning

Planning for the network consists of the following steps:

- Investigating network requirements
- Performing site surveys
- Starting to formulate a deployment plan

Investigating Network Requirements

To design a successful network, it is important to learn upfront what the network operators want from the finished network and investigate what the locations are like. You can then create a design that meets those needs within the architectural parameters of the site. Whether you are installing a completely new network or a replacing an existing one, all deployments involve the following initial tasks:

- Define final network expectations
- Define client counts and types
- Identify applications being used
- Determine minimum throughput the network needs to provide

This task is one of the most critical steps in a network design and will also be one of the most critical steps in the process. Everything done after this will point back to the document created to determine if the proposed solution meets these requirements. This is will also prove to be one of the more difficult steps to accomplish.

Final Network Expectations

Conducting a detailed interview session with the primary stakeholders and IT staff is a great place to begin to collect the information needed to meet the school's goals. Getting a good understanding of what is expected from the network when the project is completed allows you to set this as a goal early on and make sure that the system being designed and implemented meets these goals. Questions about the number of student and staff devices, types of devices, and the applications they want to use are some of the things that should be asked in the interview session before any planning takes place. In many cases you are replacing an existing network. Ask questions as to why the network is being replaced.

- Are there problems with the existing network?
- Is the existing network slow or unreliable?
- Is the existing network using older technology and the main goal a network refresh?
- What type of client onboarding is being used if any?
- How will the new network be managed?

Asking questions like these can help determine what the new design will encompass; 802.11ax AP's, Multigig switching, upgrading their WAN connectivity, or IoT. Addressing these types of unknowns upfront and identifying bottlenecks will help ensure the new network will meet expectations and satisfy the goals set in the design session.

Other areas of interest to make sure you are addressing is secure onboarding of clients and how RUCKUS Cloudpath can simplify that process, the emergence of IoT networks and how RUCKUS Networks can support a new IoT network and simplify existing IoT deployments.

RUCKUS TOP TIP!

Understanding the requirements before starting the design is the only way to ensure that the final design meets the customers' requirements at completion of the project.

Client Count and Type

Questions about student and staff device numbers, types and the applications they want to use are some of the things that should be asked in the interview session before any planning takes place. Device numbers has long been a driving force behind network designs, but types of clients can also affect a design. Is the client a laptop or phone, can it do enterprise grade security like 802.1X or is it limited to personal security using Pre-Shared Keys (PSK)?

In a new deployment, all of these numbers will be estimates, and it is a good practice to overestimate the number of clients and underestimate on the type of clients (lean towards older and not as capable as opposed to newer and more capable device types). For an existing network, examine the current usage statistics and use these as part of a conversation of what they see as problems needing solved today and where they see the network in the future. All of these factors will influence the design and configuration as the design progresses.

Applications

The types of applications that expect to be used on a broad scale can help determine the next step, throughput. Will the predominate applications in use stream directly from the internet or from internal resources? What do the administrators see in the future of their network as technology progresses? This is also a good time to discuss with the IT staff around what applications they are wanting to prevent on the network and how to manage that aspect of the network.

Throughput

This will be the final metric that the network gets graded on, and it influenced by the preceding factors. Throughput is often misunderstood, and in some cases gauged solely on running a speed test and looking for the highest number. Conversations with the IT staff to understand, and then determine this figure will give the network designer a benchmark to design to, ensuring that when completed the network meets all the expectations of the network as defined earlier. While getting speed test results of 900 Mbps download and upload is an amazing thing, is it really what the devices need? Managing this expectation from the beginning facilitates honest conversations with the IT staff and executives about what their network really needs to deliver.

Site Surveys

After spending time with the staff to determine what a successful network will look like and how it will operate, investigating what is existing in the space is the next step. To be clear, this step doesn't apply to new construction where nothing exists today. Predictive designs, sometimes referred to as a "predictive survey", happens in the next phase. Site surveys are used to determine what is existing so that a plan can be made to leverage what is existing for the new network and what needs to be replaced. Use this time to determine the actual building topology and identify desired coverage areas and existing wiring closets and cable pathways.

All site surveys should start with good location maps. Getting accurate maps for locations can prove difficult at times, so any advanced warning that can be given to the staff to gather these maps is beneficial. These maps are then used during both the on-site surveys and later in the design phase. Having multiple physical copies and access to electronic copies will enhance the final result.

Site surveys can be broken down into 2 sections, wireless and wired, which are discussed next.

Wireless Surveys

Wireless surveys are useful in identifying any RF issues that exist in the current network, and in locating where the existing AP's are located if they are to be relocated or removed. Professional Wi-Fi software like Ekahau Pro or AirMagnet are invaluable in wireless surveys and are the basis of any wireless design as the project moves forward. Ekahau Pro is the recommended platform as it's the tool of choice by RUCKUS SE's globally.

At this phase of the project, wireless surveys can come in different forms. One commonly referred to survey really isn't a survey at all. The term "predictive survey" is really a misnomer and needs to be stricken from your vocabulary. In the past when someone would use the term predictive survey, they often referred to an exercise that wasn't a survey at all; sitting at a desk and building a model in software that would predict what they thought the new network would look like. Where to place APs in the new network and then provide the ever popular "heat map" that executives are expecting. To be clear, this is not a survey! It is a design based on predictions either assumed or learned from other steps.

While there are other types of "surveys" that can be done the three kinds discussed here are:

- Passive wireless survey
- AP on a Stick (APoS) or "Empirical" survey
- Configuration investigation

Passive Wireless Survey

A passive wireless survey is useful in determining the health of existing Radio Frequency (RF) coverage. This is accomplished using a site survey tool, like Ekahau Pro, and walking the entire facility to measure the RF across the entire spectrum. Results of a passive survey can show configuration miscues like poor channel management (AP's on the same channel) or transmit power on an AP that is either too high or too low. Newer additions to Ekahau Pro can scan for devices that are harmful to Wi-Fi networks, like Bluetooth devices or wireless cameras that can have a negative impact on the network.

Passive surveys are great, but they do have some limitations that make them not as advantageous in some scenarios. Things to consider about a passive survey:

- Passive surveys take time and cost money. Does the project timeline and budget allow for this task?
- What is the information looking to be collected? Is there another way to collect this data?
- Will any information collected be used in the design of a new system?
- Did IT staff indicate any failings in the existing system that would warrant a passive survey before the installation of the new system begins?

Not every project requires or warrants a passive survey of the existing RF space before moving on. This decision needs to be made after discussions with the project team so an informed decision can be made. Sometimes the information looking to be gathered can be done with low cost Wi-Fi scanning tools in a fraction of the time, and cost, of a passive survey.

As a final step in any successful project a validation survey should be conducted. Validation surveys are passive surveys done after final installation to verify to the project team and the stakeholders that the project objectives have been met. Validation surveys are also very useful for any troubleshooting that needs to be done later to show what the system was at final acceptance.

AP on a Stick

An AP on a Stick (APoS) survey is exactly as it sounds. The surveyor uses an AP, usually the same model AP that will be used in the final design, that is mounted on a mast (stick), usually a tripod, and then surveys around the AP, continuing out in a pattern until the signal level is below a threshold that devices can detect. Since not all clients are created equal there isn't a designated signal level to measure to, but a good rule is to try to survey out until an RSSI of -90 dBm is seen. The point where the received signal drops below -90 dBm is known as the "cell edge."

After reaching the edge of the AP cell, the survey information is then "frozen" in the survey application, the AP is then moved to a new location, and the process is repeated. While this is a very valuable type of survey to do, it is also time consuming for the team doing the survey, and costly for the entity footing the bill, and therefore not always completed. The information gathered during a process like this will validate the attenuation values of walls and other obstacles in the structure, giving the designer more information to utilize during the design phase.

Using an APoS survey is just one way to determine attenuation values but there are quicker ways. Using any device to generate a valid 802.11 signal, measure the RSSI value next to a wall in the same room as the device, then move to the other side of the wall and measure the signal seen on the other side. This drop in RSSI number can then be used as the attenuation value for that wall. Repeating this procedure for every wall type is a way to gain insight that can be passed to the designer to be incorporated into the final predictive design.

RUCKUS TOP TIP!

Any survey methodology can be used at any time depending on the requirements of the project. Don't be afraid to mix and match as need to accomplish the end goal.

Configuration Investigation

Part of any wireless survey (passive or APoS) should include investigating the current controllers and their configurations. Documenting SSID's, radio settings, VLAN assignments, and security settings are key to delivering a solution that meets expectations at the end of the project. Doing an investigation of the current configuration can also be done as part of wired surveys that are discussed in the next section.

Different Design Methods

In an attempt to explain the different design methods, the following chart was created for an Ekahau "Wi-Fi Day" showing the differences between different design methods. These focus solely on the work that is done prior to purchasing hardware and the installation of the network. See Figure 1: Wireless Design Methods (Image courtesy of Sam Clements).

If choosing the predictive design method, the cost and effort are significantly less, but it raises the risk that the design chosen for the network won't work. A 100% predictive design based on "best guesses" and assumptions are low effort, which translates to a lower cost for the project, but raises the risk of the design having issues after installation. For an empirical or APoS survey the effort doesn't get much more than this and as such, the financial cost is much more. The advantages of this type of survey is the results are what the results are; it is really hard to argue the results from this type of work. What is measured when placing an actual AP and surveying the surrounding areas is exactly what will be when the fixed AP is installed. The risk of having problems with the final design of the system using this method are low – the designer already knows what the coverage and performance are going to look like because that work was already done.

A mix of these types of designs, known as a hybrid model, makes some assumptions (all classroom walls will be the same) and instead of doing an APoS survey for every classroom, only one classroom is surveyed, and the results extrapolated to the others. This decreases the risk since the information now becomes an "educated guess" without taking the time (and cost) to perform essentially the same survey across a large number of classrooms. This hybrid model is a good cross between the other 2 options by reducing the risk some without greatly increasing the time and cost associated with the design of the network.

Figure 1: Wireless Design Methods (Image courtesy of Sam Clements)

If an APoS survey is not completed, then measurements need to be taken of wall attenuation to assist the designers with the finish product. Every type of wall needs to be measured to ensure that any predictive design is as accurate as possible. In the predictive design process, as much empirical information that is fed into the software reduces the risk of the design, and final installation, being flawed. A good rule of thumb to remember at this stage of the project is “garbage in = garbage out.”

Another option is to do an APoS survey after the predictive design, but before installation, to validate any presumptions in the predictive design. This is helpful in certain areas that have been identified as possible problem areas that the designer wants to verify and then adjust their design from the results. Again, this is a time intensive process that isn’t always in the budget but will reduce the risk that the final solution that is implemented works as expected.

The final active step of any solution should always be a validation survey. This is a passive survey done before final handoff to the network administrators and is done for a couple of reasons:

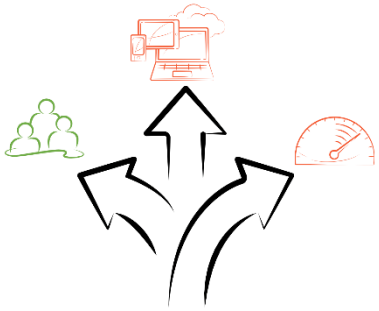
1. Confirm that what was installed matches the predictive design. Coverage holes can show APs that weren’t installed, or APs not functioning due to faulty cabling or cables being plugged into the wrong port on the AP.
2. Results can be used during future troubleshooting steps to look for changes in the system and environment. The survey becomes the “gold standard” to refer to later.

Wired Surveys

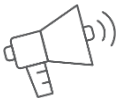
Wired surveys are needed to determine where existing wired locations and switches exist. IDF’s and MDF’s need to be identified, as well as any data centers. It is also critical to identify the types of cabling in place. Is it the latest category of cabling (Cat 6A) or is it old (Cat 3/5) and needs to be replaced to support the defined requirements? Understanding the current wired infrastructure is an important step as it is a critical link in the data chain.

Wired surveys should try to collect the following information:

- Existing VLANs and subnets. It is important that any migration be done in such a way that the new system be deployed in a different VLAN from the old system. This is to avoid any potential conflict that may arise between them.
- Existing routes. Existing routes or routing information must be clearly identified and documented so that security risks can be assessed. It is important that infrastructure systems and devices cannot be accessed and compromised by unauthorized users.
- Existing restrictions, access lists and traffic rules. Existing ACLs, permissions and traffic rules should also be clearly identified and documented to assess security risks and also to ascertain there is no interference to proper functioning of the new wireless network.
- Multicast and broadcast traffic in the network. Due to the way multicast and broadcast traffic is transmitted over wireless, the presence of large amount of multicast and or broadcast traffic is bad for Wi-Fi. To audit this, simply use a laptop running a packet capture and connect to the core switch with a mirror port (for capturing multiple VLANs) or access port on the VLAN of interest to capture about 30 minutes or more of traffic and analyze the traffic looking for suspicious devices generating a large amount of multicast or broadcast traffic.
- Quality of cabling and patch panel connections. This may be basic but in education environments, many properties have old infrastructure that are of poor quality. Some have cabling exceeding 100 meters and do not have a full site cable test report.
- Types of Ethernet switches (make, model, performance).
- For wireless networks to be secure and effective, only managed switches that support 802.1q VLAN should be used. Unmanaged switches should not be used.



- Power over Ethernet (PoE) switches should also be used as far as possible. PoE switches are used to power access points, cameras, sensors, and other wired devices directly. Avoid using unmanaged PoE injectors or DC power supply. Using PoE switches have the advantage of being able to remotely power cycle access points without the need for physical access to the access point.
- Heat dissipation will also be a consideration when using such switches. Many locations are not well ventilated and cannot dissipate heat coming from the switches, causing the switches to operate at or exceeding their temperature limit. This will lead to early failures and network downtime.



RUCKUS TOP TIP!

If the wired infrastructure, switches and cables, can't support the wireless network, it will first present as a wireless problem. Make sure just as much effort is put into the wired network as the wireless network.

Power over Ethernet

Power over Ethernet, or PoE, is a subject that is quickly becoming something that can no longer be taken for granted. More devices are now relying on PoE and the demands on the switch to deliver even more power is something that needs to be considered.

Terms to be familiar with to better understand PoE are:

- PSE – Power Sourcing Equipment. The device that provides power to the device. Can be a PoE switch (recommended) or a separate device inline between the switch and the device (not recommended).
- PD – Powered Device. Any device that requires PoE.

The Institute of Electrical and Electronics Engineers (IEEE) is the governing body that sets the standards for most current networking protocols, to include wired (802.3) and wireless (802.11). PoE is covered under 802.3 and as of this document, there are three standards defined for PoE, although there are other vendor proprietary enhancements available.

Power budgets have to be considered when deploying access points and other devices which may require power. 802.11ac access points from most vendors will require 802.3at (or PoE+) power supplied to the device. However, they may work with 802.3af but with reduced features. Newer access points, like Wi-Fi 6 (802.11ax) or Wi-Fi 6E (6 GHz) with additional IoT radios will require more than 30 watts of power, necessitating a switch that can provide 802.3bt or Power over HDBaseT (PoH) power.

ICX switches support a proprietary enhancement to the PoE standard known as PoE+ Overdrive. This enhancement allows devices to request higher amounts or power above the 802.3at (30 W) by way of LLDP. This ability requires the ICX switch hardware to be robust enough to handle the extra current, temperature, and overall stress of supporting up to 45W over the same 2-Pairs—this is a RUCKUS differentiator. See Table 1: PoE Standards and Alternatives on RUCKUS ICX Switches for more details.

PoE Class/Name	**802.3af PoE**				**802.3at PoE+**	**PoE+ RUCKUS Overdrive**	**802.3bt PoE++**				**HDBaseT RUCKUS PoH**
PoE Type	Type 1				Type 2	-	Type 3		Type 4		-
Class	0	1	2	3	4	-	5	6	7	8	-
PSE Watt	15.4	4	7	15.4	30	45	45	60	75	90	95
PD Watt	12.95	3.84	6.49	13	25.5	-	40	52	62	71	-
Minimum Cable Reqd	Cat5				Cat5e		Cat6				
Number of wire pairs	2 Pairs						4 Pairs				

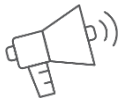
Table 1: PoE Standards and Alternatives on RUCKUS ICX Switches

Note: The Power Sourcing Equipment (PSE) numbers are the maximum output power as measured at the RJ45 connector of the PSE device.

The Powered Device (PD) numbers are the worst-case maximum power delivered to the PD, assuming 100M of Cat5/5e/6 wiring between the PSE and PD.

RUCKUS ICX switches use LLDP and a series of events to detect and then classify the devices attached to a switch. This classification then determines how much power to allow the device to draw from the switch.

PoE and PoE capabilities must be examined when deploying more access points and other PoE devices to a switch. The PoE switch must have sufficient power budget to power all the PD connected to it as well as for the switch operation. A power budget is the maximum required power that is required across all the devices compared to the maximum available power on the switch. Some vendors may over subscribe their PoE, e.g. a switch with 24 ports of 802.3at power (24 ports x 30 watts per port = 720 watts) may only have a maximum power budget of 370 watts, or enough for 12 ports of 802.3at power. Finding these switches during the survey will avoid problems during the deployment phase. For a more in-depth review of PoE and PoE budgets on a RUCKUS ICX switch, please see the section on ICX Settings and the end of this document.



RUCKUS TOP TIP!

Planning for future PoE needs as well as switch capacity is critical. Wired infrastructure is upgraded less frequently than Wi-Fi hardware. Many times, lack of capacity on the wired infrastructure (cable plant and switching hardware) will present as wireless problems in the future.

Deployment Planning

While onsite, plans can start to formulate about what deployment will look like. Ask about items that can become obstacles later on. These can include, but not limited to:

- Established network change freezes
- Configuration planning
- Equipment staging locations
- Installer access to the locations
- Physical limitations for AP mounting

Network Change Freezes

Many organizations have established times where network changes are not allowed to happen. Planning around these periods will ensure the timeline and budgets aren't impacted. Identifying these times ahead of time are crucial to the overall plan on any project.

Configuration Planning

Knowing if an organization has a preferred way of configuring their hardware, and then how they manage it. If they have a dedicated Network Operations Center (NOC) or is it the janitor between lunches? Do they require all of the traffic be tunneled to a specific point, therefore requiring a SmartZone-Dataplane or is using Local Break Out (LBO) acceptable? Defining who will manage the system, and how they will manage the system, after project completion will allow the designers to deliver a system that meets these requirements.

Equipment Staging

Some projects won't have a secure location to stage the equipment onsite, necessitating the installers to stage and store the equipment at a different location before beginning the deployment phase. If the project has a location to stage and store the equipment, determine who has access to this location and how the installers will gain access. Many projects have gone over time thanks to the one person with the key to the room with the equipment going on vacation and taking the key with them.

Installer Access

Many facilities have guidelines around visitors and contractors and how they access the facility. Talk with the stakeholders during the initial site survey to better understand what needs to happen so when the team arrives on Day 1 of deployment they aren't delayed. With physical and on-site security taking center stage, especially in the education field, ironing out these questions early on can prevent problems and incidents during the later stages of the project.

Access Point Mounting

While exact locations of where the AP's will be mounted may not be known, paying attention to existing infrastructure and noting different limitations can facilitate the design process and limit changes later on. Is there an area with drop ceilings in only part of the room but not others? Is there a ceiling there at all or an open ceiling plan? If the facility is still in the planning phases, contact the architects and work closely with them on questions like this.

All of these questions, when discussed early on in the project, will save time and money in the long run, making for a smoother project and a final network that functions like a well-oiled machine.

Wireless Network Design

The network design phase is when everything that has been defined and discovered in the previous steps are put into a comprehensive design that can be modified quickly and easily to meet the end requirements and expectations before installation commences. The network design phase is where all the decisions are made around hardware and services needed to support the requirements gathered earlier, as well as a design that will fit into any architectural limitations previously identified. This phase is where the majority of time will be spent as it is the bridge between the "wants" and the delivered solution. This design section is broken down into four key sections that will be covered in depth:

- Radio Spectrum Capacity
- Wireless Network Design
- Additional Network Requirements
- Wired Network Design

Radio Spectrum Capacity

Before any "heatmaps" can be generated to show to executives, it's important to understand the real limiting factor in any wireless design. In the past, the Access Points themselves had limiting factors based on the hardware that was inside the AP. Processors and radios that came in older APs may have limited the capabilities of the APs, but not any longer.

Modern AP's with modern processors and radio chipsets have followed Moore's Law (that the speed and capabilities of computers can expect to double every two years) like the rest of technology, and have improved vastly over the past several years. The AP is no longer the limiting factor in the wireless design process. Every manufacturer will brag that their AP will now support at least 1,024 clients, or even more. Most people know

that this is an absurd number and that planning for that many clients per AP is a bad idea. What designers are beginning to understand better is that now the limiting factor of capacity rests in the radio spectrum, not the hardware. Talking about Wi-Fi design without touching on the radio spectrum would be foolish.

Understanding the Spectrum

All wireless services, Wi-Fi and others, are classified by what part of the wireless spectrum they fall into. How and why that happens is beyond the scope of this document, but just trust that for Wi-Fi they currently fall into the bands known as 2.4 and 5 GHz. In a truly recent development, Wi-Fi 6E will introduce the 6 GHz band as well. For this discussion, we will focus on what is currently available.

All bands of radio spectrum are separated into channels, and for Wi-Fi, the standard channel is 20 MHz wide. This width on the channel defines a lot of how Wi-Fi works, and understanding how those 20 MHz wide channels fit together and function can greatly enhance any design.

One of the biggest considerations is the negative impact of co-channel and adjacent-channel interference. Co-Channel Interference (CCI) will occur if channels are reused at close distances and with very little attenuation of the signal strength between them. The 802.11 protocol is designed to handle such a scenario, but the tradeoff is reduced performance since airtime will be shared between these "cells". To prevent two devices from transmitting at the same time, any Wi-Fi device that hears another device talking on its channel must wait until the medium is available. This means that, effectively, two APs transmitting on the same channel that can hear each other will act like one AP. You will have two APs, but only one Wi-Fi device can transmit at a time. All others will be forced to wait. RUCKUS SmartZoneOS 5 introduced a new feature called Auto Cell Sizing, which automatically adjusts radio settings in co-channel APs to minimize the impact of CCI. Another RUCKUS feature that assists with this is the BeamFlex+ technology built into every RUCKUS AP. BeamFlex+ focuses the RF towards a specific client, limiting the RF being transmitted towards other APs.

Both of these innovations help with minimizing CCI but aren't a substitute for a well-designed network. Think of them as a helpful tool to have for areas of the design that prove to be problematic.

Adjacent Channel Interference (ACI) can also impact the performance of close-spaced (several feet) clients transmitting on adjacent channels. Even though the channels are considered non-overlapping, some impact can still occur if the devices are close enough. Access Points mounted too closely and operating on different channels on same band may also have a measurable performance penalty during concurrent operation. One way to visualize this is to think of a conversation between two people (person A talking to person B). They are each using a megaphone to talk to the other. They can hear each other fine both at close range and at a distance. But consider what happens if we add a third individual (person C) standing nearby to and using a megaphone to transmit to a fourth (person D). Even though person C is speaking to someone else entirely, they are so close to person A that person A can't understand what it is hearing from its client, person B. Effectively, the APs are so loud they are making each other deaf when they transmit regardless that they are using "non-overlapping" channels.

Deployments that require smooth roaming between APs will need an overlap between cells. Many documents will refer to a “percentage of overlap” between cells but calculating this overlap is almost a mathematical impossibility. Since the size and shape of the cell coverage changes infinitely, calculating this number becomes an exercise in futility. A better way to design coverage is by looking at primary and secondary signal strengths at any given location in the plan. Clients should always see at least two APs at an RSSI better than -75 dBm at any location for good roaming to occur.

When we refer to cell overlap, in this case, we are not referring APs on the same channel. Preferably, they are on different channels. They do need to be close enough that a client can hear both, so the overlap is in physical distance rather than spectrum overlap. In cases where the APs overlap both in distance and channel (CCI), a target of 15-20dB (or more) separation is recommended between each AP.

In K-12 networks many times an AP is in every classroom and in many cases 80 MHz channels are used in 5Ghz to increase capacity and speed for the classroom. This practice is not necessarily wrong depending on the density of clients and the layout of the school in question. If the building has a smaller number of classrooms and less students 80 MHz channels could be a possibility. In the case of a larger building with dense classroom grouping and higher client density the suggested channel width is 40Mhz. A good rule to follow when selecting channel widths during the design phase is to use larger channel widths, until you can’t. Try 80 MHz wide channels until the CCI becomes an issue, then back off to 40 MHz wide channels. If 40 MHz wide channels still cause too much CCI, then back off to 20 MHz wide channels

Since the world is a large place, not all spectrum is managed the same, not all of these rules will apply to everyone. The concepts are the same, but some of the numbers will change. Ensure that the proper regulatory rules are followed for the location the network is going to be installed.

2.4 GHz Channels

The spectrum allocated for 2.4 GHz is less than 5 GHz, no matter what channel plan is in place for your regulatory domain. The other universal truth is the channel assignments in the 2.4 GHz band was done wrong. What is meant by that can be answered in looking at the 5 GHz channel plan. The channels in 2.4 GHz are defined sequentially – 1, 2, 3, 4, etc. while the 5 GHz channels are spaced out – 36, 40, 44, 48, etc. The sequential channels in 2.4 GHz allow the hardware to assign channels that overlap each other. Channel numbers are 5 MHz apart, but the channels are 20 MHz wide. You don’t need to know what a MHz or Hz is to know that 20 is more than 5. Channels work best when they don’t have to share the spectrum with another channel. This phenomenon is known as ACI and was discussed in the previous section.

2.4Ghz should always be set to 20 MHz as there is not enough channel separation to allow for channel bonding (channel bonding was introduced with 802.11n.) Depending on your regulatory domain, there are either 3 or 4 non-overlapping channel options at 2.4 GHz, the graphic below gives an example of this configuration. Using any other methodology will result in either CCI or ACI and will impact the network. The amount of impact depends on any number of variables, but there will be some impact.

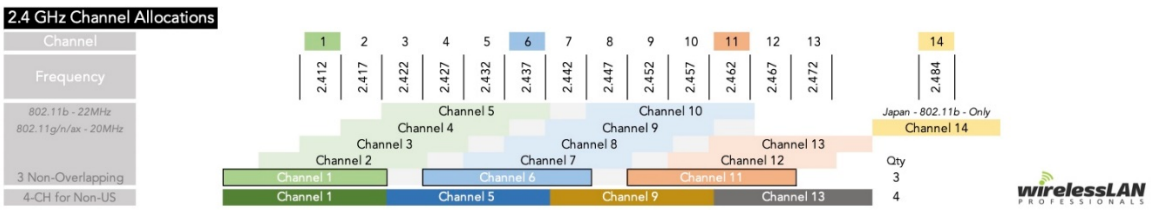


Figure 2: Channel Allocations for 2.4 GHz (Courtesy Wireless LAN Professionals)

5 GHz Channels

For 5 GHz, there are a maximum of 24 non-overlapping 20 MHz-wide channels, plus channel 144 which can be used in some cases i.e. if AP and client devices support it. Theoretically, you could have a deployment with 24 APs with no overlapping channels, 25 if the clients support channel 165. As the channel width increases, the number of non-overlapping channels goes down. With 40 MHz wide channel bandwidth, there are 12 non-overlapping channels. At 80 MHz-wide channel width, which yield the higher 802.11ac data rates, the number of non-overlapping channels is drastically reduced from 24 to 6. Due to 160 MHz channel widths (available with 802.11ac "Phase 2" devices) only offering 2 non-overlapping channels, this is never recommended as a best practice.

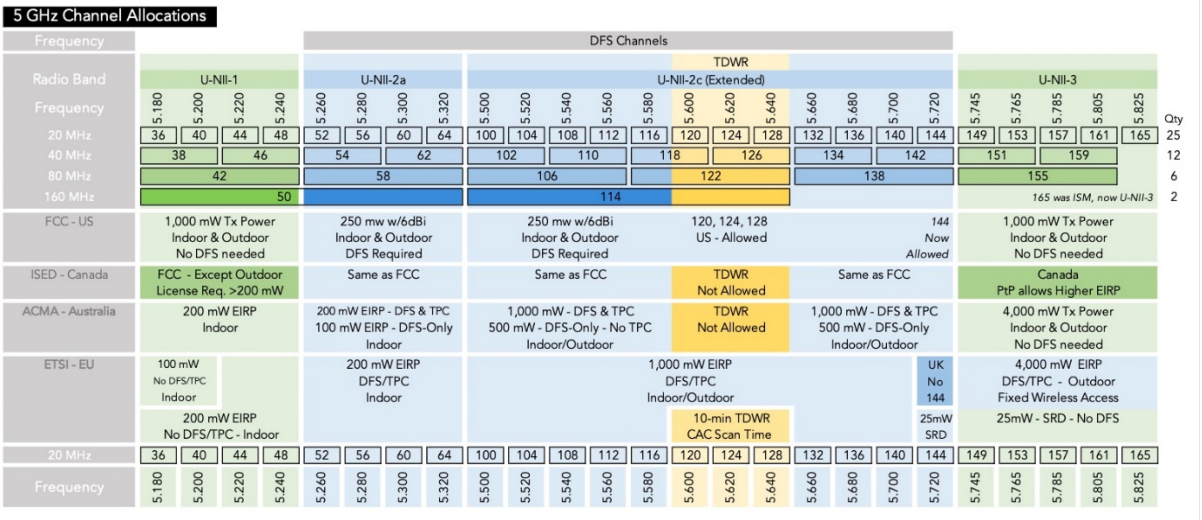
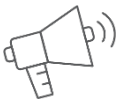


Figure 3: Channel Allocations for 5 GHz (Courtesy Wireless LAN Professionals)



RUCKUS TOP TIP!

With the advancements in AP and switch capabilities, the Radio Frequency (RF) spectrum is now the chokepoint. A well design wired backhaul with Multi-Gig connections from the AP to the switch and from the switch to the rest of the network, airtime on the RF channel is now the new chokepoint. Understanding how the RF affects overall performance will lead to a stable network that stands the test of time.

The biggest source of interference to a Wi-Fi channel is other Wi-Fi, not other possible sources of interference.

Wireless Design

Wireless network designs are done using professional Wi-Fi software such as Ekahau Pro (referenced here as it is the standard that the RUCKUS SE's utilize) and takes all of the defined requirements into consideration when planning a network. Wireless network designs are based on the following and need to be identified and defined before proceeding. While this step can change, it is best to have the requirements defined so designers know what the expectations are, and if modified during the process, the designers have a guide to fall back on. Things that need to be identified and defined before a predictive plan can commence are:

- Defined coverage/capacity zones (basic connectivity, high speed connectivity, high capacity zones)
- Access Point Selection
- Controller Selection

The goal of this section isn't to explain how to use the tools available, but things to be used as a best practice within the tool used to design the network.

Defining Coverage Zones

This part of the process is seemingly an easy step, but experience tells a difference story. A coverage zone is where the staff is asked to identify exactly what is expected from the network at every location across the campus. For schools, this generally falls into 3 categories:

- Classroom
- High Density
- Basic connectivity

Along with the number of devices that may be present in each category, the type of device as well as what the user will be trying to accomplish in these locations need to be considered. During the design phase there could be multiple of each type of coverage areas and getting these defined correctly in the planning software will help identify locations that don't meet the defined criteria early on. The number of SSID's and security types will be discussed in a later section, coverage zones are focused on the capacity of the channels, which is the real limiting factor in a Wi-Fi system as discussed previously.

Utilizing Zones in the Planner Tool

Wi-Fi planning tools have the capability to assist the designer during this stage, if the feature is used correctly. Identify these zones within the tool and taking the time to define the requirements for each zone, will ensure that the final design meets all the requirements defined during the previous steps.

Classrooms

Classrooms are predictable, and some of the easiest areas to define and design for. The number and type of devices are well known, and the needs for the types of applications and throughput can be defined. For K-12 environments, most designs start at the classroom and work out from there.

High Density

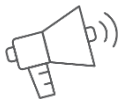
High density areas are locations where less control over the device types and types of applications being used is possible. Areas that fit the high-density classification include cafeterias, auditoriums, gymnasiums, and multi-purpose areas (spaces used for everything previously noted.) In high density areas, a premium is put on getting connectivity and a minimum throughput level, but generally not to the same level as classrooms.

Basic Connectivity

Basic connectivity can best be described as outdoor areas. In the past stakeholders usually refer to these areas as “nice to have, but not a requirement” but in a COVID-19 world this has changed. Areas that used to be considered *nice to have* are now the only areas users are allowed to be. Open air spaces where users can be spaced out have become the normal while still needing to maintain traditional coverage areas like classrooms, cafeterias, and auditoriums for when users are moved back inside. The design principal for these outdoor areas remains the same, the biggest change is in the criticality of these spaces and the concept that the far reaches of these outdoor areas weren’t as important. Now, every corner of every parking is lot critical to provide coverage whereas before just the areas near a building would work OK.

Traditionally the time and budget hasn’t been normally allocated to nice to have areas but the year 2020 has changed a lot of things from *what was* to *what is* and outdoor Wi-Fi is now taking the forefront in requirements. By using correct coverage requirements for an outdoor zone like a parking lot or stadium, designers can select APs like the T710S, T610S, or T310S and utilize the sector antenna pattern to focus the coverage in certain areas. APs like the T750 and T710 can be used where an omni-directional pattern is advantageous. While placing the AP can appear easy, the challenge comes when trying to connect these APs back into the infrastructure. The challenges like this the RUCKUS P300 Point-to-Point/MultiPoint (P2P/P2mP) can be utilized to provide network connectivity/backhaul in locations where running fiber to each AP isn’t possible.

Time spent in these areas can appear to be a waste during the design phase, but it is time well spent. Don’t breeze past areas like this, it can prove to be a long-term problem resulting in multiple call backs after the project is completed.



RUCKUS TOP TIP!

Defining the proper zone requirements before starting to place APs is critical to ensure the completed design has the best chance to meet the requirements once the system is installed.

Understand that over time, the requirements of the network will change. It is expected that as the needs of the change the network requirements will need to be adjusted to match. Static networks that met the needs previously might not always meet the needs of today. Think of networks not as a static piece of hardware but as living organism that needs care and feeding over time, and make the needed adjustments as they come up, don’t wait for total system failure to make the needed adjustments.

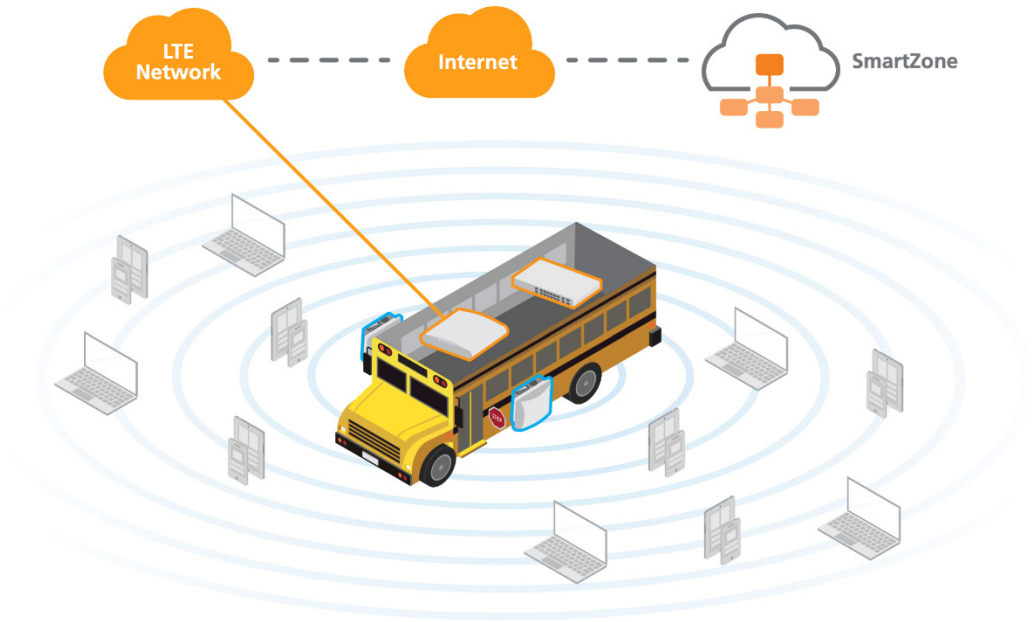
School Bus Wi-Fi

Along with outdoor Wi-Fi, Wi-Fi in school busses have sprung to prominence in a surprising way. When students stopped needing busses to transport them to the school, districts started to repurpose these idle resources as a way to bring the school to the student. Many students found remote learning difficult due to the lack of access to quality broadband internet connection, known as the "digital divide" which has led to something known as the "homework gap." The lack of access to high speed internet leading to challenges with homework has forced school districts to think outside the box to solve this challenge in many communities across the globe.

In response, some school districts have adopted innovative solutions to extend the reach of the classroom. By repurposing some of the estimated 480,000 idle school buses across the United states alone, districts are creating Wi-Fi hotspots in under-privilege communities so that their students can get online. In addition to helping students keep pace with the digital transformation, Wi-Fi-enabled buses can also deliver meals and other services formerly provided by the schools. With pilot programs across the country getting rave reviews, the trend is growing and helping kids in need to bridging the digital divide.

CommScope has developed a simple and reliable connectivity kit to help educators address the technical challenges of deploying school bus Wi-Fi. The kit includes CommScope RUCKUS indoor and outdoor APs (M510, T310 or T610), a PoE-enabled ICX switch (7150-C08 or 7150-C12) and the hardware needed to mount the APs on the buses' exterior. The RUCKUS M510 utilizes its cellular backhaul capability to connect the bus to the internet while the ICX switch provides connectivity from the T310 or T610 hung on the side of the bus to the M510 acting as the gateway. The CommScope RUCKUS connectivity kit is being implemented in several pilot programs for school districts in northern California. With the support of CommScope engineers, the school districts will be able to provide safe and reliable, high-speed broadband access to students and families who do not have the means to get broadband connection at home.

For more information on the School Bus Connectivity kit use the following link
https://www.commscope.com/globalassets/digizuite/494410-the-connected-school-bus-wifi-solution-brief-co-114565-en.pdf



Access Point Selection

During a wireless network design, selecting the models of APs to be used needs to be decided before starting the task of placing an AP on a map and generating the infamous heat maps that thee executives expect to see. Different APs will have different antenna patterns and when placed into a planning tool with the proper attenuation artifacts built in (like walls and other attenuating items) can give an accurate expectation of what can be expected from the wireless system once installed.

RUCKUS offers a broad choice of indoor and outdoor access points that work well in any environment. RUCKUS APs can be broken down by the letter that precedes the model type. See Table 2: RUCKUS AP Designators for a complete breakdown.

Letter Designation	Use Case
C	Indoor Access Point, Wall Mount, with Cable Model
H	Indoor Access Point, Wall Mount
M	Indoor Access Point, Mobile with LTE backhaul
R	Indoor Access Point, Ceiling Mount
E	Outdoor Access Point, External BeamFlex+ Antennas*
P	Outdoor Point to Point/Multipoint Bridge, Internal Antennas
T	Outdoor Access Point, Omni or Directional with BeamFlex+

Table 2: RUCKUS AP Designators

Most of these AP models can be utilized in multiple controller scenarios (Unleashed, RUCKUS Cloud, SmartZone) and the controller methodology be changed as the requirements change, e.g. when first deployed the staff chose to utilize Unleashed APs but as requirements change, they decide to move to RUCKUS Cloud. Controller products can be changed without the need to change out the AP hardware, a RUCKUS differentiator. Controller

types will be covered more in depth later in this document. When trying to decide with AP to use, know that RUCKUS excels by bringing the advantage of BeamFlex+ technology with nearly every AP.

Wi-Fi 6 vs Wi-Fi 5

No conversation these days can be had about APs without discussing Wi-Fi 6 at some point. Wi-Fi 6, or 802.11ax, is the latest amendment from the IEEE aimed at "High Efficiency" Wi-Fi (the IEEE full name is 802.11ax HE). Along with this high efficiency comes an increase in speed and modulation rates. See Table 3: Wi-Fi 5 vs Wi-Fi 6 for a comparison between some of the specifications in Wi-Fi 5 and Wi-Fi 6 APs.

Wi-Fi Version	IEEE	QAM	Spatial Streams	Top Theoretical Speed	MCS Index	Modulation Type
Wi-Fi 4	802.11n	64 QAM	3	1.950 Gbps	MCS 0-23	OFDM
Wi-Fi 5	802.11ac	256 QAM	3	2.340 Gbps	MCS 0-9	OFDM
Wi-Fi 6	802.11ax	1024 QAM	8	4.083 Gbps	MCS 0-11	OFDMA

Table 3: Wi-Fi 5 vs Wi-Fi 6

By reviewing the table, it is easy to see the increase in speed as the versions have evolved over time. As the Quadrature Amplitude Modulation (QAM) increased from 64 QAM to 256 QAM, and Spatial Streams increased from 3 to 8, the top speed increased as well. As a reminder, this theoretical maximum speed is just that, theoretical. There are many factors involved in achieving that top speed, and even then, that is simply the maximum connection speed a device can achieve, actual throughput will be less than that thanks to the overhead that is incumbent in Wi-Fi.

The biggest change in the evolution from Wi-Fi 4 to Wi-Fi 6 is the "Modulation Type" in the far-right column. Ever since the days of 802.11a and 11g, Wi-Fi has used Orthogonal Frequency-Division Multiplexing (OFDM) for encoding the data on the chosen frequency (or channel). With Wi-Fi 6 this changed to Orthogonal Frequency-Division Multiple Access (OFDMA). The reason for this advancement can be found in the explanation of why Wi-Fi devices will never achieve that mythical top speed – the management overhead.

The majority of traffic on a Wi-Fi network is actually management and coordination between all of the devices (called stations or "STA") on a Wi-Fi channel, regardless of the SSID or whoever owns the AP on that channel. The majority of this coordination and management overhead is very small, around 300 bytes per frame (this is the official name of a packet that is sent over Wi-Fi), not the maximum set by the Maximum Transmission Unit (MTU), usually 1,500 bytes. With the average frame size of 300 bytes, most of the traffic on a channel at any given time isn't transmitted faster than 0.024 Gbps (or 24 Mbps) which isn't even a decent load on a network from 15 years ago!

OFDMA was introduced to Wi-Fi as a new technology but in fact it was "borrowed" from cellular LTE networks. LTE was a leap forward in the speed of cellular networks thanks to this increase in efficiency; the key being the Multiple Access part of OFDMA. If 24 Mbps is plenty for the overhead, and that can be achieved using less than the full, 20 MHz wide channel, why not combine multiple users looking to pass just a little bit of data into the same channel at the same time, but in their own smaller 2 MHz wide "channel" called a "Resource Unit". This frees up time on the channel for devices that really need the 140 Mbps available to a two spatial stream device on a 20 MHz wide channel.

With the AP in control of scheduling these “allocations”, up to 9 devices could send or receive at the same time using these Resource Units. With 9 devices getting their data at one time, instead of receiving the data in sequential order, much more time on the channel can be dedicated to the devices needing more throughput. More time on the channel means sending and receiving data faster. It might not be encoded at a faster rate, but thanks to the increased efficiency of the available channel, you get your data faster.

Which APs to Purchase?

When it comes time to select an AP model, or multiple models, to include into a design, there isn’t an easy answer. Wi-Fi 5 vs Wi-Fi 6, 2x2:2 vs 3x3:3 vs 4x4:4 vs 8x8:8, dual band vs tri-band vs quad band (future APs to support 6 GHz Wi-Fi 6E), indoor vs outdoor, there is no shortage of models to pick from, and to be overwhelmed by. No guide can ever ascertain which specific model of AP to select for any given scenario since they are all unique to the network in question. That being said there are some general rules to follow to help guide the selection of which AP to use.

- Refresh Cycle – Some organizations need to rely on their hardware for up to 7 years so consider purchasing hardware that will still be supported in 7 years. If an organization has the budget to refresh every 3 years this isn’t as big of a concern.
- Future Proofing – Installing the latest hardware ensures that the network will be ready for the newer clients when they are released. This also ties into the refresh cycle.
- Risk Aversion – Newer hardware comes with inherent risk as vendors work out the bugs with the new code to support the new hardware. Some organizations try to avoid this risk, so they opt for a more proven solution, which runs counter to the first 2 items.
- Client base – Not all clients are capable of 4x4:4 or of using the 6 GHz spectrum. Also, not all clients are ever going to need 800 Mbps offered by wider channels. Understanding the clients that will be used is crucial in selecting AP model types.
- New Features – Newer APs will have the newer features supported for longer than older APs.
- Requirements of the coverage area – Will the area in question have hundreds of clients or just a couple? Selecting APs designed for high-density for a small conference room can be a waste or selecting APs designed for a small conference room in a high-density area can result in a crippled network.

The last consideration when selecting an AP is Wi-Fi 5 vs Wi-Fi 6. RUCKUS has a proven track record with both technologies and selecting one over the other isn’t an easy decision. The final piece of advice when selecting a newer model of AP vs an older model AP, like the R750 vs the R720, comes down to a feature or specification that isn’t found on any specification sheet.

Newer APs come with newer silicon inside the AP. Faster and better processors mean that even in an environment of all Wi-Fi 5 clients, deploying Wi-Fi 6 or 802.11ax APs means better performance for the older clients. Better performance for all clients, “future proofed” networks for when Wi-Fi 6 clients do appear on the network, longer life span of installed hardware resulting in a longer refresh cycle. The upside to installing the latest generation of APs is numerous while every day the risk to installing the latest version diminishes. Organizations can also feel comfortable installing Wi-Fi 6 APs today as the next generation of APs, the yet to be

released Wi-Fi 6E, will also use the 802.11ax protocol. When needed organizations can simply deploy the next generation of AP with the additional spectrum availability where extra spectrum is needed and when client devices start to appear on the market.

RUCKUS TOP TIP!

To ensure getting the most out of an AP mounted in the ceiling, elect for Wi-Fi 6 APs. They will have the most features updated in the future.

Indoor Access Points

With a multitude of indoor APs, designers can select from a number of APs to meet the requirements defined earlier. From ceiling mount to wall mount, the indoor AP line offered means that the proper AP can be selected no matter the requirements needed for the space.

Figure 4: RUCKUS R610

Outdoor Access Points

With outdoor deployments, AP mounting locations can be few and far between, reducing the capacity in areas that usually need them the most. The saving grace in areas like this can be found in the type of device being used in these areas. Mobile devices like phones and tablets prevail, and users aren't looking to use heavy bandwidth applications. These lower powered devices (to preserve battery life) with less capability (1 spatial stream compared to 3 spatial streams) assist the designer if this is defined in the planning tool.

In most scenarios, designers turn to external antennas to focus the RF signal from a single point to the area being covered, like from a building out into a parking lot. External antennas do have their advantages but also add extra cost to a project not only in extra hardware but also the extra time to mount the antenna as well as the AP. Using APs like the RUCKUS T310S and the T610S allow for this directivity while keeping the ease of installation of an AP with internal antennas. Removing the extra hardware also removes additional points of failure, not only from physical damage but also from weather intrusion, like moisture getting into an RF connector.

Access Point Locations

Once a designer has the requirements defined within the planning a tool and a selection of APs to be utilized, the rest of the design process is pretty straightforward. Select the AP, place it on the map, and then watch the resulting coverage. Placing APs can be done in any order, but most prefer to start with the most critical areas first and move out to the other areas to ensure that the design meets the most criteria set as possible. Care needs to be taken to avoid areas noticed during the site walk done in previous steps as locations where mounting isn't possible, or where wired backhaul or power could become an issue.

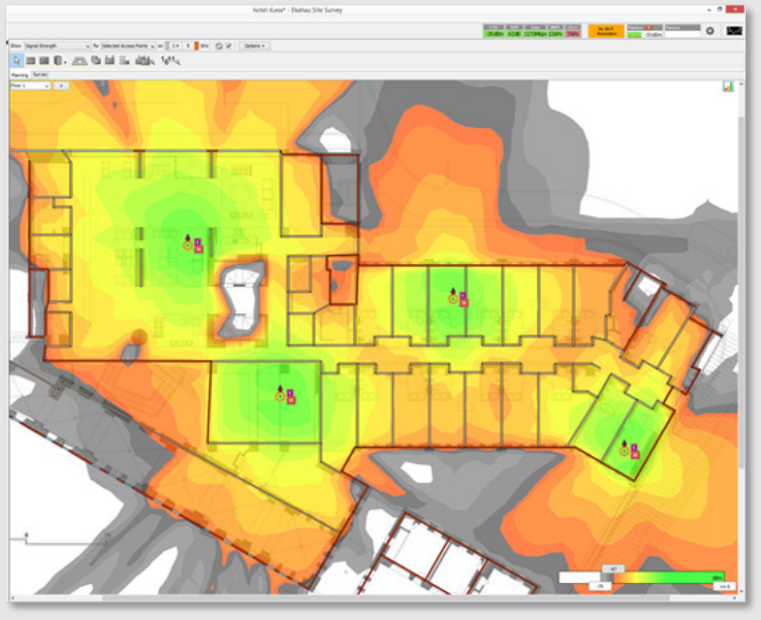


Figure 5: Ekahau Predictive Design (image: Ekahau.com)

Another consideration is indoor locations are not limited by using indoor APs only. Certain areas may call for sectorized antennas with special RF coverage patterns that are only offered by “outdoor” APs. Gymnasiums, auditoriums, mechanical spaces, and other areas that may have unique challenges that could benefit from these APs being used even though technically, the spaces are indoors.

Conversely, the opposite does not hold true. Indoor rated APs are generally not a good fit for outdoor locations due to weather and moisture concerns related these outdoor locations. If an indoor rated AP is selected to be utilized outdoors for a special feature (needing the additional Ethernet ports featured on an H510 AP) consideration needs to be taken to protect the AP from the outdoor environment by utilizing outdoor rated enclosures that can not only protect from the elements but also from possible vandalism of theft.

Controller Selection

Controller selection can be an issue with some vendors but with the flexible selection offered by the RUCKUS lineup of APs, it isn’t as big of a concern. Where it does come into consideration is the wired network design, so covering this before getting to that step is prudent.

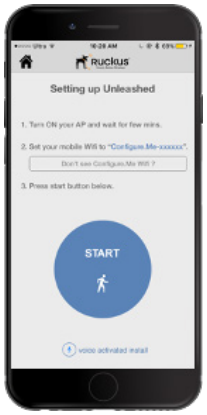
RUCKUS offers a multitude of controller options but for this document the focus will be on the following:

- RUCKUS Unleashed
- RUCKUS Cloud
- RUCKUS SmartZone

Each option offers both advantages and limitations that need to be considered for each deployment location and administrator experience and expertise. From a positive, as mentioned earlier, most of the APs can be managed by any of the controller options, giving the designer flexibility not seen in many other vendors.

RUCKUS Unleashed

RUCKUS Unleashed is the concept that the network won't have a controller from the traditional sense. In an Unleashed deployment, the first AP configured will act as the "Master AP" and as additional APs are brought online, they will join the existing AP and inherit the configurations from that device, as well as future updates. Allowing administrators to manage the system and receive alerts on their mobile device, gone are the days of needing to sit in front of a computer to know when problems arise. Being able to move about the campus and still monitor the network acts as force multiplier for staff who wear multiple hats. RUCKUS Unleashed can support up to 128 APs and 2,048 clients per network (more with Unleashed Multi-Site Manager) and up to 8 ICX switches.



RUCKUS Cloud

RUCKUS Cloud is an industry leader in the Cloud controller market. RUCKUS Cloud offers the benefit of running a full featured platform but for locations that have a "Lean IT Staff." Offered as a subscription model, RUCKUS Cloud allows the IT staff to focus on what is important to them, managing the wireless network and clients, while shifting the burden of traditional controller maintenance to a dedicated team focused on doing just that. With 24 x 7 support and an "always up" mindset that comes with cloud deployments, this solution offers the best of both worlds. RUCKUS Cloud can also manage ICX switches for a single control plane for both wireless and wired. With unlimited scalability, there is never a concern of outgrowing your management platform.

RUCKUS SmartZone

RUCKUS SmartZone is the full-blown controller that large organizations often think of. Offered as a physical device that can be located in a data center or a virtual instance on either private or public cloud, the options can be flexed to match what any location is looking for. As with RUCKUS Unleashed and Rucks Cloud, RUCKUS SmartZone controllers can also manage RUCKUS ICX switches. RUCKUS SmartZone comes in Essentials or High Scale versions to match any scale needed; from small rural school districts to the largest urban districts imaginable, SmartZone has an option that fits any need. See Table 3: SmartZone Network Controller Family for a breakdown of SmartZone controllers and specifications.

	Appliances	Virtual Appliances
Medium and/or Distributed Campus	SmartZone 100 (SZ100) 60,000 clients per cluster 3,000 APs 600 switches	Virtual SmartZone – Essentials (vSZ-E) 60,000 clients per cluster 3,000 APs 600 Switches
Large Campus	SmartZone 300 (SZ300) 450,000 clients per cluster 30,000 APs 6,000 Switches	Virtual SmartZone – High Scale (vSZ-H) 450,000 clients per cluster 30,000 APs 6,000 Switches

Table 4: SmartZone Network Controller Family

Note: The number of supported APs and switches as of Q2 of 2020.

RUCKUS TOP TIP!

Pick the controller needed today without fear of future needs. Being able to move all AP models between controller platforms is a RUCKUS differential!

Wired Network Design

With all the suggested discovery items have been identified in the detailed design session, we should now know how many and what type of APs, switches, and what type of client onboarding and security we will be deploying.

Wi-Fi planning and survey tools like Ekahau will generate a report with the location, specific model and power levels you will need to deploy the APs, but this will need to be followed up with Visio or CAD drawings with exact locations of not only the APs but the switches, any IoT bridges and wiring closets.

In order to have a stable and robust wireless network, the structured cabling and switching infrastructure has to be able to not only support this new wireless network today, but also for years into the future. The next 2 sections will cover both of these subjects.

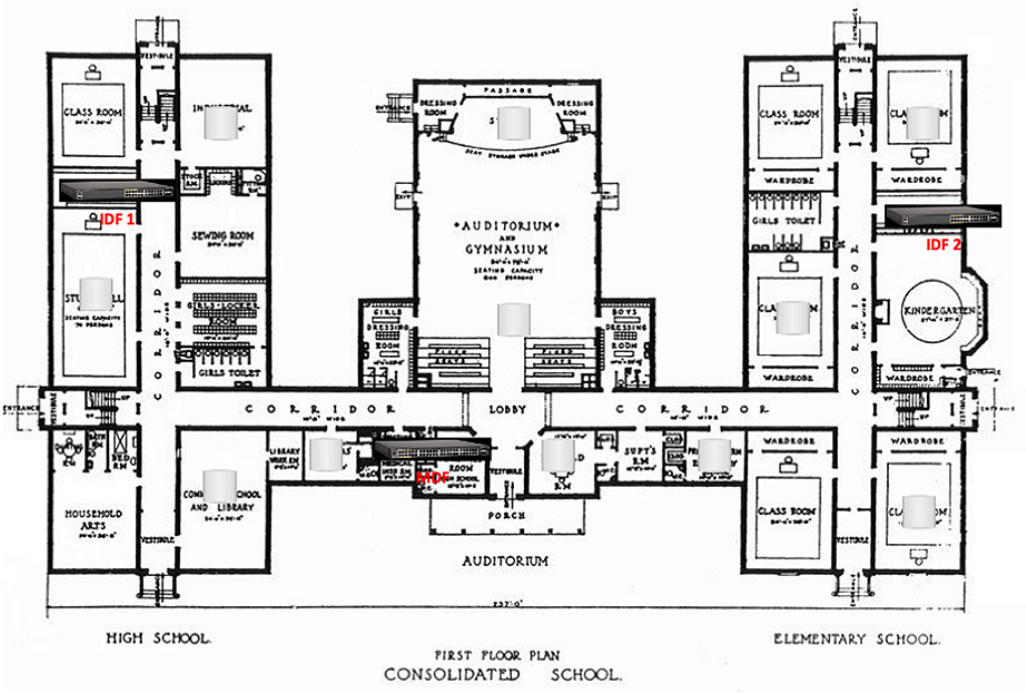


Figure 6: AP and Switch Placement

Structured Cabling Design

Structured cabling is the foundation for reliable high-performance networks. A well-planned infrastructure not only provides the bandwidth required for today's most demanding applications it also reduces operational costs, as **up to 70% of network issues are related to cabling**. Additionally, it's important to plan your structured cabling so that it lasts through 3-5 technology refreshes. The costs to rip and replace cabling can have a serious impact on your network projects budgets and timing. Planning your network infrastructure so that it lasts through multiple technology refreshes will reduce the cost and implementation timelines of those future network upgrades.

The information provided in this section is a simplified guide; links to more detailed cabling standards and resources can be found at the end of this section. Please refer to your local building codes and Authority Having Jurisdiction (AHJ) for codes and building safety requirements.

RUCKUS TOP TIP!

A robust and "future proofed" wired infrastructure (cable plant and switches) will ensure a high performing wireless network for years to come.

Architectures

CommScope supports multiple network architectures. Maximum flexibility allows our education customers to design and deploy the network that is best suited for their environment. **Many factors should be considered when you determine which network architecture is best for you,** from the size of your network, available telecommunications room space, maintenance, staffing and the occurrence of moves adds and changes.

Copper to the Classroom

A traditional star topology where there is fiber backbone that spans from a Main Equipment Room (MER)/ Main Distribution Frame (MDF) to multiple Telecommunication Rooms (TR) / Intermediate Distribution Frame (IDF) and then extends from the TRs up to 100M to the devices within the classrooms and common areas with copper category cabling. Consolidation points can be added as a passive distribution point to reduce distance on cables for future moves adds and changes.

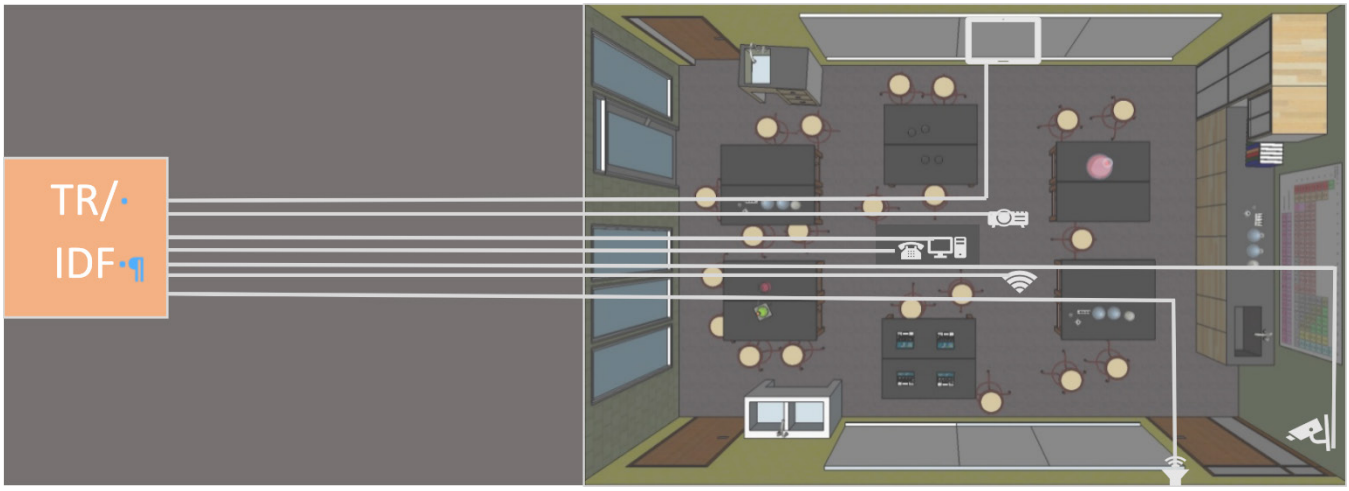


Figure 7: Copper to the Classroom

Fiber to the Classroom

Fiber to the Class is a distributed access architecture that gets the access layer of your network closer to the endpoint devices in the classroom. Instead of running copper cables to all your devices from a TR/IDF, fiber cables are installed from the TR/IDF or MER/MDF to a classroom or pod of classrooms where you locate a network switch and run much shorter copper category cables to your devices. This design offers maximum flexibility for simple moves adds and changes as pre-terminated cables can be typically be added quite easily without the need of special training. It also provides the high-performance fiber optic cabling closer to the endpoint devices which will help provide future support for Machine to Machine (M2M) communications, edge computing and AR/ VR applications.

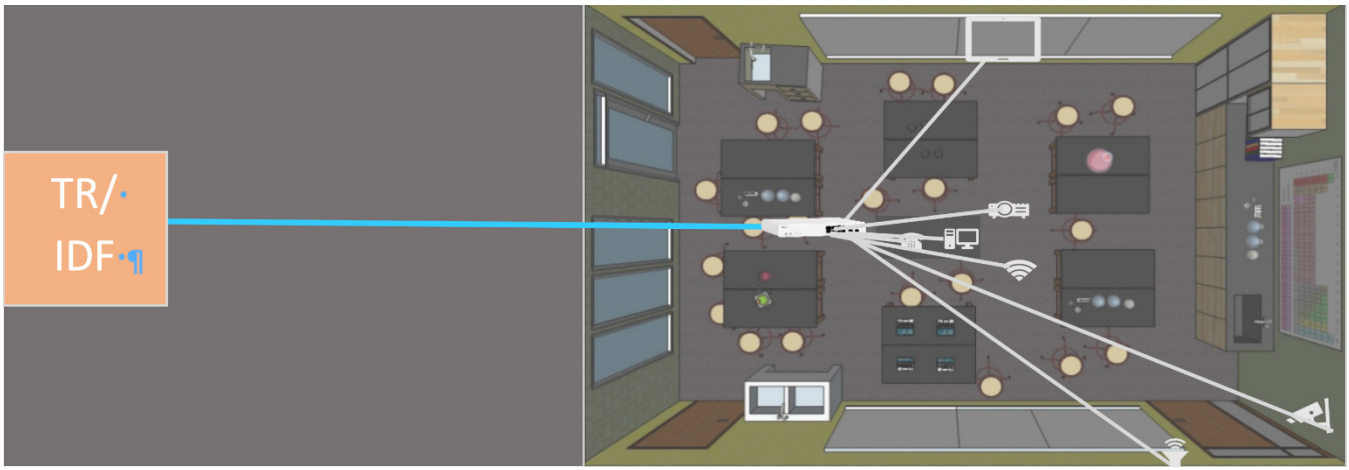


Figure 8: Fiber to the Classroom

Design Considerations

When designing networks for the classroom, doing both fiber and copper to the classroom have advantages and disadvantages. The goal here isn't to differentiate which design is better but to illustrate the differences so the final decision best matches the requirements at hand.

Copper to the classroom

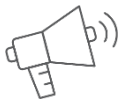
Running copper lines to the classroom is advantageous when there isn't a lot of devices expected to be connected in each classroom. By consolidating the switching hardware in the TR/IDF, the number of switches to manage as well as backup power considerations are less. Physical security is also easier since controlling access to the TR/IDF is usually factored into the facilities planning.

The downside to this methodology is adding additional capacity later, or relocating the drops, is expensive and time consuming. With this configuration all of the needs of the network are consolidated in a single closet. This requires having enough copper ports in the IDF to accommodate current needs as well as expansion across a wide area of the building. The entire Power over Ethernet (PoE) budget is consolidated so the switches chosen needs to be able to accommodate the current needs as well as future expansion factored in. Any other downside to this is generally well known since this is the traditional way that networks have been designed and deployed in the past.

Fiber to the classroom

Running fiber to each classroom has grown in popularity recently. A single fiber run to each classroom can be much cheaper than multiple cables. With a compact switch in each room, additional devices can be connected without much work. Also, by distributing the PoE needs across many devices, higher power switches aren't needed in the TR/IDF.

At first glance it may appear this solution offers the greatest flexibility; it does come with caveats to consider. With fiber running to each room, the IDF switching hardware will need more SFP ports to support the multiple fiber runs while also needing to support some copper PoE ports for infrastructure in the IDF (IP phones, PoE cameras, IoT sensors). Securing the physical access to the ports can also become a challenge. Limiting access to staff while restricting access to students and guests can be a challenge and depends greatly on the needs of the network. The other downside is with a switch in each classroom the backup power/Uninterrupted Power Supply solution can quickly drain the budget for the project. Management of a solution like this also needs to be considered as the number of devices to configure and maintained will be much more that the traditional copper to the classroom design.



RUCKUS TOP TIP!

Placing a switch in each classroom means more SFP ports needed in the IDF and not as many copper ports. By running copper cables to each classroom there will need to be more copper ports in the IDF with higher power needs.

Also, don't forget about aggregate bandwidth needed on SFP model switches, both on the switch and upstream to the core or upstream aggregation point.

Not every factor can be included in any document, make sure to look for specific issues related to the design in question as they can affect the design of the wired network.

Whichever design a customer chooses to use, CommScope RUCKUS is there to assist with cabling, switching, and wireless needs.

Planning and Product Selection

Proper planning and product selection now can make all the difference when it comes time for test and turn up of the network. Along with the network devices like switches and APs, CommScope also offers a variety of products to ensure the network equipment performs as expected.

Telecommunications Spaces and Pathways

Planning your telecommunications spaces and pathways in an integral part of your network infrastructure. Consideration should be made to accommodate network equipment, power and power backup equipment and pathways and conveyances to accommodate cable bundles. There are detailed standards available for designing and building your telecommunications spaces, but some standard guidelines include:

- Ensuring 3 feet of clearance around racks and equipment. This requires understanding your equipment depths that will be rack mounted.
- Rooms should have dedicated power circuits, that have local or system level battery backup and/ or UPS.
- Telecommunications Rooms should be equipped with a proper grounding system to the room and extend to racks and metallic cable conveyances.
- HVAC should be based on the equipment heat / power loads and optimal operating temperature for your equipment.

CommScope offers supportive hardware for your Telecommunications Rooms as well as cable management solutions for copper and fiber cables. Category 6A is recommended for your horizontal / device cabling. Category 6A has a slightly larger outside cable diameter because and is heavier than Categorey6 and 5E, this requires that your pathways and conveyances including vertical and horizontal cable management be sized appropriately. CommScope's horizontal and vertical cable management was built specifically to accommodate Cat 6A cables. Our Fiber Guide solution protects and manages your fiber optic trunk cables and jumpers.

Figure 9: CommScope Racks & Cable Management

https://www.commscope.com/product-type/cabinets-panels-enclosures/frames-racks-cabinets/

https://www.commscope.com/product-type/cable-management/

Building the Backbone

Converged networks are driving the need for robust campus and building fiber backbones. More and more devices are coming on to the network and that means network backbones will need to handle rapidly expanding bandwidth demands. Your campus cabling backbone should provide no less than 100G in bandwidth and larger campuses and technology rich campuses should be building to 400G. This can be accomplished with Singlemode or Laser Optimized Multimode Fibers OM3, OM4 and OM5. Your intra building backbone should have Singlemode and Multimode Fibers and your campus backbone should have Singlemode Fibers and if distance permits Multimode OM4 or OM5 Fibers. Multimode OM4 and OM5 fiber provides 10G of bandwidth up to 550M. Multimode network electronics are typically more cost effective, and some systems require the use of MM fibers, so it's good to have both available. Singlemode has the most bandwidth capability and from a building and campus standpoint distance is not a limiting factor for SM fiber.

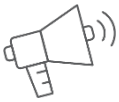
The LC connector is the defacto standard for network equipment and it provides a small form factor for improved density and better performance over other legacy fiber connector styles. Fiber termination shelves can be rack or wall mounted, the size of your Telecommunications Room and number of connected devices often drives which type of fiber shelf is best suited.

The most important thing to remember when it comes to your fiber backbone is that bandwidth demands are expanding to accommodate new learning technologies like Augmented and Virtual Reality platforms, Wi-Fi for everyone, and Operational Technologies from building management systems to health and safety systems. An inadequate fiber backbone will keep you from being able to successfully deploy these emerging technologies. **Plan your fiber backbone to last through 3-5 technology refreshes and 15-20 years of use.**

CommScope offers a comprehensive portfolio of fiber cables and connectivity for your campus. We offer pre-terminated cables and cables with protective armor that can be installed with other cables in conduits and without innerducts. Our powered fiber cable solution provides extended distance support for PoE devices that are more than 100 meters from the nearest telecommunications room.

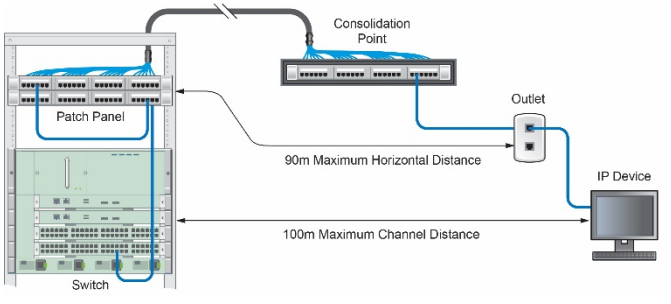
https://www.commscope.com/globalassets/digizuite/2152-campus-fiber-ordering-guide-co-112931-en.pdf

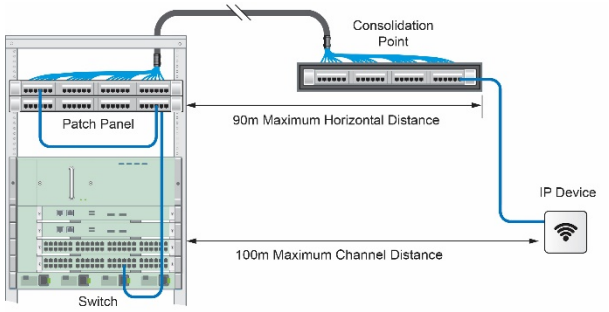
https://www.commscope.com/product-type/networking-systems/powered-fiber-cable-systems/



RUCKUS TOP TIP!

Fiber backbone infrastructure planning needs to incorporate decades of use so plan for this to outlast the rest of the network for many refresh cycles in the future.





Workstation and Device Cabling

Category 6A is recommended for your device cabling. Category 6A provides up to 10 Gigabits of bandwidth and can support the highest 4 Pair PoE standard 802.3bt Class 8. **It's recommended to install a minimum of (2) Category 6A cables to each telecommunications outlet including ceiling device locations; this is especially important for Wi-Fi Access Point locations.** Cabling should be terminated to a Category 6A outlet at the device location and a Category 6A patch panel in the Telecommunications Room, each cable should be labeled at both ends and tested with Category 6A cable certification equipment. Horizontal Cat 6A cables should not exceed 90 Meters with an additional 10 meters allowed in patch cables for a total maximum channel length of 100 meters.

For ceiling and wall locations where a telecommunications outlet is not practical, you can utilize our Ceiling Connector Assemble, CCA, it offers a simple termination to apply an RJ-45 end for direct connection to a device, versus the typical outlet and patch cords installation.

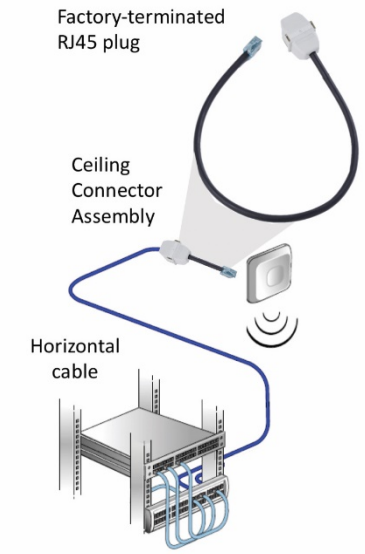


Figure 10: Ceiling Connector Assembly

RUCKUS TOP TIP!

When designing and installing copper cables, it is easier and cheaper to install more runs and drops than needed to ensure easier growth and expansion in the future.

Labeling, Testing and Documentation

Your structured cabling system should be labeled at both ends of all cables, both copper and fiber. Cable labels should be applied to identify the cable at each end. Termination hardware should be labeled at the port level at both ends. Rooms, racks, power circuits and network equipment should be labeled as well. Labels should be professionally printed, and labels should have appropriate rating and adhesion for their environment so they will last through the lifespan of the structured cabling system.

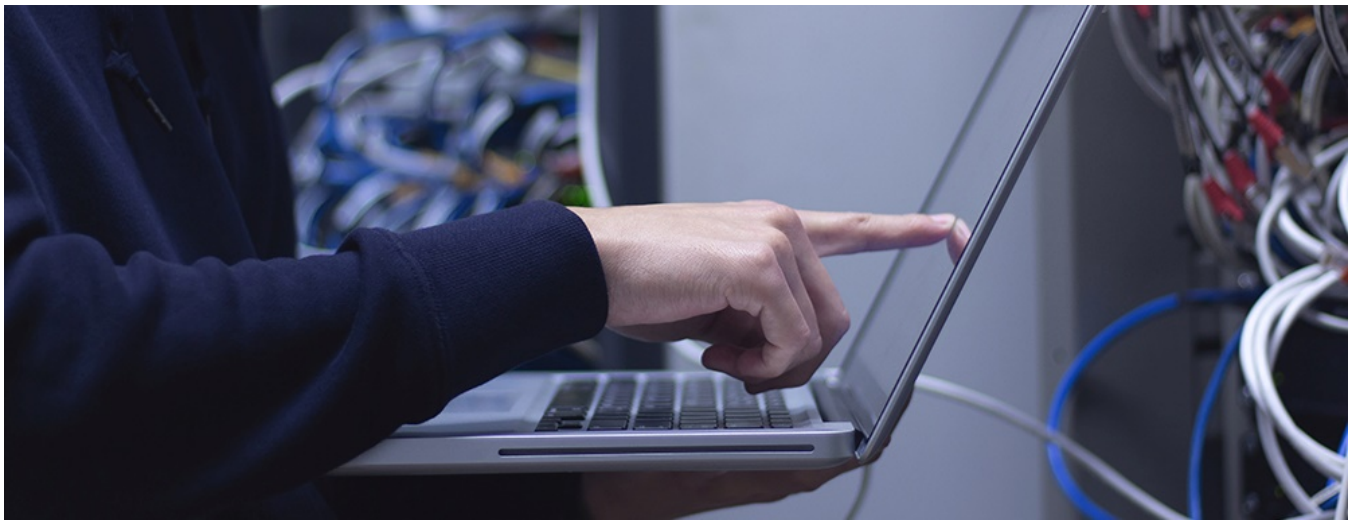
Testing is a critical component to your structured cabling system. The majority of network problems stem from cabling issues. Requiring each copper and fiber cable be tested and certified to the corresponding standard helps prevent unnecessary connection issues that can slow network deployments and cause significant downtime on active networks.

Properly documenting your network is essential to ongoing maintenance and troubleshooting efforts. Documentation should be maintained in a central repository with backup resources in case of a data loss. As-built drawings that include device cabling locations, backbone cables and Telecommunications Rooms elevations along with a record of all cable tests and cable system warranty information should be maintained and updated regularly with moves, adds and changes information.

https://www.commscope.com/resources/labeling-templates/

RUCKUS TOP TIP!

Proper testing and documentation during installation is crucial for future operation and troubleshooting. Ensure this is done and documented not only for the customer but also the partner.



AIM Automated Infrastructure Management

Automated infrastructure management (AIM) solutions are hardware/software systems that monitor, map and document connectivity across an entire network. They can also help you manage your PoE capacity on your campus. CommScope's AIM system is called ImVision. ImVision is an integrated platform of software and hardware that automatically tracks and updates your network infrastructure and provides real time information to assist in MACs, mitigating security risks and provisioning services. **Applying physical location information to network management data provides the most comprehensive real time view of your network and is what sets ImVision AIM apart from other network management tools.** The data exchange framework, defined in the ISO/IEC 18598 standard, is responsible for facilitating interoperability between AIM solutions and other third-party applications.

https://www.commscope.com/product-type/networking-systems/automated-infrastructure-management/

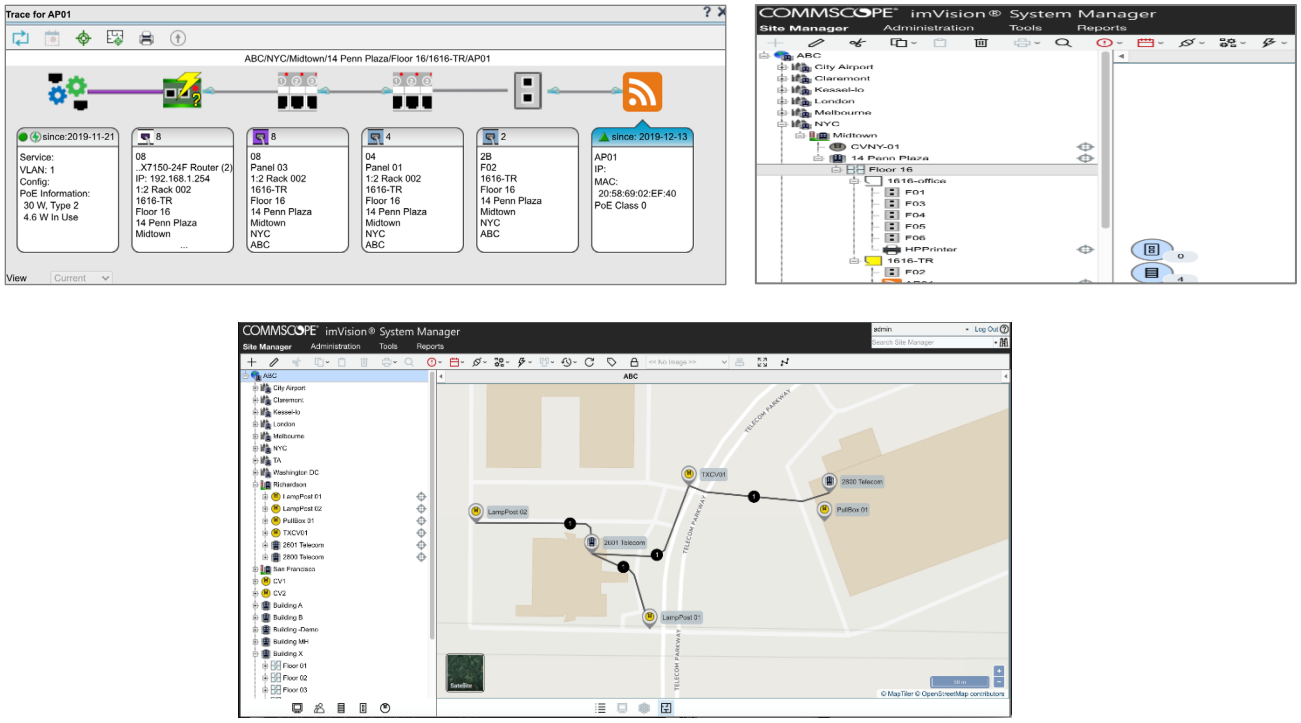


Figure 11: CommScope ImVision AIM Dashboards

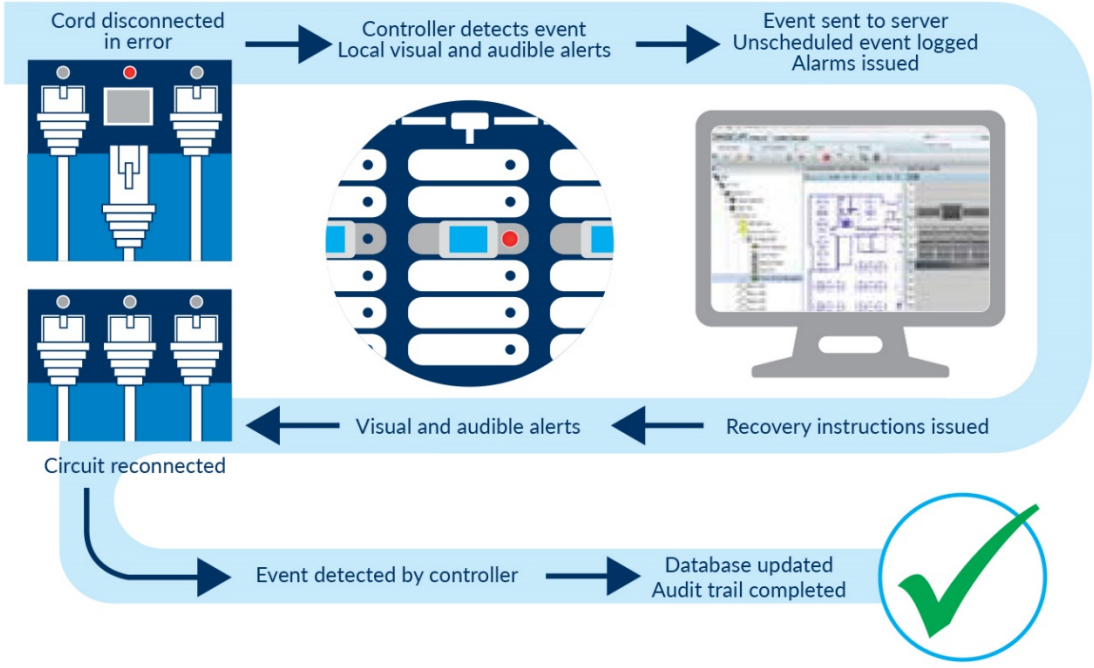


Figure 12: Automated Incident Management with AIM

RUCKUS TOP TIP!

ImVision is a crucial tool not only in documentation but also troubleshooting both wired and wireless issues as they arise.

Warranty

Your structured cabling system is intended to last 15-20 years and through multiple technology refreshes. CommScope offers a comprehensive 25 Year Warranty to protect against material defect and provide guaranteed performance of our cable system when installed in accordance to our installation guidelines by a CommScope Certified Infrastructure Solution Provider. CommScope's PartnerPro Network is a network of the most highly qualified and trained professionals in the industry. Our Infrastructure Solution Providers have completed a rigorous training regimen along with CECs to maintain their CommScope certification.

PartnerPRO® NETWORK

With so much riding on your network infrastructure a comprehensive warranty backed by the leader in network infrastructure and installed by the most qualified technicians in the industry is the right foundation for your education network.

https://www.commscope.com/resources/warranties/

https://www.commscope.com/partners/

Additional Structured Cabling Design Resources

Official Wired Infrastructre Design Guide

https://www.commscope.com/globalassets/digizuite/61603-campus-design-guide.pdf.

PoE Implementation Guide

https://www.commscope.com/globalassets/digizuite/3145-poe-implementation-guide-co-112435-en.pdf?r=1

Universal Connectivity Grid Design Guide

https://www.commscope.com/globalassets/digizuite/3465-universal-connectivity-grid-design-guide-br-108900-en.pdf

6A SYSTIMAX X10D Design Guide

https://www.commscope.com/globalassets/digizuite/2620-gigaspeed-x10d-design-install-guidelines-tp-109086.pdf?r=1

CommScope SYSTIMAX Structured Cabling Design and Engineering Online Training

https://www.commscopetraining.com/courses/cabling/sp3321/systimax-design-engineering/

Data Center Structured Cabling Best Practices

https://www.commscope.com/resources/eBooks/Data-Center-eBook/

CommScope cCatalog App

https://www.commscope.com/resources/apps/ccatalog/

CommScope eCatalog (go to PRODUCTS section)

https://www.commscope.com/

Device Types and Count

Along with APs that have been identified previously, the wired network design also needs to take into consideration other devices that need to be connected. These devices can be, but not limited to, desktop computers, cameras, printers, and IoT sensors. Along with the devices that are currently known, care needs to be taken to allow for future growth. Once a stable network is in place, there is a tendency for others to just take for granted that additional switchports are available and never take into account that a switch might not have available ports.

Future growth should be defined early in the process as a percentage. Allowing for 15 to 20 percent of growth is a best practice. In practice that means that if an Intermediate Distribution Frame (IDF) is defined to support 12 devices, plan for an additional 20% growth so the switch really needs to support 15 ports. This planned growth is cheaper to account for in the long run as upgrading a switch to higher port counts is cheaper before purchase than after. It also removes the downtime needed to replace the switch, or the effort to stack in the near future.

Power over Ethernet

Device types are important to determine needed bandwidth and PoE capacity. As more and more devices become reliant on PoE (overhead lighting as an example) ensuring that additional ports and PoE is available in the future is something to consider more and more. PoE was covered in depth previously, see the section titled Power over Ethernet to review if needed. When selecting a new switch for a switch replacement or new installation, ensure that the new switch is capable of providing the power needed not only today, but in the future as well.

RUCKUS ICX switches and their ability to manage PoE allocations and ensure every device is allocated the power they need without wasting the overall power availability is another way that RUCKUS ICX switches provide value.

Switching infrastructure

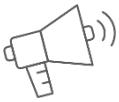
The ethernet switching infrastructure is the heart of the network. Based on the assumption the readers of this document have an understanding of ethernet and fiber infrastructure, we will not cover any limitations of where the switches are to be deployed but rather show a common example of how a RUCKUS ICX would be configured to accommodate staff, students, guest, and things like cameras and network printers in a typical K-12 deployment.

Compact vs Standard Switches

Depending on the requirements of the network, RUCKUS ICX switches combines enterprise-class switching features with high performance at entry-level price. The ICX 7150 series of switches are available in three formats: standard, Z-Series with multi-gigabit support, and compact. The switch can operate in fanless mode outside of the wiring closet to provide silent operation for classrooms or other noise sensitive environments.

It is this compact, silent switch that network designers in the K-12 environment can really take advantage of. The Ruckus ICX 7150 compact switches come in 8, 10 and 12 ports models and offer PoE on all ports. The ICX 7150-C10ZP delivers up to 90W per port of PoE power and multigigabit Ethernet at 2.5/5/10 Gbps speeds. With 2x1/10 GbE uplink/stacking ports, the ICX 7150-C12P and C10ZP deliver high performance in a small package.

The standard Ruckus ICX 7150 switches are available in 24-, and 48-port 10/100/1000 Mbps models with four 1/10 GbE dual-purpose uplink/stacking ports. These switches are available with or without PoE+ power. Silent operation is available for out-of-closet environments. The ICX 7150-48ZPand ICX 7150-C10ZP offers multi-gigabit ports, each with PoH up to 90 watts. The ICX 7150 series supports stack-level high availability and stack level ISSU (In Service Software Upgrade) to ensure service resiliency and business continuity.



RUCKUS TOP TIP!

Define the requirements needed for each switch and switch location and then find the RUCKUS switch that fits those requirements.

Switching Design

Based on our site surveys and design guide we have an example deployment consisting of the following:

- 10 RUCKUS R610 access points for Wi-Fi access
- 2 RUCKUS ICX 7150-24P POE switches in each Intermediate Distribution Frame (IDF)
- 1-2 RUCKUS ICX 7450-48P POE switch in the Main Distribution Frame (MDF)

Assumptions

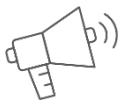
1. Router providing firewall, DHCP, DNS, and NAT services either on site or at a district data center
2. WAN connection is sufficient to handle the number of users and type of traffic traversing both the internal districts WAN and internet traffic.

For most deployments, the capacity of the WAN connection will be the limiting factor in the design. With new APs and switches supporting MultiGig connections (connections above 1 Gbps with Cat6 cable) and fiber connections between the IDF and MDF capable of well above 1 Gbps, understanding where the majority of devices will be accessing the data from is important. For locations that access all their data from offsite (centralized district data center, public cloud locations, or the internet) this WAN to connection to everything offsite becomes critical to understand. For locations that host some content locally the WAN connection won't need to be scaled as large, but it is still something to consider.

See Table 4: WLAN & VLAN Assignment for an example wired network assignment.

Users	SSID	VLAN	User profile	Notes
Staff	802.1x either with existing radius or with RUCKUS Cloudpath	100	No Rate limiting and district-based staff firewall rules.	Consideration must be made for the event of a substitute teacher or training teacher to gain access.
Students	802.1x either with existing radius or with RUCKUS Cloudpath	200	100mb rate limit and district-based student firewall rules and traffic policies.	Application visibility and OS policies should be considered for student networks for added network optimization.
Infrastructure devices	Wired connection or DPSK (dynamic pre-shared key) assigned to the devices MAC.	300 Printer etc. 350 for Cameras	No rate limiting, no firewall policies except for cameras which access only to an NVR/DVR	All cameras should be wired into switches but can be uplinked via the Wi-Fi if needed.
Guest	Guest authentication portal via the RUCKUS controller or RUCKUS Cloudpath onboarding	400	Rate limit 12Mbps, client isolation on the WLAN, firewall policy of internet only traffic.	Guest networks can be as simple as accepting terms of use for temporary guest but in the event of the need for extended guest accounts, RUCKUS Cloudpath can accommodate a more advanced Guest onboarding.

Table 5: WLAN & VLAN Assignment

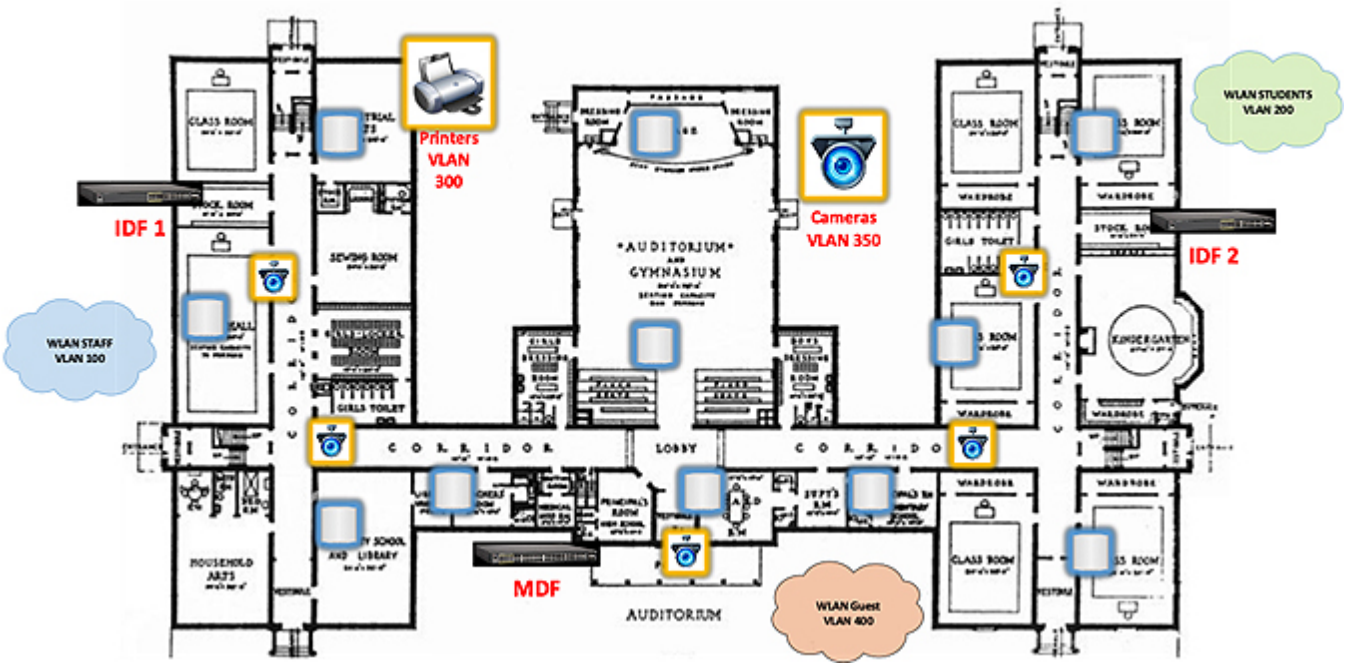


RUCKUS TOP TIP!

When selecting SSIDs, try to keep the number of SSIDs at 4 or less, with three SSIDs being optimal. Utilize RADIUS attributes and DPSK to help assign devices to the required VLANs to limit the number of SSIDs to as few as possible to reduce beacon overhead.

When selecting VLANs and IP subnet sizes, ensure enough IPs per subnet and spacing out the VLAN IDs and IP subnets to allow for future growth. Assigning sequential VLAN ID's and Subnets now makes expansion tricky.

The drawing below represents the combined network. The colored clouds represent the separate WLANs broadcast and their corresponding VLANs; the infrastructure devices are represented by shaded icons as well as VLAN designation. Each AP and camera are connected directly to a RUCKUS ICX switch.



Switch Configuration

The illustration below represents the 3 port types configured for this sample deployment. The group of blue ports represents the switch ports set to trunk mode to accommodate the RUCKUS APs utilizing local breakout (LBO) in which the traffic from each SSID is placed into their respective VLAN on the local switch, not tunneled to a central location. The orange group represents the ports set to access mode and tagging packets with VLAN 350 for the security cameras, the green group or ports represent the ports set to access mode and tagging packets with VLAN 300 for the infrastructure devices such as computers and printers. To be clear, the devices are not required to be grouped as shown, this was done for visual effect only. Ports can be assigned as desired/needed for each IDF/MDF.

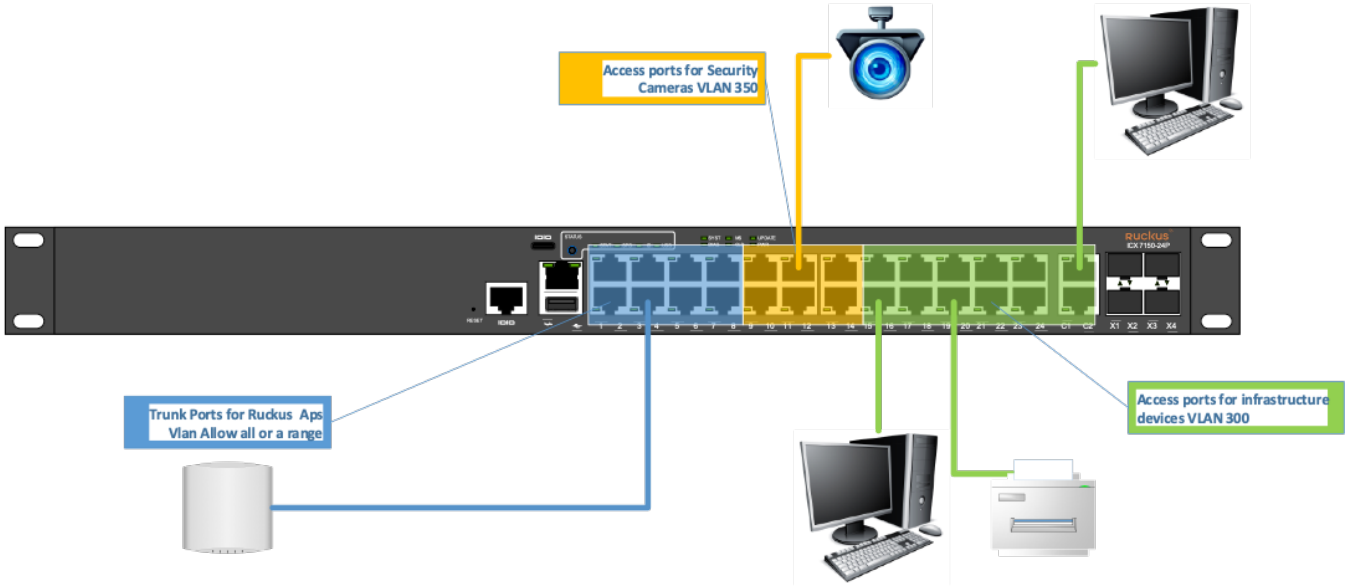


Figure 13: Switch Configuration

Switch Management

RUCKUS ICX switches offer diverse management options that can accommodate any level of experience. From the traditional Command Line Interface (CLI) management to the latest cloud management via RUCKUS Cloud managing the switching infrastructure has been brought to the masses.

While CLI is always available, switches can also be managed by any of the wireless controllers discussed in the Controller Selection discussed earlier. Switches can be managed by RUCKUS Unleashed, RUCKUS Cloud, or RUCKUS SmartZone (physical or virtual). This flexibility is a RUCKUS differentiator that allows any network administrator the flexibility and stability to manage and monitor both the wired and wireless network in any method they prefer.

Client Onboarding

Briefly referenced in Table 4: WLAN & VLAN Assignment, considerations need to be taken on how devices will join the network. Factors affecting how clients can be broken down into the following considerations:

- Security Requirements for each WLAN
- Types of devices that will be seen
- What network resources each type of device will be allowed to access

RUCKUS has many built in features that can facilitate client onboarding depending on specific needs or network administrators can use RUCKUS Cloudpath to manage all of their onboarding and client profiling needs. The Cloudpath Enrollment system is discussed more at the end of this section.

Security Requirements

Security requirements is a topic that should have been discussed during the initial meetings with the stakeholders. Existing policies need to be examined to determine the requirements for securely joining devices to the network. Existing Public Key Inventory (PKI) systems need to be taken into account, and then applied to each WLAN as needed. Determining client capabilities allows for determining what security is allowed.

Not all devices can support certificates needed for WPA2/WPA3-Enterprise which is where WPA2/WPA3-Personal using RUCKUS DPSK enters the discussion. Dynamic Pre-Shared Keys (DPSK) are a RUCKUS Patented technology found in the Unleashed, Cloud, and SmartZone controller platforms. DPSK technology allows the same functionality of a standard WPA2/WPA3-Personal Pre-Shared Key but with the individual control offered by WPA2/WPA3-Enterprise solutions. For more functionality and control external DPSK (eDPSK) using RUKCUS Cloudpath is also an option. Using eDPSK allows a server external to the controller, like RUCKUS Cloudpath, to manage the clients using the DPSK functionality.

These requirements will also determine what devices and users are allowed to use the network for and what they are allowed to access. RUCKUS solutions can leverage 802.1X authentication, captive portals using social media log ins, DPSK for assigning each guest their own PSK, or no restrictions at all.

Devices Types

Any Wi-Fi network will see many different devices that need to access the wireless network. Not only are there hardware considerations that need to be understood (iPad or Chromebook) but also who ultimately has control of the device, and as a result, how those devices are managed and what they are allowed to access when connected to the network.

District Owned Devices

These are devices that are provided by the school district and can be managed by IT staff to ensure updates are applied and certificates can be generated for each device. The delineating factor with these devices is that both the device and the person using it are considered “trusted” so generally more access to the network is allowed with these devices.

Considerations also need to be taken with devices that, while owned and managed by the district, aren’t fully capable when it comes to not only security (some devices can only do pre-shared keys, not certificates) but wireless Internet of Things (IoT) devices with limited radio capabilities (only supporting the 2.4 GHz band) and other limited power options.

BYOD

Bring Your Own Device (BYOD) is the concept that instead of district owned devices being provided to faculty and students, each person will bring a device of their choosing to be utilized on the network. Devices like this are harder to maintain security updates, don’t always allow for certificates to be loaded on them, and therefor aren’t seen as fully trusted devices. While the person who uses this device is trusted, due to the lack of control

over the device itself, the device isn't fully trusted. BYOD devices are generally allowed to access network devices like printers but, depending on district policy, nothing else but the internet.

Guest Access

Guest devices that are allowed access to the network differ from BYOD. With BYOD devices, the person who owns the device is trusted while the device itself isn't. With guest access, neither the device nor the owner is trusted, but access to just the internet is the goal of the service. How these devices are allowed to connect to the network should be defined in policies discovered during the initial meeting, but best practice design is once these devices are connected, the device should be isolated from other devices on the network, and all the traffic needs to be isolated via 802.3 mechanisms from any corporate resource. At that point access to the internet can be provided per the wired design.

RUCKUS Cloudpath Enrollment System

As part of the RUCKUS ecosystem, RUCKUS Cloudpath is a software/SaaS platform that delivers secure wired and wireless network access for District-Owned devices, BYOD, and guest users. It streamlines getting devices on the network and secures every connection with powerful encryption. Cloudpath software gives you granular policy control over what network resources users can access. It lets you deliver a great end-user experience and virtually eliminates helpdesk tickets related to network access. Choose from cloud-based or virtualized on-premises deployment. Cloudpath software supports any user, any device, and any network infrastructure.

Increase Security for Users, Devices, Data and the Network

Cloudpath software secures network connections with WPA2/WPA3-Enterprise—the highest standard in secure Wi-Fi. The system encrypts data in transit between the device and Wi-Fi access points for maximum security. It lets you define and manage polices for network access so that users see only what they should see. You gain visibility and control over what devices are on the network, and the power to revoke access at any time. A device posture check with remediation during onboarding ensures that only devices with appropriate security safeguards in place gain access.

Streamline Network Access for BYOD Users

The sheer volume and diversity of devices that require network access can cause headaches for IT departments. What if BYOD users could self-provision their devices with intuitive self-service workflows? With the simple onboarding portal in Cloudpath software, they can. Users get a great experience without IT intervention. BYOD users initially gain access with existing login credentials. The system installs a digital certificate on the device so that users authenticate seamlessly from that point forward—without having to re-enter a Wi-Fi password.

Give Visitors Easy, Self-service Guest Wi-Fi

No matter what the environment—schools, colleges, hotels, public venues, or anywhere, really—the first thing visitors ask is "How do I get on the Wi-Fi?" Cloudpath software delivers secure guest access for visitors without involving the IT helpdesk. Guest users simply self-register for internet access via an intuitive portal and receive login information via SMS, email, or printed voucher. You can customize the login portal, guest workflows, terms and conditions, and more for a trouble-free and secure user experience.

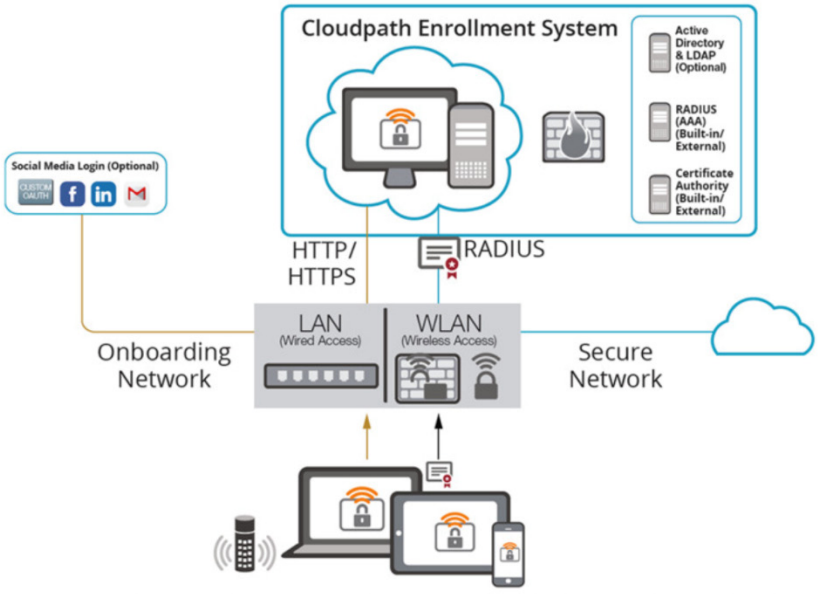


Figure 14: RUCKUS Cloudpath Enrollment System

RUCKUS eDPSK managed by Cloudpath

As discussed earlier, RUCKUS eDPSK managed by Cloudpath is the ultimate solution to securely onboarding and managing a wireless network when using 802.1X authentication methods aren't possible. This solution is also the answer to recent developments with random MAC implementation introduced in Apple's iOS 14, Android 10, and Windows 10. Cloudpath's ability to manage the devices using the single DPSK assigned to a user, whether it's multiple devices or a single device that is randomizing its MAC address, is second to none in the marketplace. With the additional challenges that random MAC addresses introduce to the operation of a network, and the number of calls that will come into a help desk if not properly managed, Cloudpath is the solution needed for the ever-changing landscape in primary education.

RUCKUS TOP TIP!

As more devices rely on the Wi-Fi network, operating these networks at any scale without a service that offers secure onboarding is becoming more and more difficult. Factoring secure onboarding into the design early allows for a more robust and stable network experience in the end.

Additional Information

RUCKUS Cloudpath Enrollment System

https://www.commscope.com/product-type/enterprise-networking/network-access-policy/network-access/

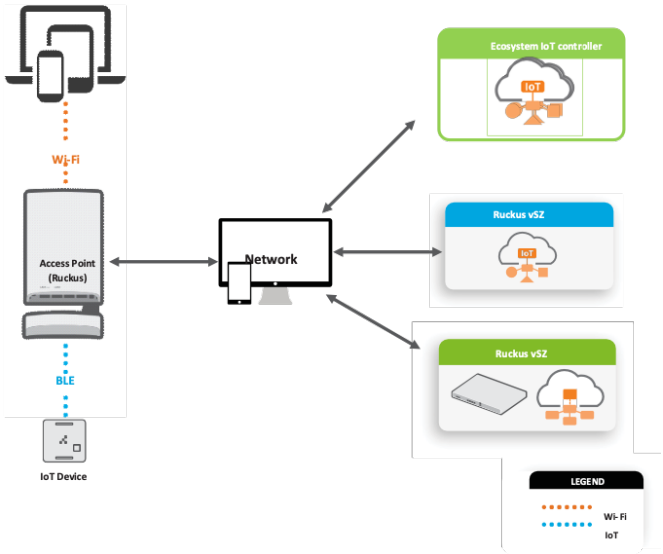
MAC Randomization Explanation

https://support.ruckuswireless.com/documents/3479-dangers-of-mac-randomization

Internet of Things

IoT Landscape

The Internet of Things (IoT) landscape is varied and rapidly changing. Each IoT system brings individual challenges and may use any number of network access technologies. When combined with other network vendors, IoT systems typically work in isolation from each other. Low power radio-based systems (Bluetooth/BLE, ZigBee, etc.) require a radio hub or gateway device specific to the protocol it uses, and that device requires a network port and power.



Best practices demand Wi-Fi systems be isolated and secured on dedicated VLANs and may need careful examination of performance requirements. Wired IoT devices can be powered using PoE, but power budgets add new dimensions to network design and switch management. Unfortunately, even solving all that, each IoT system is usually logically isolated from every other one with proprietary management systems.

RUCKUS IoT Vision

RUCKUS has a vision of unifying and integrating multiple IoT technologies and vendors so that they are secure and can integrate with each other, passing secure messages from one IoT system to another so that more complex problems can be solved with the interaction of multiple technologies – a simplified and unified network infrastructure. RUCKUS brings the networking expertise to our partners, who bring expertise in their areas.

At the logical layer, IoT devices are secured and unified by the RUCKUS IoT Controller, a virtual machine. IoT devices use a lightweight message protocol called MQTT (think 'https for IoT'). Because all such traffic is encrypted and forwarded to the RUCKUS IoT controller (acting as a MQTT broker), messages from different IoT systems can trigger functions on each other. A vaping or sound anomaly event can trigger not only an alert but can trigger a PTZ camera in the hallway to focus on the bathroom door or pull existing video from a VMS (Video Management System) with the correct time stamps to identify the involved students.

Depending on the physical layer, RUCKUS simplifies IoT connectivity. RUCKUS ICX switches have unmatched flexibility and scalability. For out-of-closet environments, ICX fan-less compact switches are silent with PoE/PoE+/PoH power options. For Wi-Fi IoT RUCKUS APs have unmatched capacity for more devices, and more performance. For Bluetooth, ZigBee and similar protocols, the RUCKUS IoT suite moves all low energy radio gateway functions onto our IoT ready APs with a mix of integrated and add in modules. The snap in IoT module becomes the gateway for radio based IoT devices, and piggybacks power and network on the AP cable. No additional cable runs or switch closet ports.

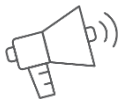
IoT Redefined: The RUCKUS IoT Suite

The RUCKUS IoT Suite solves many of the problems currently present in networking and IoT deployments.

- **Consolidated IoT Device** Management – A single place to look for all IoT devices and an IoT management system that eliminates the need for additional gateways and separate management

systems. A single IoT pane of glass makes management and troubleshooting simpler and more intuitive for what would otherwise be a dauntingly complex task.

- **Reuse Existing Infrastructure** – IoT can be deployed across the existing LAN and WLAN infrastructure, saving on deployment time and reducing costs. By providing a common point of management and cabling, multiple physical layer networks are consolidated into a single converged network. This simplifies IoT device onboarding and establishes uniform security protocols and policy.
- **Multi-layered Protection** – data transmitted between IoT Suite components is protected via standards-based security such as over-the-air encryption, SSL-secured MQTT and HTTPS REST communication.
- **Simplified Device Onboarding** – RUCKUS IoT Suite quickly connects IoT devices simply and easily.
- Expedited Deployment of follow on IoT – connect an IoT Module to an IoT-ready RUCKUS AP to quickly upgrade the WLAN to support new wireless technologies such as ASSA ABLOY locks, BLE ID tags or wristbands or building automation sensors.
- **Easily Deployed and Managed IoT** – IoT devices can be managed through the RUCKUS IoT suite for a sum greater (and less expensive) than the parts.



RUCKUS TOP TIP!

IoT has quickly gone from a niche, nice to have ability, to a necessity in a very short time. With network refresh cycles typically being longer than client device refresh, planning now to incorporate IoT into the network now will save time and money in the future.

Vaping Detection

While not meant to be an in-depth discussion on vaping detection, any discussion about IoT solutions for education networks wouldn't be complete without a discussion about vaping and the need to detect when students are vaping on school property. For primary and secondary education, the core mission is not only to educate the students, but also to take reasonable steps to ensure the learning environment is safe and secure. E-cigarettes were initially marketed as a way to help adult smokers quit the habit. However, companies moved quickly to targeting non-smoking youth, introducing a variety of flavors, personalization of vape devices, etc. Just to be clear, vaping is inhaling a heated and vaporized liquid (e-juice, vape juice, etc.) from an e-cigarette, vape, or any similar device. Overwhelmingly, the juices are nicotine based, with an infinite variety of flavors, although other drugs, such as cannabinoids can also be taken this way.

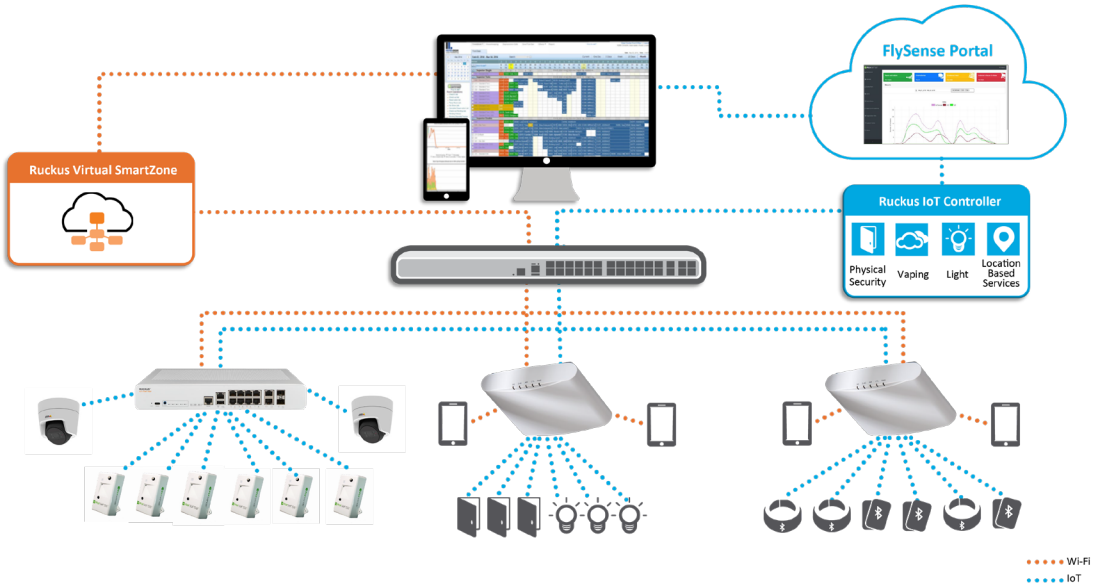


Figure 15: RUCKUS & Soter IoT Network

As they are with so much in our society, schools are right in the middle of the vaping epidemic. Schools are responsible for the health and wellness of the students in their care and are required to put into place measures to help protect students from exposure to harmful or unsafe conditions. Parents of students expect the school to protect their children from both the health implications as well as the social pressures that can create anxiety and emotional conflicts between students, which can result in psychological health concerns.

The need to cope with vaping is straining educational resources. Vaping in schools is a leading cause for out-of-school suspension. High school out- of-school suspensions cost the country $35bn annually, squeezing already tight district and school budgets as well as decreased national economic potential. Costs include added administrative oversight, remediation/counseling, parent meetings, credit recovery programs, increased truancy, increased criminal justice costs, and fewer graduates/reduced Higher Ed enrollment, and a lower-skilled work force.

Monitoring for vaping is difficult. The residual odor is easy to mask, the visual signature is limited, and use in areas protected by personal privacy such as restrooms is common. Supervision by faculty may be limited by other priorities like teaching, the high costs for faculty monitoring, union contracts that limit responsibilities, or understandable privacy concerns. Restrooms are particularly difficult in that they preclude visual supervision by faculty or security cameras.

A vaping detection sensor connected over a RUCKUS network enables a cost-effective means to directly target vaping use on campus. Ruckus has partnered with Soter Technologies to bundle an ICX PoE switch with FlySense™, Soter's real-time vaping and elevated sound incident detection solution. FlySense gives schools control of areas where they cannot place a camera. Soter's multi-sensor devices are capable of detecting vaping, as well as smoke and noise disturbances that may suggest violence or bullying. On detection, alerts can be sent by text or email, with simple and thorough customization of who gets what alerts on what schedule. Integrations with the RUCKUS IOT suite enable sensors to trigger additional connected devices such as security cameras (outside of bathrooms) and incident notification lights.

Soter is the networked vaping detection solution provider with a mission to simplify school health and safety. RUCKUS is the only network vendor to recognize how critical this technology is in schools and to elect to specifically test, QA and support FlySense sensors, and to work with Soter on advanced network standards. To learn more about Soter and its integration with RUCKUS networks you can use the following links.

Vaping Detection Overview

https://www.commscope.com/globalassets/digizuite/62526-sb-vaping-detection.pdf

Soter Technologies

https://www.sotertechnologies.com

Better Together: RUCKUS Networks and IoT

A great IoT deployment is only as great as the foundation it is built upon. The RUCKUS portfolio is designed from the ground up to deliver better experiences: to get devices on the network quickly and easily, keep them on reliably, and deliver the capacity and scalability needed to support new applications and devices. RUCKUS is the only network vendor to recognize how critical this technology is in schools and to elect to specifically test, QA and support Zigbee BLE sensors, and to work with advanced network standards.

Better Deployments

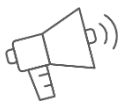
RUCKUS access layer ICX switches come with more PoE options and higher PoE capacities (PoE+, PoH) than other vendors switches, and we are the only network vendor to commit to testing and support of IoT devices. RUCKUS things should “just work”, and we bring our networking expertise to this partnership so that managers can focus on their IoT deployment instead of troubleshooting switch issues with other network vendors.

Better Security

The RUCKUS IoT Suite secures all manner of IoT devices. IoT traffic is tunneled over SSL to the IoT controller so that it is encrypted, it is securely isolated from the rest of the network, and it is rule checked. Instead of dozens of sensors accessing the IoT partner’s management system, one readily secured controller accesses the cloud managed system on their behalf.

IoT Strategy – Integration and Futureproofing

IoT has been the high-tech buzz phrase for some time, but it is now truly here. A piecemeal approach will mean higher costs and complexity down the line, while RUCKUS’ integrated approach will enable multiple IoT systems to interact and integrate with each other. Deploying a RUCKUS IoT controller will secure IoT sensors today and position the school for simplified deployment and integration of the next IoT system tomorrow.



RUCKUS TOP TIP!

CommScope RUCKUS has numerous IoT partners, contact CommScope RUCKUS for any questions surrounding any IoT requirement.

RUCKUS Analytics

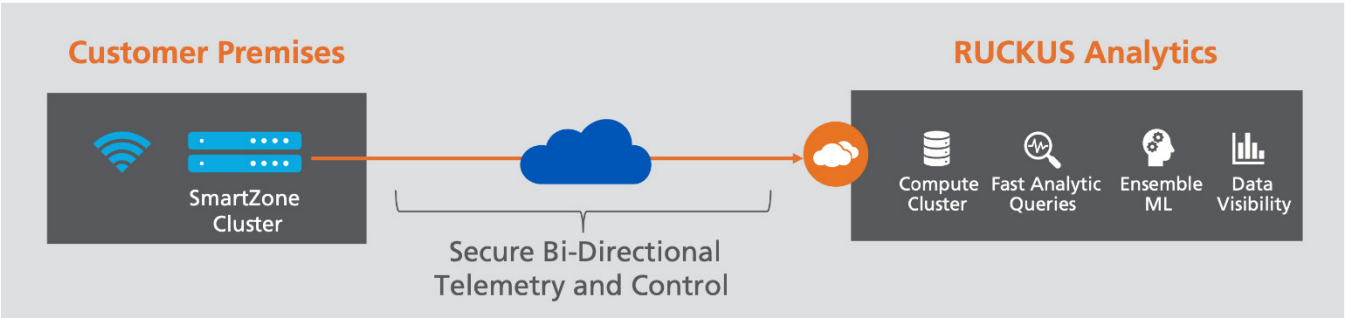
As technology advances, it is becoming increasingly difficult to track and manage everything that is utilizing and depending on both the wired and wireless networks. On its own any of the RUCKUS management systems (Unleashed, Cloud, SmartZone) provides base level information that, for most administrators, is enough to manage their network from on a day to day basis. How many devices are connected now or in the past, the amount of data being passed, is there a network device that isn't online anymore, all of this information is available.

As networks and technology evolves, the need for more visibility into the network has grown. RUCKUS Analytics from CommScope is a cloud service for network intelligence and service assurance. Powered by machine learning (ML) and artificial intelligence (AI), it gives IT teams comprehensive visibility into network operations. It accelerates troubleshooting and helps staff meet their network SLAs. Available for use in conjunction with RUCKUS Cloud or SmartZone on the code version 5.1.2 or later, this tool leverages ML for root cause analysis and remediation and AI to classify incidents so staff has a better understanding of the most impactful issues that need to be addressed first.

Single Pane of Glass

In a world where more and more platforms are needed to manage IT infrastructure requiring multiple screens, licenses, and time to educate staff, being able to reduce these platforms and screens required to manage and troubleshoot the network is crucial. While "Single Pane of Glass" is an industry buzzword it's really a misnomer. The idea isn't to only use 1 screen or window but to reduce the number of monitors and screens required for network engineers and administrators to a number more manageable. Minimal screens and platforms allow IT staff to quickly and efficiently deal with issues, freeing up time to focus on other tasks. For a glimpse on how RUCKUS Analytics can assist network administrators in a day to day scenario follow this link: https://www.commscope.com/globalassets/digizuite/536389-RUCKUS-Analytics-Infographic-IG-114389-EN.pdf

As a hosted service, RUCKUS Analytics relieves you of the burden of managing an in-house network analytics platform. Because the system stores data in the cloud, capacity is virtually limitless and expands instantly as your network environment generates more data. You don't have to worry about running out of capacity, forecasting disk utilization or figuring out when to add resources. RUCKUS Analytics does that for you transparently using containers and microservice orchestration. The software does not require an on-site data collector. Cloud deployment enables the machine learning algorithms embedded in RUCKUS Analytics to provide maximum insight.

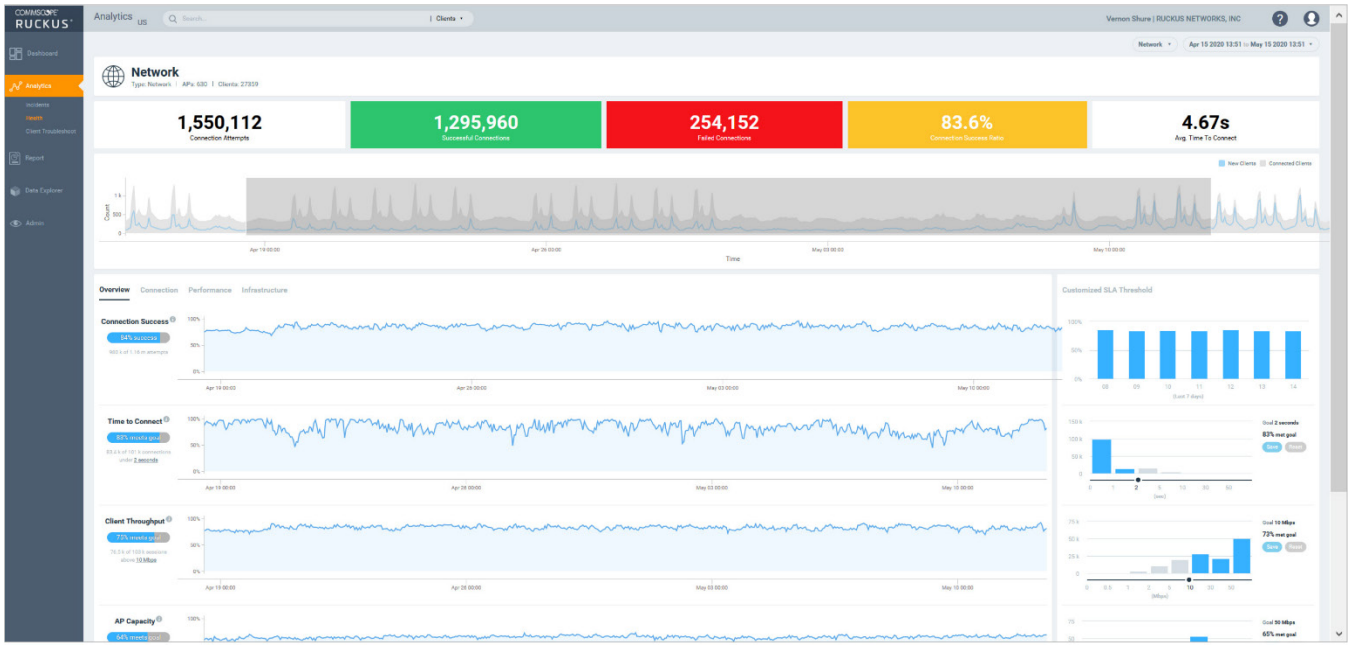


Service Assurance

The service identifies service assurance incidents, classifies them by severity, traces root causes and makes specific recommendations for remediation. It automatically monitors network health relative to configurable thresholds. Advanced client troubleshooting and incident analytics give IT teams the power to address service issues for individual users and devices. The service also delivers robust reporting and informative dashboards. Create custom dashboards and data visualizations with the Data Explorer tool—and flexibly explore your network data warehouse with drag-and-drop ease.

RUCKUS Analytics has an industry-unique combination of attributes:

- Automated data baselining and insights driven by ML and AI
- Health and SLA monitoring
- Powerful, holistic troubleshooting
- Automatic classification of incident severity
- No requirement for an on-site data collector or overlay sensors
- Granular access to raw data with deep exploration and custom dashboards
- 12 months of storage with flexible data reporting

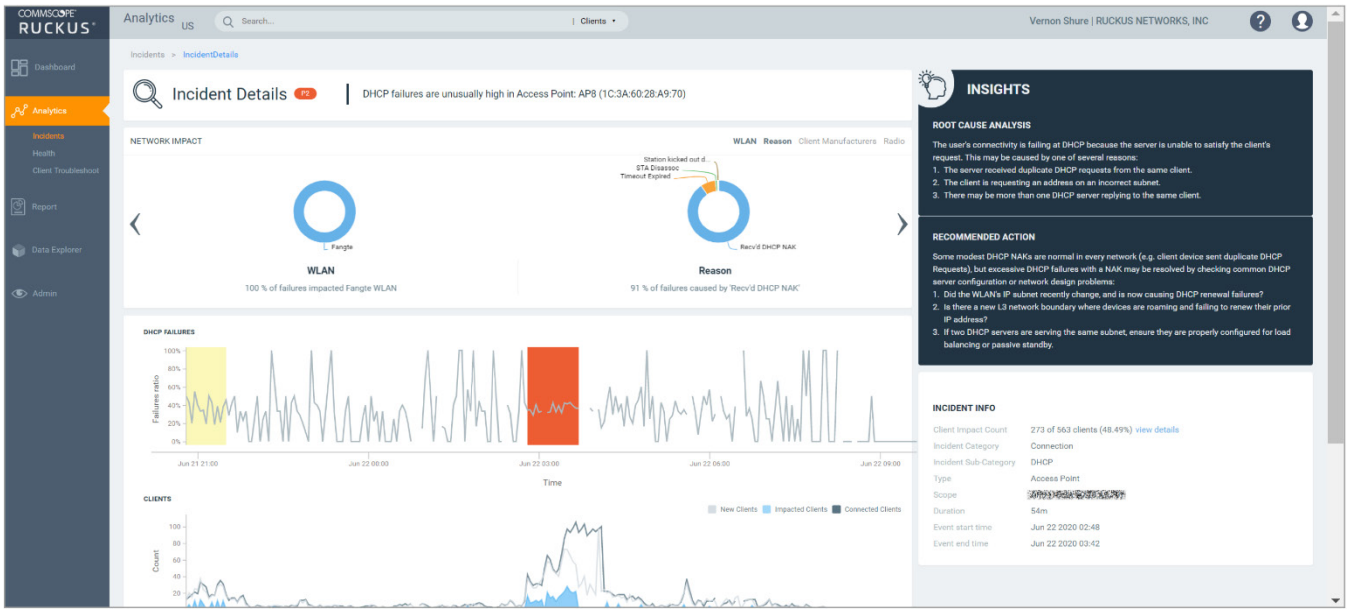


Incident Analytics

RUCKUS Analytics enables machine-assisted proactive networking for your RUCKUS deployment. It automatically establishes a normal range of behavior for each network element, without requiring any input from IT. Then it uses machine learning to automatically identify service incidents related to connectivity, performance and infrastructure that affect user experience. It uses artificial intelligence to classify service incidents by severity—so you can address the highest-priority issues first.

The system provides details for each incident, including:

- Root cause and recommended action
- Affected areas (client operating system types, access point models, firmware versions, WLANs and more)
- Other impact details, including severity, client impact and duration
- List of impacted clients
- Presentation of the underlying data that drives the incident



As dependency on technology in education increases, administrators need better understanding of the impact of downtime has on the learning experience. Setting Service Level Agreements (SLA) in RUCKUS Analytics allows IT staff and administrators understand the impact of the network on the learning experience. With additional insight into the health of a network, staff can identify and resolve issues before they become service impacting and users start to complain.

Additional information on RUCKUS Analytics can be found here https://www.commscope.com/product-type/enterprise-networking/service-assurance-network-intelligence/network-analytics/

Small School Example

Middle of Nowhere School District is a small district in a rural setting. Their budgets are small, their student population is representative of that, and their IT budget and staff are smaller still. Even though *Middle of Nowhere School District* doesn't have the student population, the classroom density, or the budget of larger school districts, the process is still the same.

Overview

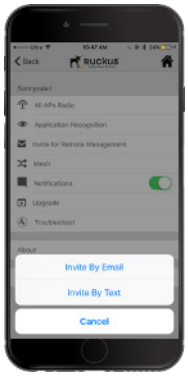
In meeting with district administrators, the local channel partner determined their requirements and has suggested that instead of a passive site survey being performed, a physical walk of the space where wall attenuation measurements are taken and wiring as well as installation challenges are noted.

Since a passive site survey wasn't performed, but attenuation measurements of some of the walls were taken, the designer can prepare of a predictive design to ensure the requirements defined by the district is met. The predictive design showed the location the APs should be placed as well as recommended channel and power settings. Transferring this AP design to a Visio design the partner can indicate IDF locations for ICX switches. From this plan the district can work with the partner to locate additional network items like cameras, printers, and desktop computers.

Proposed Solution

To help this district save on budget, the partner has recommended the following:

- RUCKUS R510 Access Points
- RUCKUS Unleashed Controller-less management
- RUCKUS ICX-7150 switches positioned in IDF



The RUCKUS R510 Access Point is an 802.11ac Wave 2 AP, proven and reliable, this AP will be in service for years to come. To manage the network RUCKUS Unleashed has been suggested. Simple to install, straightforward to configure, simple to manage, big on features. With built-in features such as Guest Services, DPSK security, Zero Touch IT onboarding and Application Visibility, RUCKUS Unleashed is a solution that fits all of their needs. For a switching Infrastructure the RUCKUS ICX 7150-24P placed in the IDF's and a RUCKUS ICX 7150-24F in their MDF is recommended.

With both wired and wireless networks being managed from the Unleashed dashboard, or the free mobile app, this allows the administrators to focus on what they need to, but still allows for assistance if the need ever arises, even from their mobile devices. As with all RUCKUS products, if the requirements change and a different solution is needed in the future, their investment is protected. Their system can be migrated to a Cloud based or full-scale controller solution without needing to purchase new equipment.

Example BOM

Qty	SKU	Description
1	9U1-R510-XX00	Ruckus Unleashed 802.11ac Wave 2 dual-band concurrent 2.4 GHz & 5 GHz, MU-MIMO, BeamFlex, PoE in, USB port. Does not include DC power supply
1	ICX 7150-24P-4X10G	ICX 7150 standard switch, 24+2 x 10/100/1000 PoE+ ports, 4x 1/10G SFP/SFP+ uplink/stacking ports, 370W PoE budget, L2 (switch image only)
1	ICX 7150-24F-4X1G	ICX 7150 standard switch, 24 100/1000 SFP ports, 2 x 10/100/1000 uplink RJ45 ports, 4 x 1/10G SFP/SFP+ uplink/stacking ports
As Needed	ICX7150-C10ZP-2X10G	10x RJ45 multigigabit ports, including 8× 2.5 GbE ports and 2x 2.5/5/10 GbE ports. 2× 1/10 GbE uplink/stacking SFP/SFP+ ports. 240W PoE budget. Delivers up to 90W per port on 4 PoH 802.3bt ready ports. Fanless.

Mid-Size School Example

Outskirts of Something School District is a mid-sized district on the outskirts of a large metropolitan city. While not as large as districts found in urban settings, they are a bit bigger than *Middle of Nowhere* with a larger student population to match. While not a large IT staff, they have some knowledge, ability, and the desire to manage and maintain their system in house.

Overview

Following the same approach, their partner sits down with them and comes up with the following plan. Along with a site walk, an AP on a Stick survey will be performed in critical areas to assist the designers in the final predictive design. This hybrid approach allows for the best of both worlds.

With the results from the APoS provided to the designer, the predictive design can be tuned to ensure the design is as close to the actual real-world environment as possible. As before, the predictive design showed the location the APs should be placed as well as recommended channel and power settings. Transferring this AP design to a Visio design the partner can indicate possible IDF locations for ICX switches. From this plan the district can work with the partner to locate additional network items like cameras, printers, and desktop computers.

Proposed Solution

Taking everything into consideration the partner, in this case, suggests the following solution:

- RUCKUS R550 APs
- RUCKUS Cloud Controller
- RUCKUS Analytics
- RUCKUS ICX Switches

The RUCKUS R550 Access Point is an 802.11ax, Wi-Fi 6 AP, cutting edge with built-in BLE and Zigbee radios, this AP represents where technology is going. To manage the network RUCKUS Cloud has been suggested. RUCKUS Cloud is a converged network management-as-a-service platform that enables IT to deliver exceptional user experiences, simply. With RUCKUS Cloud, “lean” IT organizations can easily provision, manage, optimize, and troubleshoot a high-performance enterprise wired and wireless network via a single web dashboard or native mobile application. With built-in features such as Guest Services, DPSK security, Zero Touch IT onboarding and Application Visibility, RUCKUS Cloud is a solution that fits all of their needs.

For a switching Infrastructure the RUCKUS ICX 7150-24P placed in the IDF's and a RUCKUS ICX 7650-48F in their MDF is recommended.

RUCKUS Analytics is a cloud service for network intelligence and service assurance. Powered by machine learning and artificial intelligence, it gives IT staff comprehensive visibility into network operations. With built in reporting features, automated health monitoring, advanced client troubleshooting, and more, RUCKUS Analytics is a powerful tool that allows IT administrators to focus on the highest priority issues to ensure that learning time isn't impacted by networks problems.

With both wired and wireless networks being managed from the Cloud dashboard, or the mobile app, this allows the administrators to focus on what they need to, utilizing the subscription aspect of RUCKUS Cloud to maintain critical infrastructure and 24 x 7 support. As with all RUCKUS products, if the requirements change and a different solution is needed in the future, their investment is protected. Their system can be migrated to a SmartZone controller solution without needing to purchase new equipment.

Example BOM

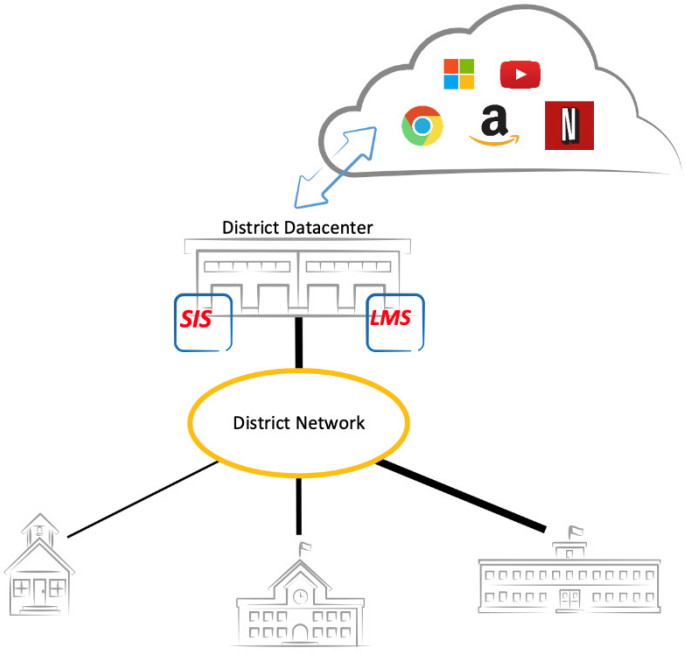
Qty	SKU	Description
As Needed	901-R550-XX00	Ruckus R550 dual-band 802.11abgn/ac/ax Wireless Access Point with onboard BLE/ZIgbee, 2x2:2 streams (2.4GHz/5GHz) OFDMA, MU-MIMO, BeamFlex+, dual ports, 802.3at PoE support. Plenum Support. Does not include power adapter or PoE injector.
1 per AP	CLD-RKWF-X001	RUCKUS Cloud Wi-Fi Subscription license. 1, 3, 5 years available, replace "X" with the years needed
As Needed	ICX7150-48PF-4X1G	ICX 7150 Switch, 48x 10/100/1000 PoE+ ports, 2x 1G RJ45 uplink-ports, 4x 1G SFP uplink ports upgradable to up to 4x 10G SFP+ with license, 740W PoE budget, basic L3 (static routing and RIP)
1 per Switch	CLD-MS71-X001	RUCKUS Cloud Switch Subscription license for ICX 7150 switch. 1, 3, 5 years available, replace "X" with the years needed
As Needed	ICX7650-48F	24x 100/1000 SFP ports, 24x 1G/10G SFP+ ports, 1 slot for 1x 100G or 2x40G or 4x10G front facing module, 4 rear facing QSFP ports for stacking/uplink
1 per Switch	CLD-MS76-X001	RUCKUS Cloud Switch Subscription license for ICX 7650 switch. 1, 3, 5 years available, replace "X" with the years needed

Large School Example

Middle of Everything School District is a large school district located in a large metropolitan area. This district has many schools spread out across a densely populated area. Their needs, along with their campuses, are complex and diverse. With a full IT staff, *Middle of Everything* brings a skill set to the table that is unmatched in the world of K – 12 education. While fully capable, *Middle of Everything* still knows it pays to work with a partner to leverage additional knowledge and experience when it comes to their upcoming network refresh.

Overview

Following their initial meeting with the district, their partner recommends a variety of surveys in different locations to ensure that when complete, the systems meets all of their needs. Passive site surveys for locations that have an existing network, but complaints are starting to come in, and site walks for others. Once these initial surveys are completed, the information is handed off to designers to prepare a predictive design. The designers request APoS surveys for specific locations to ensure the predictive design is correct, adjusting their predictive models to match what is discovered during the APoS surveys. Due to the size and complexity of this project, the partner also suggests validation surveys be completed after the new network is installed to ensure that *Middle of Everything School District* can hit the ground running when the doors open for the new school year. Even as an extra step with extra time and extra cost, it is an assurance to the district that what they expected is delivered.



Proposed Solution

As part of this design, the partner recommends the following solution:

- RUCKUS APs depending on the location and requirements with the R750, R650, and R550 for indoor locations and the T750 and T610 for the outdoor locations.
- RUCKUS virtual SmartZone – Essentials (vSZ-E) controller located in their district data center to manage each school independently based on their needs.
- RUCKUS Analytics to assist the IT staff.
- RUCKUS Cloudpath for onboarding staff, student, and guest devices.
- RUCKUS SPoT for tracking interactions
- RUCKUS IoT for sensor tracking (vaping)
- RUCKUS ICX switches

Leveraging the extensive portfolio of Wi-Fi 6 access points that RUCKUS brings to the table, the designers can provide a good mix of indoor and outdoor proven access points to facilitate wireless connectivity for any environment. Connecting to a virtual SmartZone – Essentials controller located in the district data center allows for IT staff to manage the entire district from a single control plane in a high availability configuration. Coupled with RUCKUS Analytics the network team will be able to solve most issues before they arise to the level of a call to the Service Desk.

With additional requirements comes additional solutions in the form of RUCKUS Cloudpath, a subscription service that assists in connecting devices to the network, from staff to students to guests, all devices are connected in the appropriate manner and given access only to what is defined in the policy. Cloudpath can be

hosted by RUCKUS using subscription licenses or hosted on-premises with subscription licenses and support licenses. RUCKUS SPoT allows for location tracking of devices to facilitate contract tracing in a time when that concept is becoming more and more important. With the addition of the RUCKUS IoT controller for IoT devices, the district can leverage the latest technology in not only running the network but also their buildings. These IoT devices include, but aren't limited to, smart lights, smart locks, asset tracking tags, and vaping sensors.

For ICX switches, the proposal calls for RUCKUS ICX7150-C10ZP switches located in classrooms, connecting to ICX7750-48F switches in strategically located IDF's, connecting to ICX7850-32Q located in the campus MDF which connects back to the district data center also using ICX7850 switches. This model of adding compact switches in each classroom allows for quick and easy copper cable runs to support anything needing in the classroom, aggregating in the IDFs before connecting to an MDF at the "core" of the campus network. From this core connections can be made to the internet for online content or to the district data center if needed.

With such a diverse and varied deployment, the ability to manage this network can seem overwhelming, but utilizing the RUCKUS SmartZone and IoT controllers allows IT staff to manage the network with relative ease. When needed, RUCKUS Analytics can be integrated to proactively spot troubles and allow staff to resolve problems before they become service impacting.

Example BOM

Qty	SKU	Description
1	L09-VSCG-WW00	Virtual SmartZone 3.0 or newer software virtual appliance, 1 instance, includes 1 AP license. Need to purchase RTU support license to continue using vSZ beyond 90 days
As Needed	901-R750-XX00	Ruckus R750 dual-band 802.11abgn/ac/ax Wireless Access Point with Multi-Gigabit Ethernet backhaul and onboard BLE/ZIgbee, 4x4:4 streams (5GHz) 4x4:4 streams (2.4GHz), OFDMA, MU-MIMO, BeamFlex+, dual ports, 802.3at PoE support. Does not include power adapter or PoE injector. Includes Limited Lifetime Warranty.
As Needed	901-R650-XX00	Ruckus R650 dual-band 802.11abgn/ac/ax Wireless Access Point with Multi-Gigabit Ethernet backhaul, 4x4:4 + 2x2:2 streams, OFDMA, MU-MIMO, BeamFlex+, dual ports, PoH/uPoE/802.3at PoE support. Does not include power adapter or PoE injector. Includes Limited Lifetime Warranty
As Needed	901-R550-XX00	Ruckus R550 dual-band 802.11abgn/ac/ax Wireless Access Point with onboard BLE/ZigBee, 2x2:2 streams (2.4GHz/5GHz) OFDMA, MU-MIMO, BeamFlex+, dual ports, 802.3at PoE support. Does not include power adapter or PoE injector. Includes Limited Lifetime Warranty.
As Needed	901-T750-XX01	Ruckus T750 802.11abgn/ac/ax Outdoor Wireless Access Point, 4x4:4 Stream, Omnidirectional Beamflex+ coverage, 2.4GHz and 5GHz concurrent dual band, (1x) 2.5G Ethernet port, (1x) 10/100/1000 Ethernet port, 100-240 Vac, POE in and PSE out, Fiber SFP/SFP+, GPS, IP-67 Outdoor enclosure, -40 to 65C Operating Temperature.
As Needed	901-T610-XX01	Ruckus T610s 802.11abgn/ac Wave 2 Outdoor Wireless Access Point, 4x4:4 Stream, MU-MIMO, 120 degree sector Beamflex+ coverage, 2.4GHz and 5GHz concurrent dual band, Dual 10/100/1000 Ethernet ports, POE in, IP-67 Outdoor enclosure, -40 to 65C Operating Temperature. Includes standard 1-year warranty. Mounting kit sold as separate accessory (902-0125-0000)
As Needed	902-I100-WW00	Ruckus IoT Module with Zigbee or BLE for 802.11ac APs
As Needed	ICX7150-C10ZP-2X10G	10x RJ45 multigigabit ports, including 8× 2.5 GbE ports and 2x 2.5/5/10 GbE ports. 2× 1/10 GbE uplink/stacking SFP/SFP+ ports. 240W PoE budget. Delivers up to 90W per port on 4 PoH 802.3bt ready ports. Fanless.
As Needed	ICX 7750-48F	48×1/10 GbE SFP+ ports and 6×40 GbE QSFP ports
As Needed	ICX 7850-32Q	32x 40/100 GbE QSFP28 ports can be split into 128x 10/25 GbE ports with breakout cables. 2x hot-swappable load sharing power supplies and 6x hot-swappable fan assemblies

1	L09-VSPT-WW00	Virtual Smart Positioning Technology (vSPoT) Base software platform as a virtual appliance, one (1) instance license, perpetual
As Needed	L09-0001-VSPT	Virtual Smart Positioning Technology (vSPoT) AP management license for one (1) AP, perpetual
2	LS9-vCLP-WW00	Cloudpath base on-site server software as a virtual appliance, one (1) instance license. No user licenses included. No support required. Server license is valid as long as user licenses are attached to it. Supports 5000 SMS messages per year, per customer. 20,000 user licenses per VM More servers may be necessary for high availability design or for additional capacity.
As Needed	L09-CLE0-XXXX	Cloudpath perpetual per-user on site license – replace "X" with total user count needed
As Needed	801-CLEz-XXXX	Cloudpath per-user support for perpetual license – Replace "z" with 1, 3, or 5-year access, "X" with total user count needed
2	L09-VSPT-WW00	Virtual Smart Positioning Technology (vSPoT) Base software platform as a virtual appliance, one (1) instance license, perpetual
As Needed	L09-0001-VSPT	Virtual Smart Positioning Technology (vSPoT) AP management license for one (1) AP, perpetual
As Needed	CLD-ANAP-X001	RUCKUS Analytics subscription license, 1 per AP and/or Switch – Replace "X" with 1, 3, or 5-year subscription

Example Summary

The previous examples are just that, examples showing different scenarios. As no two locations are the same, the final design for each network won't be the same, and the goal isn't to say that it should be. What is the same, across locations big and small, is the approach and the steps followed to achieve a design that meets the defined requirements for *that* location. Small schools may need a full empirical survey and vSZ clustering for redundancy. The large school might not have the budget for an APoS survey and chose to go with a Cloud controller solution. The takeaway should be to make sure that the design implemented meets all the requirements that are defined at the beginning of the project. If all of the requirements defined are met then it is a good design, regardless of the particulars of the chosen hardware.

Configuration Best Practice

As networks have evolved from having one computer in each classroom to every person having 3 network capable devices and the entire classroom being connected, so has the complexity of configuring the network to support the numerous devices and traffic requirements seen today. Configurations and settings can appear overwhelming but will fall into one of 3 settings:

- WLAN Settings
- Radio Settings
- ICX Settings

WLAN settings covers best practices for WLANs. This is how traffic really makes the transition from the radio to the ethernet port. Radio settings cover best practices for managing the RF spectrum and ICX settings discusses best practices to support a wireless infrastructure.

WLAN and radio settings are located on the Master AP for Unleashed and the controller for Cloud and SmartZone and will differ slightly between them on how they are configured. For details on how to configure

them see the user guide for each deployment. Depending on the deployment model, ICX settings can be done on either the switch Command Line Interface (CLI) or a controller User Interface (UI). For this document the CLI will be used.

WLAN Settings

WLAN settings are things that are done on a per SSID basis, not necessarily on the radio side, that is covered in the next section.

Band Specific WLAN

When creating a WLAN for staff, students, or BYOD, set the WLAN to only be used on 5 GHz. This reduces the chance that devices will connect to 2.4 GHz and result in a poor performance. For guest networks that are generally best effort services, it is OK to use these as dual band to reduce issues with any guest devices that might be used that don't support 5 GHz, the 2.4 GHz option is there.

Also, not all IoT devices used in the enterprise will support the 5 GHz band. Investigate all devices that will be used on the network to determine if there are any critical devices that only support 2.4 GHz to ensure they have the coverage needed.

Use Separate VLANs for each Use Case

Referenced earlier in Table 4: WLAN & VLAN Assignment it is important to separate out the traffic into its own respective VLAN. By separating out the traffic into separate VLANs it allows the wired network to work more efficiently and cuts down on Layer 2 broadcast storms. Using dynamic VLAN assignment and a pool of VLANs can also help segment the traffic even further.

VLAN 1, as the default VLAN, should not be used for any services. Using other VLANs allows for greater control of where the data is allowed to go without the fear of the default VLAN not being removed from all uplinks and unused ports.

Do Not Hide the SSID

Hidden SSID's are a relic from a previous age of "security". The misconception is that by hiding the SSID it added to the "security" of the network by not allowing others to discover it in the clear. In order for a device to join the network, the SSID would need to be typed into each device, making it more difficult to join. The irony of this is malicious devices can simply scan for the probes of the devices trying to join that network and see the SSID in plain text.

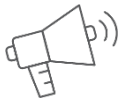
Set WLAN to OFDM Only

Orthogonal Frequency-Division Multiplexing, more commonly known as OFDM, settings on the WLAN prevents older devices from joining and slowing the network down. OFDM has been in Wi-Fi since 802.11a in 2001 and 802.11g in 2003. 802.11b is the only protocol that doesn't use OFDM as the basis of transmitting. 802.11b uses Direct-Sequence Spread Spectrum (DSSS) defined in the original standard. DSSS is inherently slow and hasn't been solely supported in any device since 802.11g was introduced in 2003. Setting a WLAN to OFDM Only essentially prevents 802.11b devices from joining the network and dramatically slowing the network down.

BSS Minimum Basic Rate

The Basic Service Set (BSS) Minimum Basic Rate (MBR) defines the rate, or speed, at which the beacon and other management frames are transmitted from the AP. It also defines the minimum rate the client needs to achieve to be allowed to join the WLAN. Default minimums are at the lowest rate for the frequency band but by raising these rates to 12 Mbps can help achieve a better-defined operating cell. 12 Mbps and 24 Mbps are recommended since 18 Mbps isn't supported by all client devices. 18 Mbps can be enabled but shouldn't be mandatory.

As clients reach the edge of a coverage area and downshift their transmitted rates, the AP can inform the client that disassociation is immanent and force the client to look for a better AP to connect to. Since a well-designed network should support a much higher rate across the entire coverage area, this can help prevent "sticky clients" or clients that don't like to roam and will stay connected to an AP long after they should have roamed to a new AP.



RUCKUS TOP TIP!

While the settings listed here are important, there are other setting that are not listed here that can affect the operation of the WLAN after installation. Refer to the Configuration and User Guide for the controller solution selected for further configurations. These guides can be found at https://support.ruckuswireless.com

Radio Settings

These are settings that are specific to the radio on the AP and will impact all SSID's that are on that AP or radio. Changes here are best viewed as controlling the RF spectrum of the solution. These settings can be derived directly from the predictive design done earlier in the process, but during fine tuning of the network after installation these are steps that can be taken to improve performance as needed.

Adjusting radio settings can be an iterative process; repeated over and over as adjustments are made. This is easiest done during the predictive design phase but depending on the accuracy of the attenuation values used during the predictive design, the post installation radio tuning can be either short and sweet or a long drawn out process.

Turn the power down on the 2.4 GHz radio

By nature, the 2.4 GHz signal will propagate further than a 5 GHz signal. Since most devices are 5 GHz capable, and designs are done around the 5 GHz signal, the 2.4 GHz signal can overpower the 5 GHz design. Client devices are not governed by any industry standard to design for so each client can behave differently, even from the same manufacturer.

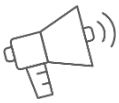
Turn off the 2.4 GHz radio

Many networks are "fixed" after deployment by adjusting the 2.4 GHz spectrum. With only 3 or 4 non-overlapping channels, depending on regulatory domains, it is very easy to end up with Co-Channel Interference (CCI) in the 2.4 GHz spectrum. Many times, it is found that even after turning down the transmit power on the 2.4 GHz radios, turning off many of the 2.4 GHz radios is found to be the solution. After turning power down, and then turning radios off, go back and adjust the 2.4 GHz transmit power back up where needed to compensate for the radios that were turned off.

Auto Radio Settings

RUCKUS offers a couple of different methods when it comes to allowing the system to control these RF settings "automagically," if you will. Whether or not these auto RF tools are enabled or not depends on a number of factors that are beyond the scale of this document. There is not a "one size fits all" answer to these questions, but some factors that come into question are:

- The size of the network. Smaller networks are easier to manually set everything based on the predictive design. Larger networks are harder to manually set both transmit power and channel on every AP, making the auto RF features more enticing.
- Administrator expertise. Some locations have the expertise on staff to manage the network and make future adjustments as needed, some do not. Unfortunately, the smaller the network, the less likely the needed expertise exists on staff to manage the RF, leading to auto RF being enabled.
- Risk acceptance. Many times, new installations are "fixed" shortly after system turn-over to the operators by someone else coming in and turning off the automatic RF features and setting everything manually. If the ability to accept the risk exists, then it is something to be considered. If the risk is too great that auto radio settings will cause issues during operation, then it's best to disable them.
- Implementors ability. It is generally accepted that most default settings for any auto RF feature from any vendor isn't the best practice, for anything. If auto RF is turned on and used, ensure that the settings are adjusted for that specific network. Every network is unique, ensure the settings for the auto RF features are as well.



RUCKUS TOP TIP!

The best practice is to ensure a sound RF design ahead of time instead of relying on software adjustments during final tuning of the system. While helpful, these software adjustments are meant for solving small issues, not fixing a flawed RF design.

The previous statement also assumes that a proper RF design was possible. When the "Best Practices" can't be followed in real world scenarios, don't be afraid to use software tools as needed.

There is a reason why Wi-Fi Professionals over use the term "It depends" as real world scenarios often prohibit best practices.

Best practice for auto channel and transmit power settings will be different for each network. Care needs to be taken to ensure the balance between functionality and a stable operational network.

ICX Settings

ICX settings are what is configured on the switch side to support the wireless infrastructure. What used to be a novelty system that utilized the wired infrastructure, wireless has almost become the primary focus of the wired infrastructure and ensuring that the wired network is up to the task is critical. The following are representative of any system and accomplished from the CLI of the switches.

Switch Port Commands

These are the commands that can be entered on ICX switches to can improve the functionality and stability of the network. These can be general switch commands or port specific commands.

Link-Layer Discover Protocol

Link-Layer Discovery Protocol (LLDP) is the vendor-agnostic industry standard in which network devices exchange information about their own system properties. This exchange is conducted over Layer 2 and generally over an Ethernet network. One of the common uses of LLDP is the ability to identify devices that are connected to a network switch. This protocol also provides additional information about device capabilities. For LLDP to work as intended, it should be supported and enabled on connected devices. Information exchanged by LLDP can be also used by network management applications and by automation scripts.

LLDP is running automatically in code versions 08.0.90 and later but can be verified by entering the "**lldp run**" command followed by "**show lldp".** The "**end**" command is issued to exit all configuration while the **"exit"** command is used to back out of configuration items one at a time.

```
ICX7150-24P Switch#configure terminal
ICX7150-24P Switch(config)#lldp run
ICX7150-24P Switch(config)#end
ICX7150-24P Switch#show lldp
      LLDP transmit interval      : 30 seconds
      LLDP transmit hold multiplier  : 4 (transmit TTL: 120 seconds)
      LLDP transmit delay       : 2 seconds
      LLDP SNMP notification interval : 5 seconds
      LLDP reinitialize delay     : 2 seconds
      LLDP-MED fast start repeat count : 3

      LLDP maximum neighbors      : 2048
      LLDP maximum neighbors per port : 4
```

Power over Ethernet

Best practice is to not change any PoE settings for ports connected to RUCKUS Access Points (APs). RUCKUS APs and switches will set appropriate power automatically. You should ensure LLDP is running to maximize communications between devices.

Distributing PoE Devices

Though a switch may be PoE capable on all switch ports, it may not be able to deliver full power to each simultaneously. You should distribute your Powered Devices evenly across your switches, and within individual switches. This reduces the load on the switches.

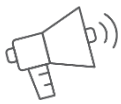
The PoE Budget

PoE best practices includes planning to ensure that the switches are able to deliver power to all connected devices and within the power budget of the switch. PoE budgets need to be carefully planned and monitored. In many cases, the default settings are sufficient. There may be instances when you want to amend the PoE settings, but ensure you understand the ramifications of the changes before proceeding.

PoE Power Options

PoE is enabled by default to all PoE capable ports on switch boot. However, RUCKUS recommends the following:

- Disable PoE power from ports that do not require it: no inline power
- Assign a priority to specific ports: inline power priority [priority] – 1 through 3, with 1 being highest
- Power should be limited to provide only the amount required to power the PD
    - Limit PoE Power by Class: **inline power-by-class** [*class*] – 0 through 4
    - Limit PoE Power to a maximum value: **inline power limit** [µWatts]



RUCKUS TOP TIP!

If the overall PoE budget of the switch becomes an issue, ensure devices that are the highest priority are set to **"inline power priority 1"** to prevent other devices plugged in later from "stealing" the power from devices with a higher priority.

Port Status

Newer Access Points require 1 Gbps connections to the network infrastructure. While most new switches have standardized on 1 Gbps connections, if not more, across the board, a post-installation inspection can reveal that isn't always the case. Using the command "**show interface brief**" on each switch will show if there are any devices that connected at less than 1 Gbps. Connections to APs that show a speed of 100 Mbps or less (see Figure 8: show interface brief below) can indicate a problem on the cable infrastructure between the switch and the device at the other end. An AP showing a connection speed of 100 Mbps or less can lead to performance problems on the WLAN in that area.

```
SSH@7150-C12#sh int brief

Port      Link     State    Dupl Speed Trunk Tag Pvid Pri MAC             Name
1/1/1     Up       Forward  Full 1G    None  No  9    0   609c.9fe7.1f84
1/1/2     Down     None     None None  None  Yes 1    0   609c.9fe7.1f85
1/1/3     Up       Forward  Full 100M  None  No  9    0   609c.9fe7.1f86
1/1/4     Disable  None     None None  None  No  888  0   609c.9fe7.1f87
1/1/5     Disable  None     None None  None  No  888  0   609c.9fe7.1f88
1/1/6     Disable  None     None None  None  No  888  0   609c.9fe7.1f89
1/1/7     Disable  None     None None  None  No  888  0   609c.9fe7.1f8a
1/1/8     Disable  None     None None  None  No  9    0   609c.9fe7.1f8b
1/1/9     Up       Forward  Full 1G    None  No  9    0   609c.9fe7.1f8c
1/1/10    Disable  None     None None  None  No  888  0   609c.9fe7.1f8d
1/1/11    Disable  None     None None  None  No  251  0   609c.9fe7.1f8e
1/1/12    Up       Forward  Full 1G    None  Yes 251  0   609c.9fe7.1f8f
1/2/1     Up       Forward  Full 1G    None  No  9    0   609c.9fe7.1f91
1/2/2     Up       Forward  Full 1G    None  No  251  0   609c.9fe7.1f92
1/3/1     Disable  None     None None  None  No  888  0   609c.9fe7.1f93
1/3/2     Disable  None     None None  None  No  888  0   609c.9fe7.1f94
mgmt1     Disable  None     None None  None  No  None 0   609c.9fe7.1f84
```

Figure 16: show interface brief

It is also best practice to include a name for the switch port. If there had been a name associated to port 1/1/2 in the example above, it would be easier to identify the device on the other end that is down. Without a name, it is hard to tell if the device connected to 1/1/3 is an AP or different kind of device, one that might not be capable of 1 Gbps connection. Future troubleshooting time might be spent only to realize that the cable infrastructure is good; the device is only capable of 100 Mbps. Also, without names for the ports, it isn't clear which port is being used to connect to other switches in this network.

Cable Diagnostics

On ICX switches running FastIron (FI) version 08.0.20 or later, there is a cable diagnostics command that can be used to test connections to a switch that are suspect. Available from the privileged EXEC mode (accessed by using the "**enable**" command), this allows administrators to run a quick test of the cable to check for issues that may be present. This command is not meant to replace proper cable testing tools, just allow for a quick check without needing to dispatch a technician.

The commands used for this "feature" are as follows from the EXEC mode:

- `clear cable-diagnostics tdr` STACKID/SLOT/PORT (This clears out any previous test to ensure only recent results are presented)
- phy cable-diagnostics tdr STACKID/SLOT/PORT
- show cable-diagnostics tdr STACKID/SLOT/PORT

Administrators can use the "show" command first and if there are results present, they can either use those results or use the "clear" command referenced above to ensure that the results shown are the most recent. See Figure 9: cable-diagnostics.

```
SSH@7150-C12#show cable-diagnostics tdr 1/1/2
No TDR data on port 1/1/2

SSH@7150-C12#phy cable-diagnostics tdr 1/1/2
SSH@7150-C12#show cable-diagnostics tdr 1/1/2

Port    Speed   Local pair      Pair Length     Remote pair     Pair status
----    -----   ----------      -----------     -----------     -----------
1/1/2     1G    Pair A          10-50M          Pair B          terminated
                Pair B          10-50M          Pair A          terminated
                Pair C          10-50M          Pair D          terminated
                Pair D          10-50M          Pair C          terminated
```

Figure 17: cable-diagnostics

Had there been an issue with the cable itself, the status column would show a different status like "open" or "short."

VLAN Usages

As discussed earlier, use VLANs to segment traffic, with management traffic also segmented off in its own VLAN. VLAN 1 shouldn't be used for anything due to its default nature and possibility of being allowed to route to places it isn't allowed by policy. Separate VLAN's for the different types of traffic allows the ICX infrastructure to operate as intended and allow for better management and identification of the traffic that is utilizing the wired network.

It is also best practice to use a "dummy" VLAN for any unused ports (seen as VLAN 888 in Figure 8: show interface brief). These dummy VLANs should never be allowed on the connection to another switch or anywhere else in the network. This added step of assigning a dummy VLAN to an unused port that is disabled prevents a device that gains physical access to this port to communicate with any other device should the port be enabled by accident. For switches located in classrooms, this could be a final safeguard should an unauthorized device or person access the physical location of the switch.

Unless a full-blown Network Access Control (NAC) is in place, these best practices of physically securing a switch, disabling any unused ports, and using dummy VLANs are layers of network security that need to be in place to safeguard against unauthorized network access. While settings like these can impede troubleshooting or quick deployments later, that is nothing compared to the results and liability if an unauthorized person or device gaining access to the network.

Port Security

While disabling unused switchports and using dummy VLANs are best practices for unused ports, there are also steps that can be taken to help secure ports that are in use. These are for locations that don't have a full NAC solution, which is outside the scope of this document, but are still serious about securing the network.

These settings can be broken down into both global configurations and port specific configurations.

Global Switch Configurations

These commands are entered from the global configuration prompt of "`switch#configuration terminal`". The variables for these commands need to be discussed with the network administrators before implementation.

- Set RSTP
  - Assessing correct weight to the switch
- errdisable recovery cause all
- errdisable recovery interval 60 (in seconds)
- port security
  - enable
  - autosave (value of 15 – 1440 seconds)
  - maximum (number of secure MAC addresses that can be configured.)
  - ip icmp attack-rate burst-normal (value 20-10000000 kbps) burst-max (value 20-10000000 kbps) lockup (value in seconds)
  - ip icmp attack-rate burst-normal 5000 burst-max 10000 lockup 300
  - ip tcp burst-normal (value in seconds) burst-max (value in packets) lockup (value in seconds)
  - ip tcp burst-normal 30 burst-max 100 lockup 300
  - violation
    - protect (Hard drop of packets from violating MACs and do not shut down the port.)

  - restrict (Drop packets from violating MACs and shutdown the port if violating MAC count exceeds 128. Value of 0 – 1440 minutes; 0 = permanent)
  - shutdown (Shut down the port for a specified time period on violation. Value of 0 – 1440 minutes; 0 = permanent)
- ip arp insection vlan (vlan to inspect)
- ip dhcp snooping vlan (vlan to inspect)

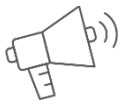
For all entries, the "**no**" command can be used to clear entries and ensure that all values are saved using the "**write mem**" command.

Port Specific Configurations

These commands are entered in the configuration mode for a specific port from the prompt `(config)#interface ethernet` STACKID/SLOT/PORT

- ip arp inspection (add/remove trust)
- ip dhcp snooping (add/remove trust)
- broadcast limit 8192

Also, care needs to be taken when using port security on ports connected to APs. With APs running in local breakout mode, the switch port will see multiple mac addresses; this is normal. For other devices, like cameras, printers, or IoT sensors, only a single MAC address should be seen.



RUCKUS TOP TIP!

Securing the network should never be taken for granted. Whether it is physical security of the hardware and ports or secure onboarding of clients, securing networks is a never-ending exercise of checking and double checking. While some items may seem small, it can be the smallest things that can trip up malicious actors attempting to access a network without authorization.

Summary

RUCKUS Networks Transforming School Networks

Today's school district administrators face a far more complex set of challenges than they did even a decade ago. In addition to providing a top-notch education, they must also ensure the safety and security of their students, faculty and staff in an unfortunately more complicated world. In the education space.

RUCKUS Networks elevates the digital learning experience with safe and reliable network access. The classroom of tomorrow promises an amazing education. Blended learning, flipped classrooms, video delivery of digital curriculum, video conference and other modern learning models can better engage students and help educators be more effective. We power the modern classroom with grade-A Wi-Fi and edge switching performance coupled with simple, market-leading secure onboarding and policy management. With the addition of the RUCKUS IoT suite, that grade-A network can be leveraged to improve safety, lower facilities costs and reduce administrative and IT overhead.

RUCKUS solutions are part of CommScope's comprehensive portfolio for Enterprise environments (indoor and outdoor).

We encourage you to visit **commscope.com** to learn more about:

- RUCKUS Wi-Fi Access Points
- RUCKUS ICX switches
- SYSTIMAX and NETCONNECT: Structured cabling solutions (copper and fiber)
- imVision: Automated Infrastructure Management
- Era and OneCell in-building cellular solutions
- Our extensive experience about supporting PoE and IoT

COMMSCOPE®

commscope.com

Visit our website or contact your local CommScope representative for more information.