

# Best Practice Design Guide

Designing for Hospitality  
December 2020

# Table of Contents

**INTENDED AUDIENCE ..... 4**

**OVERVIEW ..... 5**

**OVERVIEW ..... 6**

**Recommended Tools .....7**  
 Intangi Iris..... 7

**Gather Requirements.....8**  
 Brand Standards ..... 8  
 End User / Property Owner ..... 8  
 Consultants..... 8  
 Collecting Site Data ..... 9

**Property Types.....9**  
 Resort / Village ..... 9  
     Key Points ..... 9  
 City / Urban Hotel..... 10  
     Key Points ..... 10  
 Heritage Building ..... 11  
     Key Points ..... 11  
 Student Residence / Serviced Apartments / Continuing Care Retirement Communities ..... 12  
     Key Points ..... 12

**Designing for Area Types ..... 13**  
 Guest Rooms ..... 13  
     Access Points..... 13  
     Uplink Medium ..... 14  
     Hallway Deployments ..... 19  
     Uplink for a New Build or Major Refurbishment ..... 20  
     Fiber to The Room (FTTR) ..... 21  
 Public Areas ..... 23  
 Conference Spaces ..... 26  
     Wi-Fi Capacity Sizing ..... 26  
     Wi-Fi AP Placement..... 28  
     Wired Capacity..... 29  
     Cabling ..... 30  
 Elevators..... 31  
     Elevator Method A: Travelling Cable using Fiber (Recommended) ..... 31  
     Elevator Method B: Travelling Cable Using Legacy Cabling ..... 32  
     Elevator Method C: Wireless Bridge using Mesh..... 33  
     Elevator Method D: Wireless Point to Point bridge..... 35  
 Back of House (BOH) / Staff-only areas ..... 36  
     AP Locations..... 36  
     Key Points: ..... 37

Designing for Hospitality

- AP Positioning ..... 38
- Outdoor ..... 39
  - Factor in Trees and Foliage ..... 39
  - Fiber Uplink for Outdoor APs ..... 40
  - Mesh Uplink for Outdoor APs ..... 41
  - Mobile Hotspot (Chauffeur Cars / Golf Carts)..... 41
- Switching Design.....46**
  - Access (IDF) Switches ..... 46
  - Power (POE) Requirements ..... 47
  - ICX Power Supply Options ..... 48
  - Stacking vs Uplinks ..... 48
  - Stacking Cables and Optics ..... 49
  - Part Numbers for ICX 7150 Switches..... 49
  - Warranty..... 50
- Infrastructure Design .....51**
  - New Construction..... 51
  - Refresh ..... 51
- Network Management (Controller).....54**
  - Choosing the Right Management (Controller) Platform ..... 55
    - Examples ..... 56
  - Ruckus SmartZone ..... 57
    - Scalability – AP and ICX Switch Management Slots ..... 58
    - Scalability - Clustering..... 58
    - Scalability – Multi-Site Clustering for Geographical Redundancy..... 59
    - Scalability – Calculating Management Bandwidth..... 59
    - Tunneling ..... 60
    - Building the SmartZone Bill of Materials ..... 61
  - Ruckus Unleashed ..... 64
    - Ruckus Unleashed Multi Site Manager (UMM) ..... 65
  - RUCKUS Cloud ..... 65
- APPENDIX – MISCELLANEOUS TOPICS ..... 66**
  - Painting Access Points.....66**
    - Painting an Indoor Access Point ..... 66
    - Painting an Outdoor Access Point ..... 66
    - Official CommScope Warranty Statement ..... 67
      - Why Does the Warranty Not Cover Painted Products? ..... 67
    - CommScope Powered Fiber Cable System (PFCS)..... 68
    - Why (not) PON/GPON/GEAPON? ..... 71
  - Glossary.....73**

## Intended Audience

This document addresses factors and concerns related to designing a wireless network for hospitality environments. Many factors can affect both the initial work and final performance. These are considered here.

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 document provides network designers, architects, and WLAN professionals guidance for designing a wireless network for hospitality environments. This document is one in a series of best practice guides. This document is the second in a series of Best Practice Design Guides created for the Hospitality market. Please reference the full suite of Best Practice Guides for Hospitality.

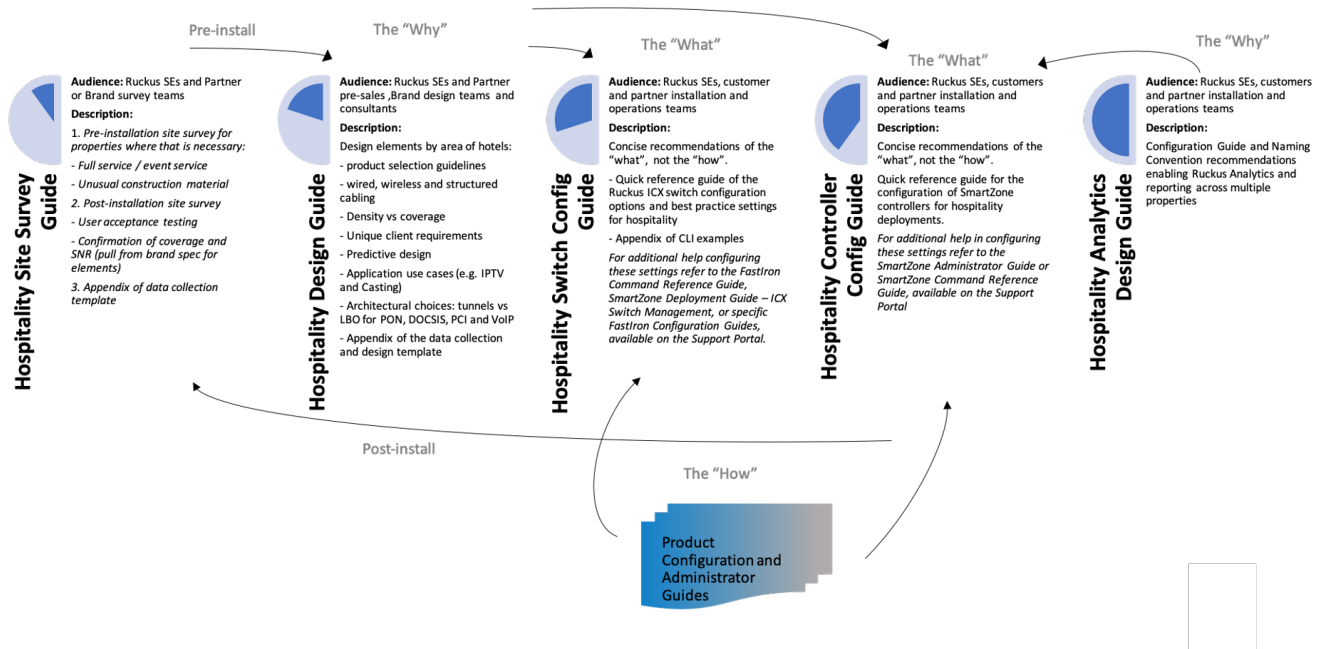


FIGURE 1: SUITE OF BEST PRACTICE GUIDES FOR HOSPITALITY

This document is intended to provide guidance to Hospitality Managed Service Providers to ensure consistency and optimal performance of deployed RUCKUS WLAN infrastructures across properties.

This document is one in a series of Best Practice Guides specific to the Hospitality vertical. Please refer to the other documents to provide a more complete picture. The intended audience for this body of work includes Ruckus Systems Engineers and customer and/or partner installation and operations teams. These documents are intended to primarily cover the "What" and some of the "Why", not necessarily the "How", when it comes to configurations. Ruckus provides separate additional resources, both in the form of online and offline configuration guides, internal/partner support portal knowledge base, and How-to videos posted to YouTube. Partners can always engage Ruckus Systems Engineers or Field Engineers with questions or assistance as needed.

## Overview

This is a guide to aid with designing connectivity throughout a building which will be accepting guests soon.

This is distinctly different from designing networks for the traditional corporate environment where there is full control over the type of devices connecting to the network. In a Hospitality environment, you have no control over the type, age and quality of the devices that guests will bring in. The network needs to support every single device that a guest brings in.

This guide is aimed at helping you build a complete network design from scratch. There are also many nuances to each design which would be impossible to cover in a single document. For the sake of simplicity, the tone of this document will be biased towards a new network deployment in a new building, but the methods and processes can be easily adapted to refurbishments or extensions of existing networks.

## Recommended Tools

Throughout this document there will be references to a few tools used to design a Hospitality network. This is not comprehensive and there may be alternative similar tools to deliver the same result.

### Intangi Iris

The Intangi Ecosystem is a vendor-neutral configuration, design, and quoting platform where network engineers use the same set of tools to efficiently communicate product and pricing data, tear down vendor-specific silos, reduce barriers of entry for new resellers, and ultimately increase the effectiveness of resellers, distributors, and manufacturers.

Tutorial: <https://www.youtube.com/playlist?list=PLjrT0rvTWLtXNav7gHRpNXHj4ZwFZUBZE>

Cost: Free (must be a Ruckus certified partner).

Visit <https://www.intangi.com/register.php> to register for access.

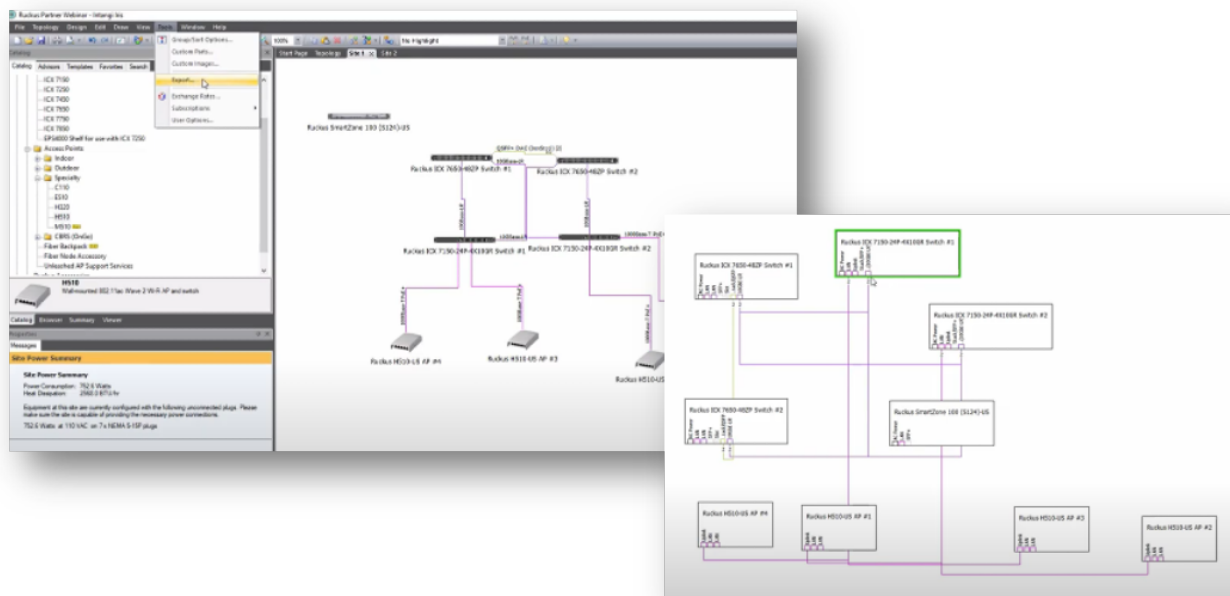


FIGURE 2: INTANGI INTERFACE

## Gather Requirements

### Brand Standards

Many brands have documented standards, which should always be adhered to when designing a network for a branded property. If you are working on a branded property, ask your customer if there are any brand standards you should be following.

Different brands have different levels of detail that vary from very simple guidelines (E.g., requiring -65dBm signal in all guest-accessible areas) to having very strict ones (E.g., specific AP placement locations, naming conventions, cabling requirements, specific switch models and switchport configurations to use).

Note: Always abide by the brand standards, even if it directly contradicts what is specified in this design guide.

### End User / Property Owner

Even if the brand standards are very specific, ask the customer a few questions to make sure you are designing the network to meet their expectations. Do not be alarmed if the customer is not very clear on the technical requirements. Use your expertise and this document to guide the process.

Here are a few sample questions to ask:

- Which areas of the hotel are in scope and which are not?
- Which areas do you expect the heaviest guest and staff traffic?
- Which areas will be open to the public and which areas will be restricted to staff only?
- Is there a particular technology that may be added now or in future (E.g., voice control, intelligent lighting, temperature/humidity monitoring and control, smart door locks, staff alert, etc.)?
- What is the expected opening date?

### Consultants

There might be a consultant involved in the process. Just as with the end user/owner, make sure you speak to them as they may be aware of other technologies being implemented that need support from the network. Pay particular attention to applications that are highly mobile, such as:

- Staff mobile terminals running applications such as HotSOS or similar applications
- Third-party IPTV systems
- IP-based CCTV systems
- PoE driven information screens or terminals requiring high power PoE.
- Wi-Fi-based VoIP handsets

Most consultants will already be familiar with the RUCKUS recommended design and any brand standards that will need to be followed. Stay in close contact during the design process as they can be a strong asset.



## Collecting Site Data

If this is an existing structure, you need to have a good understanding of the building. The construction style, materials used, and possible cable paths will directly impact the design and can change the entire design.

A site survey should already have been done using the Site Survey for Hospitality Best Practice Design Guide. It is the first document in this Hospitality suite of documents. Use the output of that guide to understand the environment and design for the building.

## Property Types

### Resort / Village

A resort is normally made up of several buildings: independent villas, event centers, restaurants and a central administration area (which is often where the core data center is located).



FIGURE 3: RESORT PROPERTIES

Due to the distances involved and because a significant portion of the cable paths are located outdoors, the infrastructure to support such a property usually relies heavily on fiber cabling and outdoor hardware. For very large resorts, expect to find multiple datacenters spread across different zones.

Finally, keep in mind the operating temperature range of outdoor components. Many resorts are located in locations with temperature extremes (both hot and cold), so any outdoor equipment, including cabling, must be rated to withstand these temperatures.

### Key Points

- Focus on fiber connectivity (cabling, switches)
- Identify suitable locations for outdoor APs
- Watch out for temperature ranges



## City / Urban Hotel

Hotels located in city centers are more of a ‘vertical-build’ hotel and tend to be more compact with symmetrical floors and symmetrical or mirrored room layouts. Often this type of hotel is entirely indoors, in some cases the only outdoor area of the hotel is a rooftop pool.



FIGURE 4: URBAN PROPERTIES

Due to the shorter distances and all-indoor environment, most of the cabling used is copper. The main challenge is finding appropriate cable paths as well as managing interference from neighboring Wi-Fi networks while minimizing signal leakage to neighboring properties and the streets surrounding the property.

### Key Points

- Mostly copper
- Identify cable paths and riser locations
- Try to minimize RF leakage outside the building

## Heritage Building<sup>1</sup>

This type of property would be of significant historic value or of architectural importance, which severely restricts what kind of alterations are allowed. Structural changes (E.g., drilling holes through walls to lay new cable paths) might not be permitted. Aesthetic standards (E.g., APs may need to be completely hidden or blended into the environment) are likely to be strictly enforced.



FIGURE 5: HERITAGE PROPERTIES

In this type of building, especially if it is of historical significance, there may already be existing cabling that can be reused, such as Coax cable from a legacy TV system or CAT5/CAT5E from a legacy Wi-Fi network.

### Key Points

- Re-cabling may be cost prohibitive or simply not allowed
- Aesthetics may be critically important
- Study existing cabling (TV antenna Coax, old CAT5E cabling) for reuse possibilities

---

<sup>1</sup> This type of 'registered' building goes by different names in different countries, see [https://en.wikipedia.org/wiki/List\\_of\\_heritage\\_registers](https://en.wikipedia.org/wiki/List_of_heritage_registers)



## Student Residence / Serviced Apartments / Continuing Care Retirement Communities

This type of property hosts *residents*, rather than *guests*. The difference here is that users will bring in their own consumer devices such as voice-control speakers, content-streaming devices, smart TVs, printers, and game consoles.



FIGURE 6: RESIDENT PROPERTIES

These devices expect to connect to a standard home broadband network. Therefore, the network needs to be designed to replicate a home environment as closely as possible while still maintaining security and performance.

At the same time, any infrastructure hardware installed inside the resident's suite is vulnerable to malicious or inadvertent tampering. The network should be designed to isolate resident devices from the infrastructure and other residents' devices and to alert and recover should any infrastructure components be subjected to tampering or an attack.

### Key Points

- Residents will expect a same-or-better experience than they have at home with their home broadband
- Expect infrastructure components installed in resident suites to be tampered with



## Designing for Area Types

### Guest Rooms

In many cases, a property will have sets of guest rooms of equal shapes and sizes. Whether these are lodges in a forest, villas in a resort, or suites in a high rise. Identify each *type* of room and design connectivity for that room type. Once that is done, it is simply a matter of copying that design across all the other similar rooms.

#### Access Points

For a few years now, Wi-Fi design of a guest room based on having an AP inside the room. This all but guarantees great connectivity for guest devices and since in-room APs also have a network switch built-in, the in-room Wi-Fi AP becomes the connectivity hub of the room.

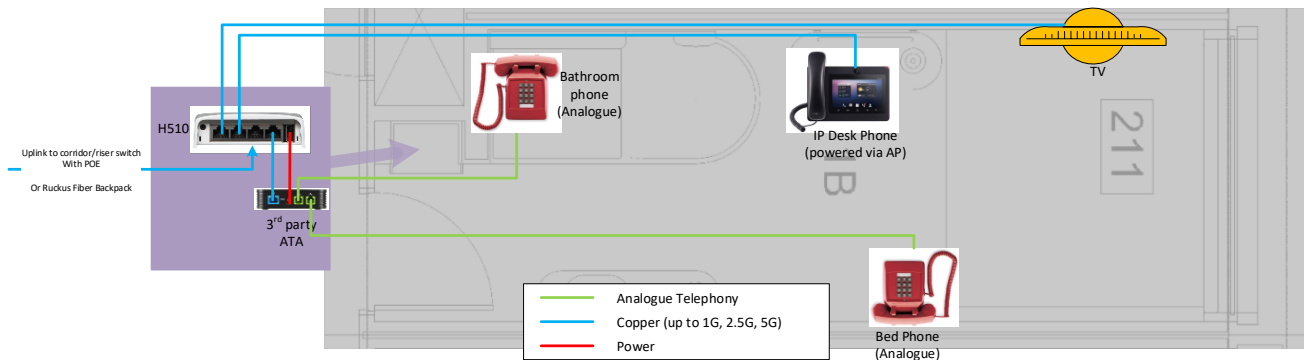


FIGURE 7: GUEST ROOM DEVICES

Using your site survey results and cabling plan, identify a few suitable locations within the room to place the AP and discuss with the customer about this placement.

A few locations where in-room APs are normally installed are:

- Below the desk
- Behind the TV / TV unit
- In a communications closet inside the room

The RUCKUS H series of wall plate access points and the C110 are designed to be installed over an in-wall electrical box<sup>2</sup> but these devices are larger than a standard outlet. Make sure the electrical box is installed with no obstructions around it, such as other electrical boxes, within 75mm / 3” of each side of the electrical box.

<sup>2</sup> This has many names across the world – Pattress, back box, wall box. Here we are referring to the box which is *inside* the wall and the light switch, power outlet or, as is in this case, the network outlet is mounted to.

The composite picture below shows the in-wall electrical box (black), the mounting bracket (metallic) and the H510 AP (white).



FIGURE 8: WALL MOUNTED ACCESS POINT

In the case of retrofits or locations where an in-wall electrical box is not possible, CommScope offers RUCKUS surface mount brackets for the H-series AP and the C110 which allows the APs to be mounted on a solid flat surface. Refer to the RUCKUS Accessory Guide to find the correct surface mount bracket for the AP being installed.

**Uplink Medium**

Until recently, the only option for connectivity to the room was through a UTP/FTP CATx copper cable between the room and an IDF. However, CommScope has explored other possibilities to ensure cable longevity, whether it is using existing coax cabling or installing new fiber cables.

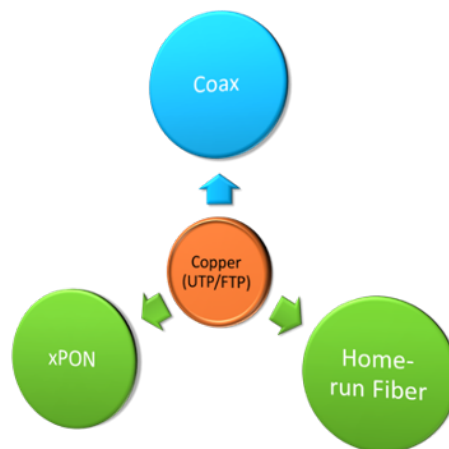


FIGURE 9: UPLINK MEDIA

Designing for Hospitality

Uplink for Retrofits

In retrofits, the choice of uplink primarily depends on what is already available in the room. Use the flowchart below to guide you on the possible approach.

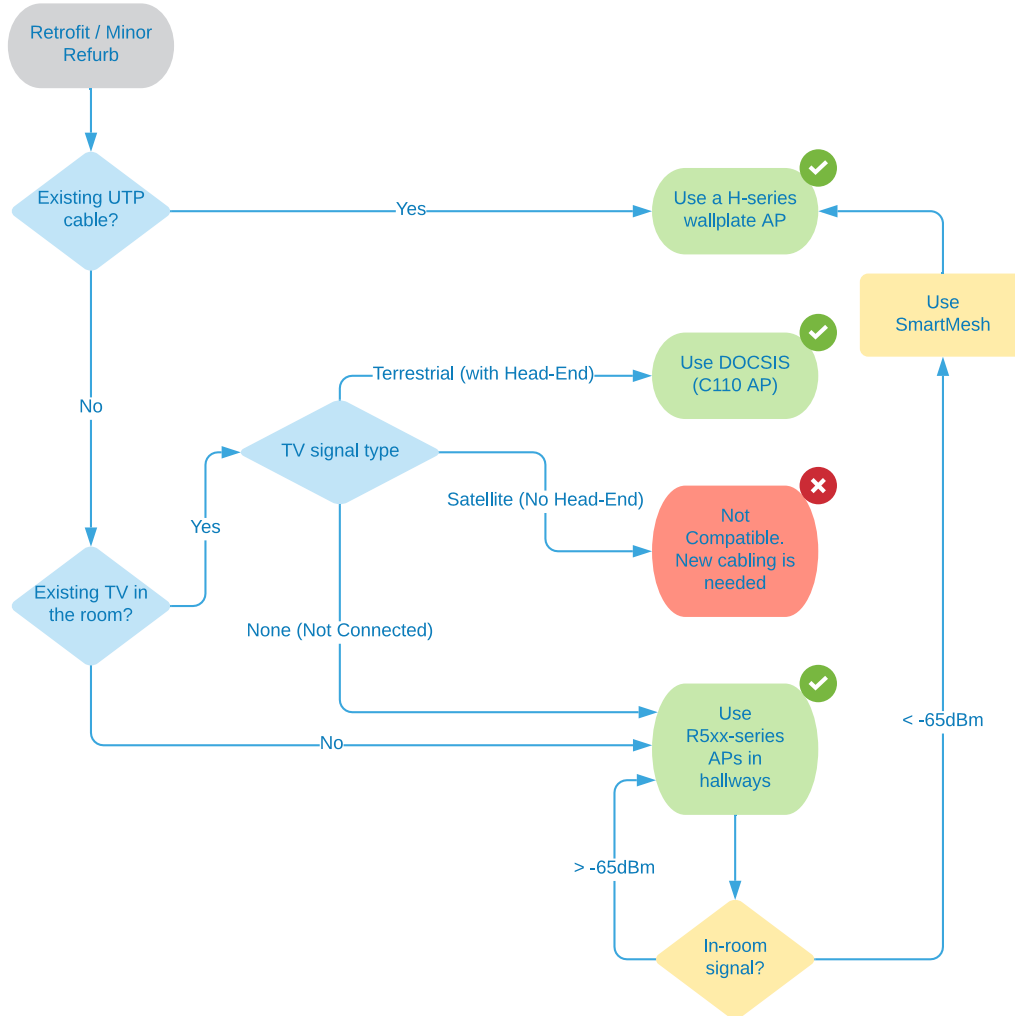


FIGURE 10: UPLINK FOR RETROFIT

If there is an existing UTP cable that is at least Category 5E (CAT5E), use an H-series AP connected to this cable. If the cable is already in use by a device (E.g., a TV or guest HSIA), this can be connected to one of the H-series downstream ports at the bottom of the AP.

If there is no UTP cable, check the TV. If this TV is connected to a head-end or centrally distributed antenna signal, this cable can be used for a DOCSIS deployment using the RUCKUS C110 as the AP and a miniCMTS installed next to the headend.

If all else fails, you may need to install APs in the hallways and ensure there is enough coverage within the rooms for good connectivity. CommScope recommends a minimum of -65dBm signal on both 2.4Ghz and 5Ghz. If the signal from the corridor APs does not penetrate into the room far enough, use an in-room H510 wall plate AP with SmartMesh enabled to repeat the Wi-Fi signal within the room.

## Designing for Hospitality

## Reusing Existing Coax Cable with DOCSIS

In properties with a working communal TV system (sometimes called SMA TV or a headend based TV system), the same coax cable can be reused for data using DOCSIS technology. DOCSIS has the advantage that it works alongside TV service, so there is no need to upgrade or modify the TV system in any way.

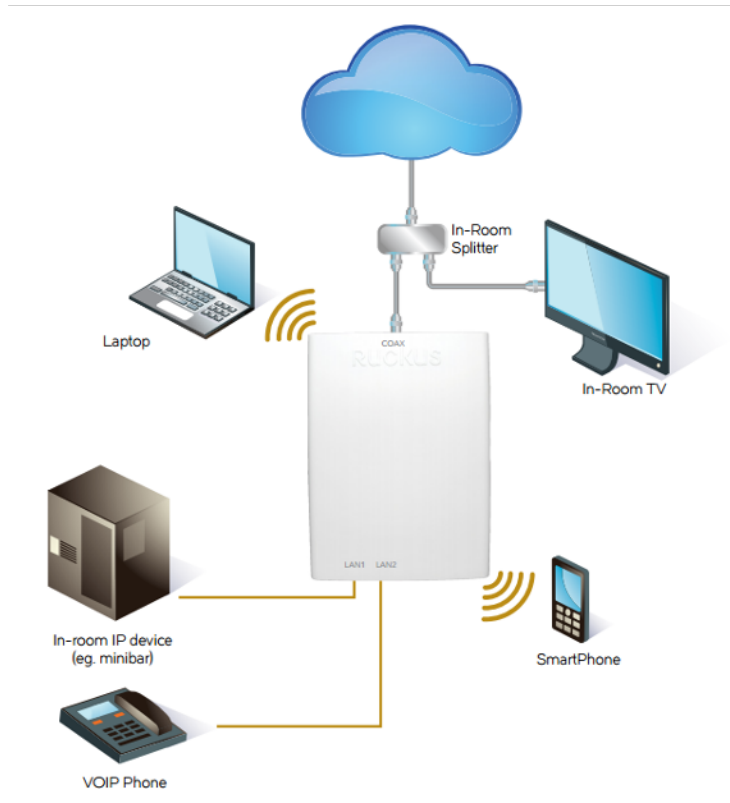


FIGURE 11: USING DOCSIS

The RUCKUS C110 DOCSIS AP is an all-in-one unit with an 8x4 DOCSIS 3.0 modem and a full-featured RUCKUS Wi-Fi AP. It also includes two 10/100 Mbps managed Ethernet ports which can be used for other wired IP systems in the room.

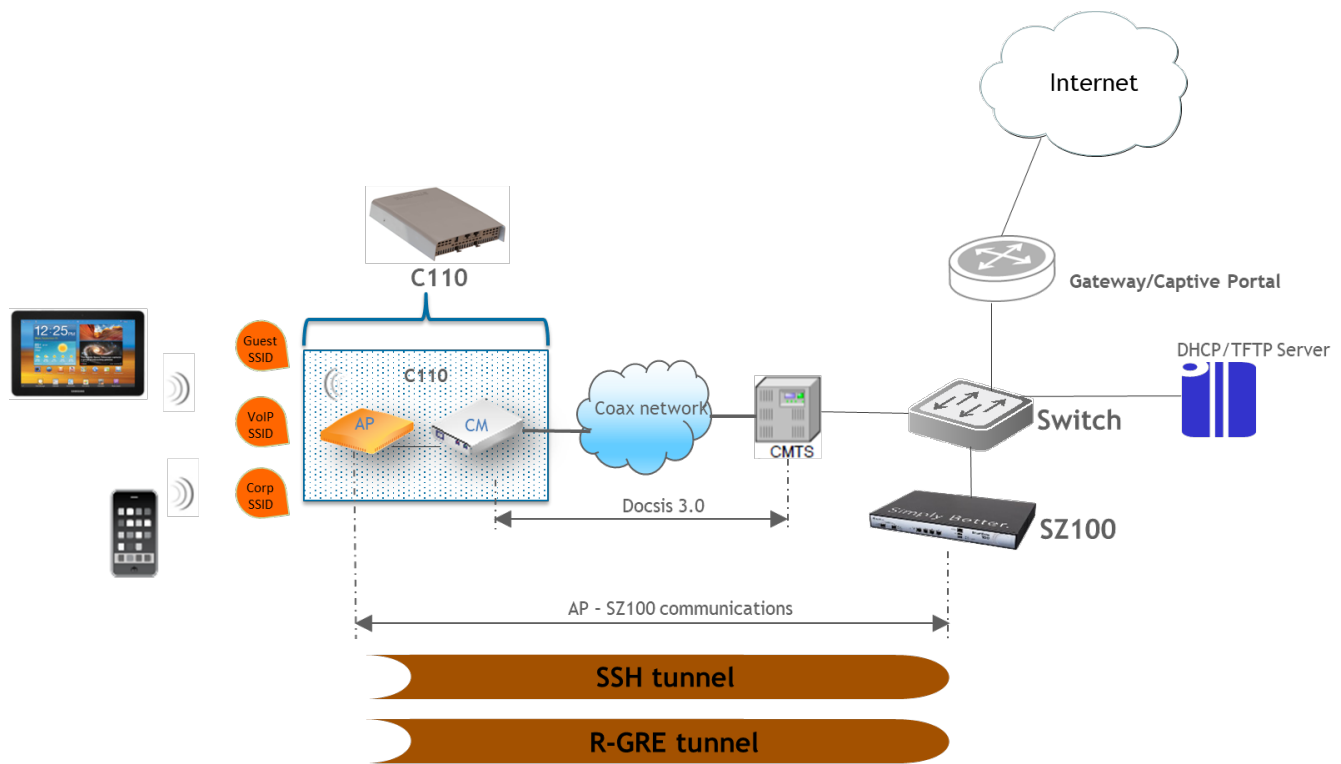


FIGURE 12: NETWORK ARCHITECTURE WITH DOCSIS

At the other end of the coax cable, you will need a miniCMTS, which is the central device doing double duty by converting the coax signals back to standard Ethernet while also managing the cable modem side of the C110.

A single miniCMTS normally manages 200-400 cable modems but check with your preferred miniCMTS vendor about this.

There are two important factors to keep in mind during design stage when considering DOCSIS:

- DOCSIS is a shared-access medium, which in best case has a total capacity as follows:

	Downstream	Upstream
DOCSIS (8x4)	304Mbps	108Mbps
EuroDOCSIS (8x4)	400Mbps	108Mbps

- The Ruckus C110 AP has a 8x4 DOCSIS modem, while a miniCMTS could support more channels (E.g., 16x8) which would allow load balancing of CMs across channel sets. In the example provided above, the miniCMTS could assign APs across 2 different channel sets, doubling the net available throughput.
- DOCSIS is designed for Layer 3

Designing for Hospitality

A DOCSIS modem and DOCSIS miniCMTS expects a service-provider style architecture where each cable modem is an independent subscriber running an independent network. Layer 2 roaming and handling hundreds of MACs on each endpoint is not the normal *modus operandi* of a DOCSIS network.

The solution is to tunnel all user traffic. All Wi-Fi traffic and preferably wired traffic should be encapsulated in a RUCKUS GRE tunnel so that the cable modem and miniCMTS will only ever see a single MAC and a single IP address on each cable modem.

If this is not possible, there are ways of tweaking the DOCSIS protocol to support traditional Layer 2 bridge architectures, but this is beyond the scope of this document.

**Key Points**

- One miniCMTS handles between 200-400 C110
- Always plan for a local tunnelling concentrator – either SZ-100/SZ-300 or vSZ-D
- DOCSIS bandwidth is shared. Some jitter is to be expected, may impact VoIP

Vendor	URL
Teleste	<a href="https://www.teleste.com/">https://www.teleste.com/</a>
Casa Systems	<a href="http://www.casa-systems.com/products/overview">http://www.casa-systems.com/products/overview</a>
Harmonic	<a href="http://harmonicinc.com/product">http://harmonicinc.com/product</a>
Pico Digital	<a href="http://www.picodigital.com/product-details.php?ID=miniCMTS200a">http://www.picodigital.com/product-details.php?ID=miniCMTS200a</a>
C9	<a href="http://www.c9networks.com/products.html">http://www.c9networks.com/products.html</a>
Vecima	<a href="http://www.vecima.com/portico/">http://www.vecima.com/portico/</a>
Blonder Tongue	<a href="https://www.blondertongue.com/bt-cmts-3210.html">https://www.blondertongue.com/bt-cmts-3210.html</a>
Technicolor	<a href="http://www3.technicolor.com/en/hi/minisites/open-software/cmc-mini-cmts-cable-modem-termination-system">http://www3.technicolor.com/en/hi/minisites/open-software/cmc-mini-cmts-cable-modem-termination-system</a>

TABLE 1: LIST OF RECOMMENDED DOCSIS MINICMTS VENDORS

## Designing for Hospitality

### Hallway Deployments

When installing APs in the room is not an option, the only alternative is to set them up in hallways between sets of rooms. This still works in many environments although it is not the preferred design.

This kind of design relies heavily on the site survey results. The site survey data determines how much attenuation (signal loss) the walls, doors, furniture and furnishings in and around the room cause.

#### How Many Rooms Can Each Hallway AP Cover?

While this is a very common question in this type of design, there isn't a straightforward answer because there are many factors to consider. Ballpark, in properties with more and smaller functional rooms, expect to cover 4-6 rooms (2-3 on each side) with one AP. In properties with larger or more luxurious rooms (E.g., marble bathrooms, full length mirrors), that number can easily go down to 2-3 rooms (1-2 on each side) per AP.

Use your preferred Wi-Fi planning tool together with the survey results to place APs in the hallways, ensuring -65dBm on both 2.4Ghz and 5Ghz at the far end of each room.

#### Mesh

If coverage from the hallway AP is not enough to reach the furthest end of the room, consider using a H5xx-series wall plate AP to create a mesh link with the corridor APs.



FIGURE 13: HALLWAY ACCESS POINTS



Designing for Hospitality

**Uplink for a New Build or Major Refurbishment**

In the case of new builds or major refurbishments, there is more flexibility in the type and location of cabling possible.

For small properties, such as boutique hotels and luxury homes, an all-copper network based on CAT6A UTP/FTP cable will provide the right balance between cost-effectiveness, ease of deployment and maintenance, and futureproofing.

In larger, more complex properties, take the opportunity to install fiber cabling from each guest room all the way back to the MDF. This avoids the need for intermediate switches and IDFs, which would require their own power and cooling and also take up space.

**Note:** CommScope recommends installing single-mode rather than multimode in hospitality environments. Even though it costs slightly more than multimode, single-mode virtually eliminates distance limitations since it can handle link lengths of 60 km / 37 miles or more. It is also the fiber of choice in the carrier GPON world, which means expertise and tools will be more readily available as more FTTH deployments are rolled out. See <https://www.commscope.com/blog/2019/choosing-to-deploy-single-mode-or-multimode-fiber-is-similar-to-flying-or-driving-for-vacation/> for more information.

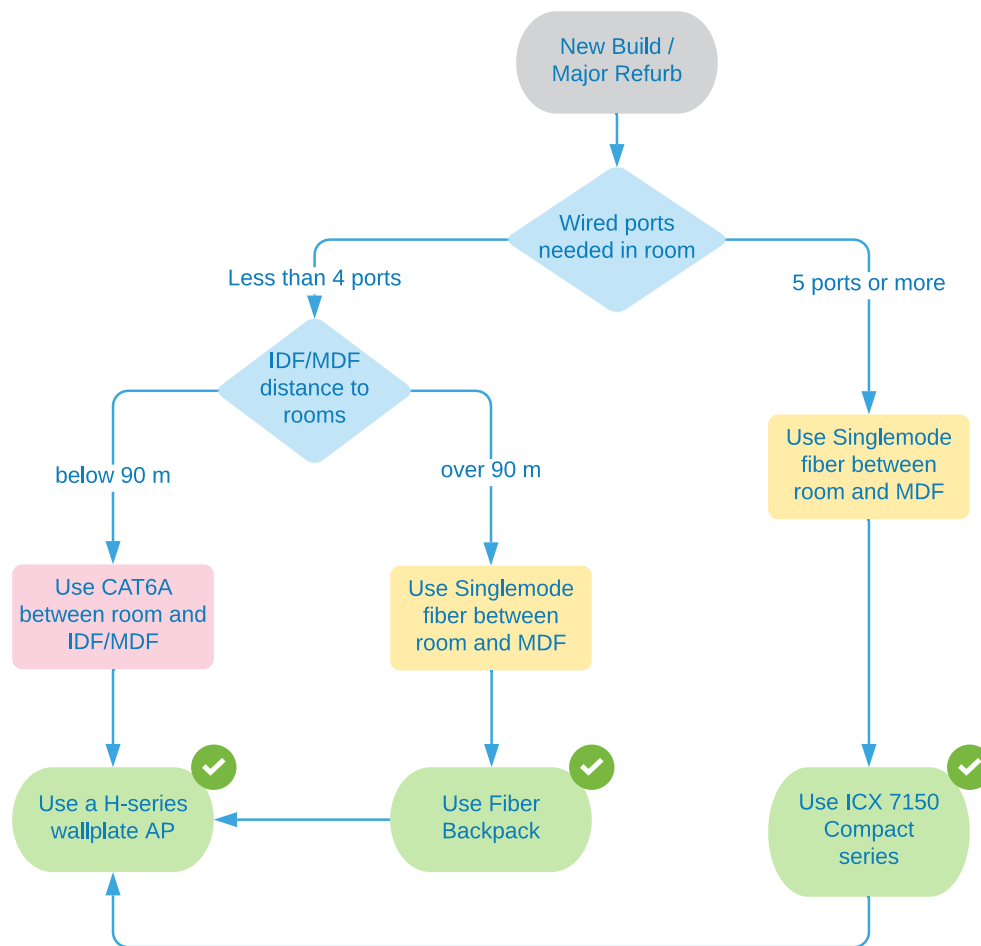


FIGURE 14: NEW BUILD UPLINK FLOWCHART



## Fiber to The Room (FTTR)

There is an increased interest in fiber-to-the-room (FTTR) architectures. Fiber has many advantages over copper, but it has two main disadvantages – cost and power.

### Pros and Cons

- Cost

Installing fiber is more expensive than copper. It's not the cable itself, in fact fiber cable is often cheaper to buy than good quality CAT6A. However, the tools needed to terminate and test fiber cable, as well as the expertise needed to properly install, terminate, and test fiber is more expensive.

The counterargument here is longevity. Fiber, especially single-mode fiber, has an almost infinite amount of bandwidth. Once installed it will not need to be replaced as bandwidth needs increase.

This means that, while CapEx is higher for fiber than it is for copper, fiber works is cost-effective than copper over the entire lifespan of the cable.

- Power

Unfortunately, technology has not (yet) beat physics, fiber cable cannot carry power in the same way we do POE on copper cables.

- However, this problem has been solved by the CommScope Powered Fiber Cable System (more about this in a [later section](#)).

### Fiber Architectures (Active Fiber vs PON)

When designing an FTTR architecture, design the network for Active Fiber using single-mode cabling. This way, every single room in the property can be run directly to the MDF, where a bank of network switches can be centrally powered, cooled, and monitored.

CommScope provides a wide range of fiber products, from simple patch cables to pre-terminated MPO-based multi-strand cable trunks. RUCKUS provides the active side of things including:

- ICX 7150-24F all fiber access switch
- Fiber Backpack adapter for the RUCKUS H510 AP



FIGURE 15: RUCKUS FIBER BACKPACK ADAPTER

PON architectures have gained traction in the industry with the promise of eliminating all active components outside the MDF. A small plastic, completely passive splitter is all that is needed to break out a single fiber into up to 64 fibers. With active fiber or copper, this would require an active network switch, complete with power and cooling.

While this may sound ingenious in theory, in practice PON is unsuitable for most Hospitality networks due to limitations in the PON protocol.

#### Key Point

CommScope does not recommend running an enterprise network over GPON, EPON, GEAPON or similar PON architectures. More info about this is in the [appendix](#).

## Public Areas

Public areas are common use spaces within hotels. These areas, such as restaurants, food and beverage service, lobbies, pool, spas, and play areas, are typically classified as mid-high dense areas. Public areas could accommodate between 10s to 100s of concurrent users depending on the size of the hotel.

Sufficient signal strength does not guarantee sufficient capacity. Although coverage can be fairly straight forward to cover an all-day dining area, there might be a need for more APs for capacity purposes to ensure each client will get a fair slice of bandwidth and speed. In public spaces, it is important to design based on both coverage and capacity. For example, a single outdoor AP might be enough to cover a pool area but may not be enough to accommodate the total number of concurrent users expected to be online at a time.

Here are a few steps and guideline to efficiently design and plan Wi-Fi for a hotel public space:

- Identify all public spaces on floor plans and layouts.  
Have a top eye view of all public spaces within a hotel. This is crucial and, depending on the size of the property, could be tricky. Some hotels have a simple lobby and an all-purpose hall; others have multi-floor areas and massive outdoor spaces.
- Ask the hotel representative to provide an estimate of the maximum number of concurrent clients at each space of public areas.  
Knowing the average number of connected devices at a given area will help plan the quantity and models of APs to be used.
- If the design is for an existing hotel, ask for a plan indicating existing cable locations.  
New Builds vs. Network Upgrades:  
It is trivial to add cable pulls in a new hotel build before walls are installed, but it could be a concern in existing hotels seeking to upgrade the Wi-Fi to the latest standards. This is especially troublesome in public areas as they are usually highly decorated and ceilings are not easily accessible. Having a layout that marks existing AP/cabling locations is a starting point to check if these locations can be utilized for the new Wi-Fi design. Based on the new design, identify any required cabling relocations or additional cable pulls.
- Plan for consistent coverage between major public spaces.  
Those are places where guests move to reach out to lobbies, pools, SPA, etc. This may include hallways, staircases, elevators, outdoor pathways.

Designing for Hospitality

- Check outdoor requirements.

In some hotels, specially resort type, outdoor areas are where most guests would spend their time during their stay. This would include swimming pools, beaches, tennis courts, aqua parks, outdoor F&B, etc.

CommScope provides multiple outdoor RUCKUS AP models and each series available in omni-directional and directional built-in antennas. In a typical hotel deployment, a mix between omni-directional and directional APs may be required. For example, APs mounted on walls covering front facing areas might be directional, while APs mounted around the pool might be omni-directional. Another use case for directional APs is to shoot coverage to terraces and balconies of the hotel. See the below sample design for illustration:

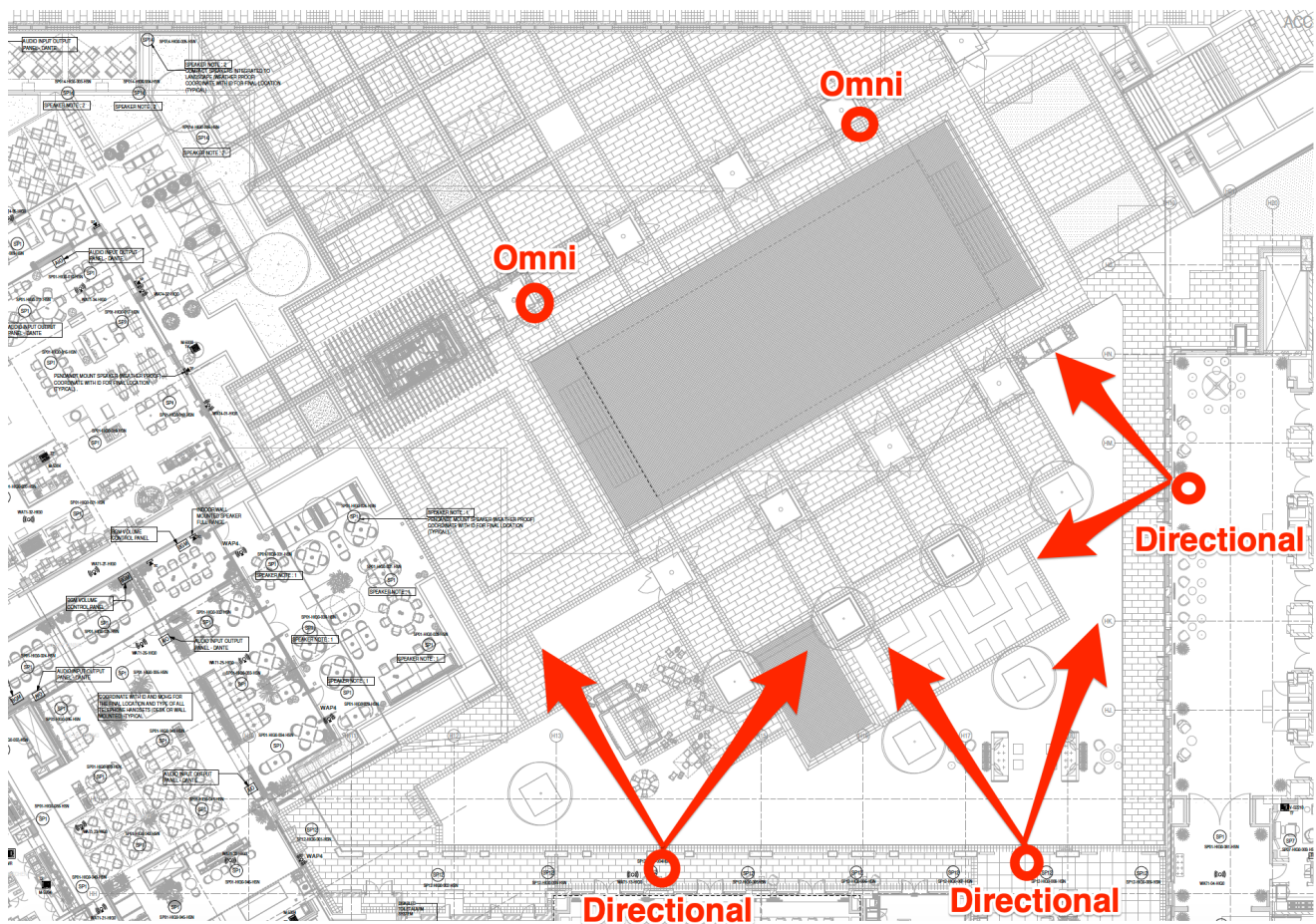


FIGURE 16: USING OMNI AND DIRECTIONAL ANTENNA ACCESS POINTS

Designing for Hospitality

- Plan AP models based on density of each area:

Area	R3xx	R5xx	R6xx	T3xx	T6xx	Remarks
Meeting rooms			x			
Restaurants		x				
Hallways	X					
Staircases	X					
Elevators	X					H510 can be used for switch ports
Main lobby			X			
Pool				x	X	
Beach area				x	X	
Terraces				X		
F&B				X		
SPA		x				

TABLE 2: AP MODEL BASED ON DENSITY



### Conference Spaces

Conference spaces can really be the stress test of a Wi-Fi network. However, somewhat surprisingly, this is the easiest area to design since it should be based on *capacity* rather than *coverage*.

This means that heatmaps and site surveys are of little use here. What is more important is to know how many devices will be used. Devices are carried by people, and what do people do in all conference spaces besides connect to Wi Fi? They eat and drink!

### Wi-Fi Capacity Sizing

The best source of information for determining capacity in a conference space is the Food & Beverage (F&B) team. They know the exact maximum capacities each venue can hold. Many times, this information is available even on the venue’s public website in the form of a capacity chart.

	Theatre	Classroom	Boardroom	Cocktail	Banquet
Great Dane Ballroom I	900	500	-	900	800
Great Dane Ballroom II	800	400	-	700	600
Great Dane Foyer	-	-	-	900	-
Doberman	40	30	20	50	40
Husky	40	30	20	50	40
Chihuahua	15	10	8	30	20

FIGURE 17: VENUE CAPACITY CHART

In this table, each row lists a meeting room, while the columns show the capacity of that room in different layouts (“Banquet” style with guests seated at round tables, “Theatre” style having only chairs, “Classroom” layout having alternating rows of tables and chairs, etc.).

This table is the starting point.

Simply take the “Classroom” layout capacity and divide by a value between 75 and 100. The resulting number will be the number of APs needed in that venue.

Dividing by 75 offers more capacity, while dividing by 100 is more cost effective. The determination of which number to use should be informed by experience, judgement, and a frank conversation with the customer to find the balance between the two.

$$APs\ needed\ for\ Meeting\ Space = \frac{Classroom\ Layout\ Capacity}{75\ (capacity)\ or\ 100(cost\ effective)}$$

#### Where does the 75 – 100 range come from? Why “Classroom” layout?

These venues are used for a multitude of event types and each has its own impact on the network. One day there could be a perfume trade show followed the next day by a technical conference, and then by a wedding. It is not possible to build a single design that is a perfect fit for every single event type, so design for the expected heaviest use of Wi-Fi.

A wedding may have more people than a technical conference, but not many people will be using the Wi-Fi network during the wedding. A technical conference will be full of geeks, potentially with multiple devices,

## Designing for Hospitality

including high performance laptops, tablets, and smartphones. The demands on the Wi-Fi network will be much higher during this kind of event.

Most technical conferences are held in the “Classroom” layout; assume that on average each participant will connect 2 devices. This means that the network should be designed for 150-200 devices per AP even though an AP can accept many more clients.

Consider the highest capacity of the room, which is often the “Cocktail”, this is normally double that of “Classroom”. However, in this situation people will usually only have a single device – their smartphone – so in the end the number of devices per AP still works out to around 150-200, with lots of capacity to spare to handle traffic spikes and roaming.

Conference spaces will often have large ballrooms, theaters or foyers as their main spaces, which are interspersed with clusters of small breakout rooms or boardrooms. When running the calculation described above, the larger spaces will need multiple APs, while the smaller rooms sometimes need less than half an AP.

As a rule of thumb:

- If a space needs 2 or more APs, use the high-end R7xx or R8xx range of APs as these are designed to handle very high densities and throughput.
- If a space needs between 0.5 AP and 1.99 AP, use a single R6xx or R7xx AP.
- If there are several adjacent spaces, with each space requiring less than 0.5 AP, either use a R5xx in each space, or use a single R6xx or R7xx AP shared between two spaces.

Pre-Function Areas will also need high-capacity Wi-Fi coverage since this is where people will congregate before and after an event and during breaks. Design for the number of connections, but use fewer APs here, for three reasons:

- Active usage will be low. Most people will be just passing through or networking rather than actively working on a connected device.
- People will be moving around. Fewer APs = less roaming = less management traffic.
- Fewer APs will allow more channel availability inside the meeting spaces.

## Designing for Hospitality

For Pre-Function Areas, the AP capacity can be doubled or even tripled compared to the meeting space APs. In this case, use the formula:

$$\text{APs needed for PreFunction Space} = \frac{\text{Maximum capacity of largest connected space}}{250}$$

- Obtain a capacity chart from the F&B team or property website
- For each space, use “Classroom” layout capacity and divide 75-100.
- If result is...
- $\geq 2$ , use R7xx or R8xx
- $0.5 < 1.99$ , use R6xx or R7xx
- $< 0.5$ , use R5xx in each space, or share R6xx/R7xx between two spaces

### Wi-Fi AP Placement

Once the number of APs needed in each space has been determined, most of the APs can simply be distributed throughout the space equally, with some exceptions:

- If there is a stage, make sure there is at least one AP immediately above or in the wings of the stage, as some conference organizers will want to create special SSIDs for presenters or streaming devices.
- Avoid placing APs in the main doorways. Doing this will result in the AP having to handle hundreds of roam events in a few seconds as guests are walking in and out of the space.
- Avoid placing APs too close to large columns or behind walls. Although this may seem like a good way to contain coverage within a specific area by using the structure’s attenuation, in reality it will only cause more retransmissions and interference due to the Hidden Node<sup>3</sup> effect.

---

<sup>3</sup> See [https://en.wikipedia.org/wiki/Hidden\\_node\\_problem](https://en.wikipedia.org/wiki/Hidden_node_problem)



Designing for Hospitality

Wired Capacity

Once the quantity and placement of the Wi-Fi APs is determined, plan the Wired network capacity. The need for high-speed connectivity during events is continuously increasing and newer high-density APs such as the R750 and R850 will easily exceed the capabilities of the humble 1Gbps 802.3af PoE switchport.

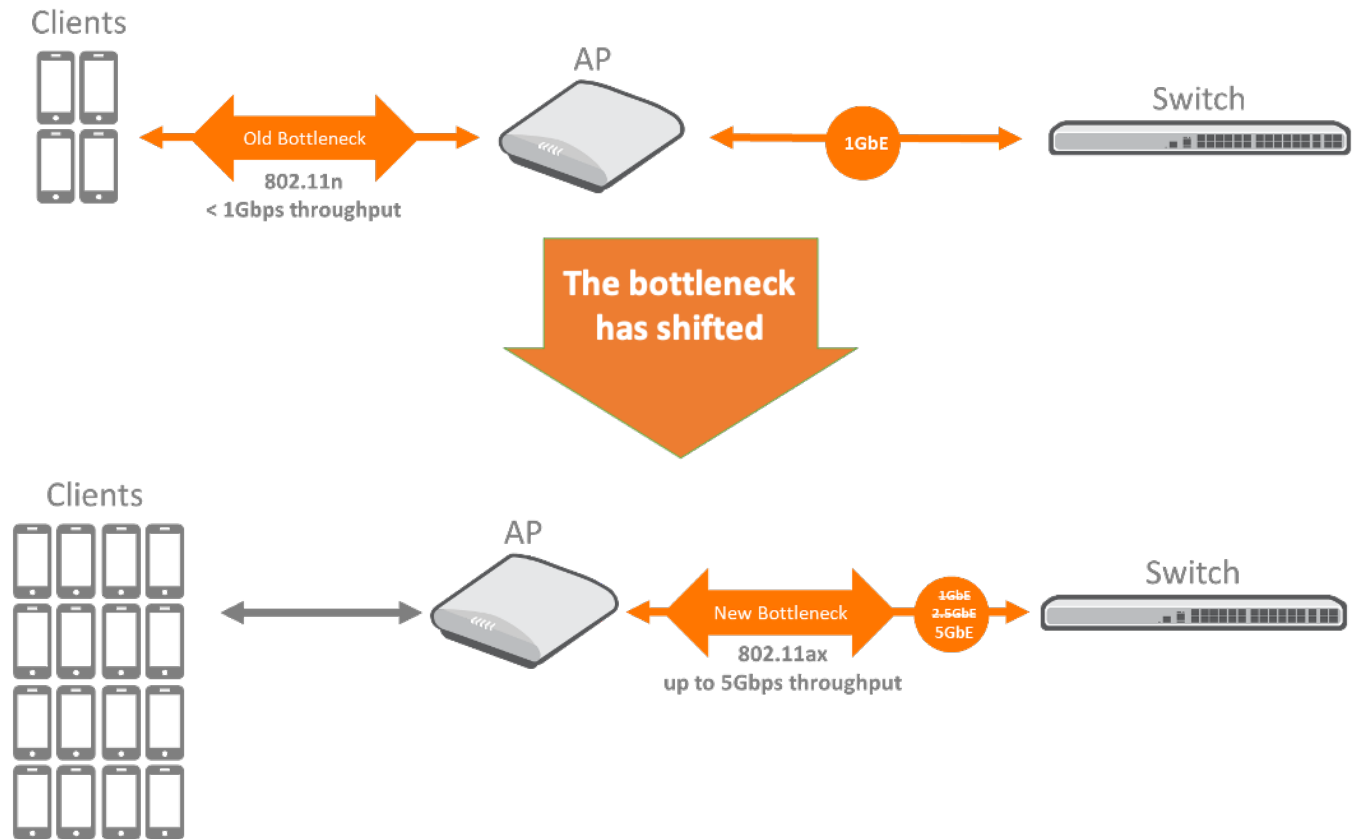


FIGURE 18: DETERMINING WIRED CAPACITY

Conference Area APs are power hungry devices. Many APs will work on legacy 802.3af PoE, but they will run at a reduced performance or radio power output. To make the most of the AP, switches driving Conference Area APs will need to be at least 802.3at capable. Thankfully all RUCKUS ICX switches support 802.3at PoE+, but in some cases the AP will require 802.3bt/PoE++.

Designing for Hospitality

The best way to approach this is to use [Intangi Iris](#).

Load the type and quantities of APs required into Iris and start adding switches. Iris lets you link APs and switches with virtual cables and set the estimated cable lengths. Iris will then calculate and immediately report any issues with the design such as insufficient PoE for a specific type of AP, or if the number and type of APs connected will exceed the total PoE budget available on the switch.

The Ruckus ICX 7150-Z series offer MultiGig and high-power POE++ across several model sizes.

Conference spaces will also need some wired ports for guest use. Generally speaking, expect each space to need 1 port per 50 guests, but work with the customer to identify the number and location of ports needed.





Also consider there may be other networking requirements such as information displays, fixed projection systems, and audio and video conferencing systems that will require wired network connectivity.

- Run high density APs (R7xx / R8xx) on a MultiGig switchport with PoE++ power delivery.
- Cater for non-PoE wired outlet requirements in meeting spaces.
- Cater for other wired systems installed in the meeting spaces.

**Cabling**

If new cabling is needed for the APs and switches, it is strongly recommend that CAT6A specified cable is installed as this guarantees full support for MultiGig speeds and high power PoE.

Keep the runs as short as possible to avoid heat buildup and reduce power consumption on the PoE switch. A small group of APs can be aggregated on a MultiGig/PoE++ compact switch, such as the RUCKUS ICX 7150-C10ZP in a nearby closet, then run 10Gig fiber uplinks to the core.

Standard	Power at Switch	802.11a/n	802.11ac	Wi-Fi 6 (802.11ax) and beyond
PoE 802.3af	15W			
PoE+ 802.3at	30W			
PoE++ 802.3bt	60W (4-pair)			
High-Power 802.3bt	90W (4-pair)			

**Elevators**

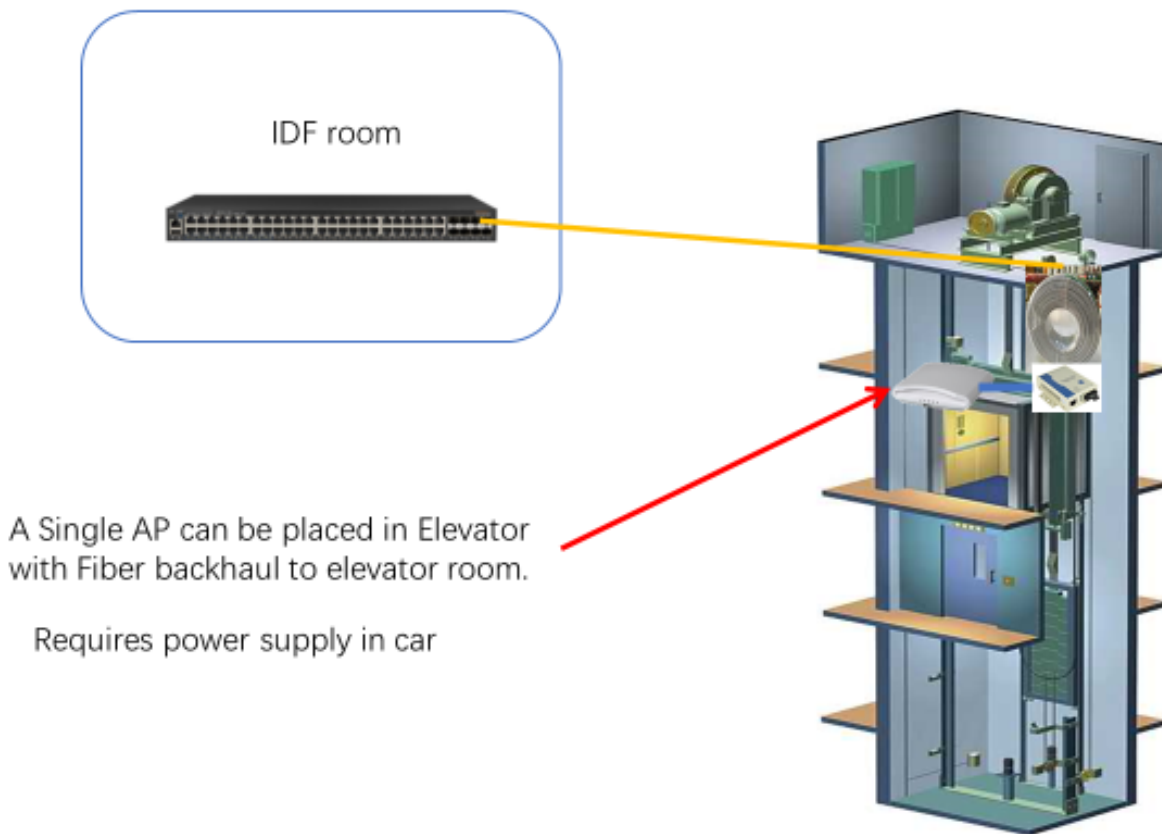
Do not (wrongly) assume that Wi-Fi coverage within the elevator will be available from the corridor APs. An elevator cabin is usually an all-metal box that is surrounded by thick mechanical and high voltage electrical components and is enclosed in a high-density reinforced concrete structure. Wi-Fi simply stands no chance.

Since elevator cabins often have power readily available, placing an AP inside the cabin is easy. Also, cabins tend to be well within the coverage and capacity capabilities of even the most entry-level of APs.

Finally, most modern elevator cabins have other IP connectivity requirements such as in-cabin IP information displays, emergency IP phone, and IP telemetry. Treat the elevator cabin similar to a guest room and use an H510 AP installed inside the cabin itself to provide Wi-Fi as well as wired connectivity to the in-cabin IP devices.

The challenge lies with the uplink from that AP to the rest of the network. There are several ways to approach this, and the decision mainly depends on whether this is a retrofit to an existing elevator vs. a new elevator, as well as the length of the elevator shaft.

**Elevator Method A: Travelling Cable using Fiber (Recommended)**



**FIGURE 19: TRAVELING FIBER CABLE**

The preferred solution is to use a network cable bundled into the elevator’s travelling cable. Use a fiber cable to avoid distance limitations and interference from nearby high-voltage cables.

A few key points to note:

- Either Single-mode and Multimode fiber cable is suitable for this application, as long as the distance limitations are respected, and flexible cable is used.
- Coordinate with the elevator supplier to identify fire ratings and bend radius requirements.
- Normally, the cable is installed by the elevator supplier or elevator maintenance contractor.
- A reliable power supply must be provided for the AP (see below).

Power can be provided in one of the following ways:

- Cabin mains power using a local PSU
- Cabin 48VDC power directly into the AP
- Remote power using the CommScope Powered Fiber Cable System and a remote 48VDC power source.

### **Elevator Method B: Travelling Cable Using Legacy Cabling**

Most existing elevators will have some type of communication cabling already installed that could be reused.

For example:

- Emergency telephone wiring may be 2-pair or 4-pair, but only 1 pair is being used by the analogue telephone in the cabin. The additional pair can be used with a 2-wire point-to-point adapter to deliver data, and sometimes power, over a single pair of telephone wire.

**Note 1:** In some cases, it is prohibited to use the emergency telephone wiring for any other application but emergency telephony, even if the emergency telephone is not impacted.

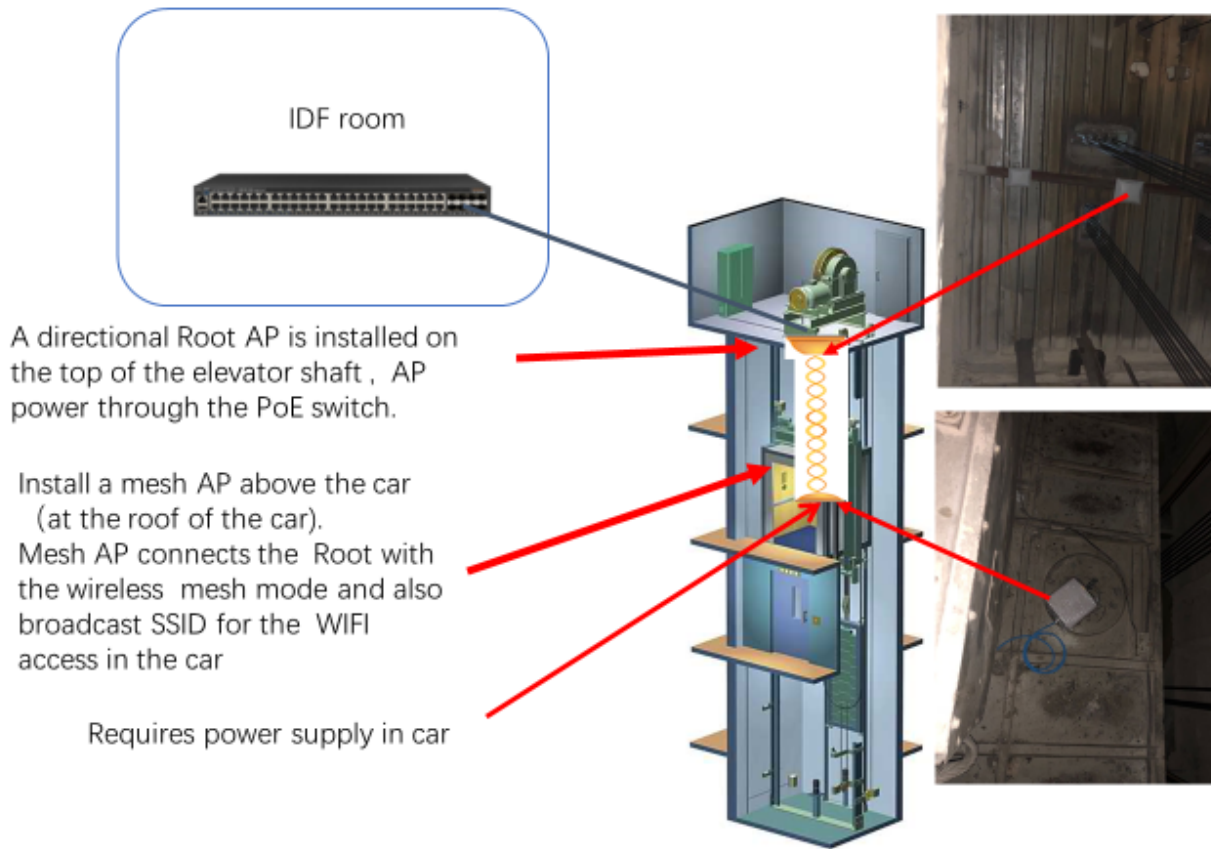
**Note 2:** Most 2-wire systems can only deliver 10Mbps or 100Mbps. Ensure your applications can work within this restriction.

**Note 3:** The telephone wire may be a direct run from the lift cabin all the way to the central telephony PBX which can be several kilometers/miles away. Most 2-wire systems have a distance limitation in the order of 100's of meters, which is considerably less than analogue telephony.

- If there is already a TV in the cabin showing live video feeds, that TV is connected via Coax cabling or Ethernet. In both cases, that same cable can be reused while maintaining full TV functionality.
- In the case of Coax, install a DOCSIS miniCMTS at the head-end. Inside the cabin, the coax cable is split into two, with one leg going back into the TV and the other leg connected into a Ruckus C110 DOCSIS AP.
- In the case of Ethernet, it is simply a matter of installing a Ruckus H510 AP and using one of the downstream ports to connect the IPTV

**Elevator Method C: Wireless Bridge using Mesh**

An alternative solution is to install a wired Mesh Root AP on the top of the elevator shaft and install a Mesh AP on top of the elevator cabin. The Mesh AP automatically creates a Mesh link to the Mesh Root AP using RUCKUS SmartMesh technology, while also broadcasting the WLANs for Wi-Fi access within the car.



**FIGURE 20: MESH CONNECTION IN AN ELEVATOR**

This solution is only possible if the elevator cabin walls and ceiling do not have very high RF attenuation (I.e., they do not block RF signals considerably). If this approach is being planned, ensure that RF penetration between the top of the elevator cabin and the inside of the cabin was tested during the site survey.

In the case of multiple adjacent elevators with a common shaft it is possible to share Mesh Root AP(s) between multiple elevators, but in longer lift shafts it is recommended to dedicate one Mesh Root to each cabin to ensure continuous line of sight between the Mesh Root AP and the Mesh AP.

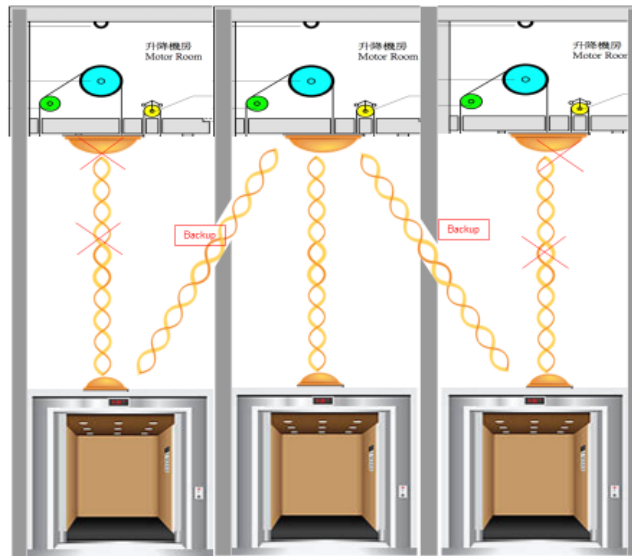


FIGURE 21: USING A SINGLE ROOT AP FOR MULTIPLE ELEVATOR SHAFTS

With multiple Mesh Root APs, Mesh APs will self-heal. If a Mesh Root AP fails, the Mesh AP automatically switches to the adjacent Mesh Root AP to ensure continuation of service.

#### Notes:

- This design is recommended when the elevator shaft height is less than 100 meters, and it is not possible to install a traveling cable.
- The Root AP must use directional antennas, preferably with a narrow beamwidth. Look for the “n” or “s” suffix in the product name (E.g., T310n, T610s, etc.)
- A reliable power source must be provided at the top of the elevator car.
- Check local regulation. In some jurisdictions wireless equipment is not allowed in the elevator shaft. In this case, only the [traveling cable design](#) can be used.



Elevator Method D: Wireless Point to Point bridge

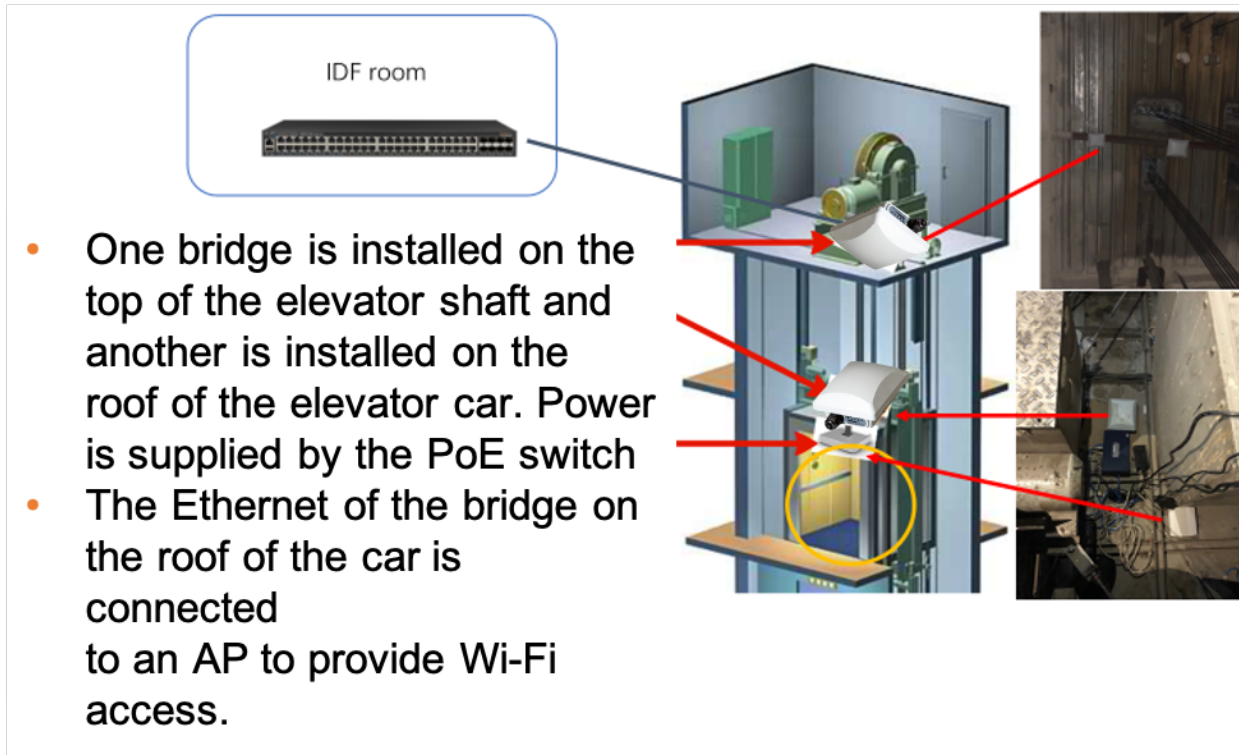


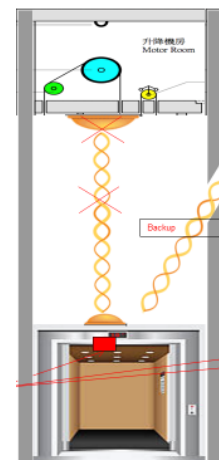
FIGURE 22: POINT TO POINT BRIDGE IN THE ELEVATOR SHAFT

In elevators with longer travels (up to 1 mile / 1.5 Km), install a dedicated Point to Point bridge combined with an in-cabin AP.

The RUCKUS P300 point to point bridge is a dedicated, transparent layer 2 bridge for long distances. Since this platform does not transmit any WLANs, a separate in-cabin AP such as a H510 will need to be used.

Notes:

- Use this design when the elevator shaft height is more than 100 meters and it is not possible to install a traveling cable.
- A reliable power source must be provided at the top of the elevator car.
- The mesh AP must have the EN50121-1 and EN50121-4 certification if installed on the top of lift car for trackside use.
- Check local regulation. In some jurisdictions wireless equipment is not allowed in the elevator shaft. In this case, only the [traveling cable design](#) can be used.



### Back of House (BOH) / Staff-only areas

Although BOH areas are considered lower dense areas in terms of concurrent users per AP, it is essential to ensure uninterrupted connectivity for staff as they move around in order to utilize mobility solutions over Wi-Fi. Today, staff relies on wireless solutions that may include VoWiFi, HotSOS, dining ordering systems, housekeeping systems, etc.

Typical BOH areas may look like a maze with many corridors and pathways, admin offices, kitchens, laundry, changing rooms, storage areas, etc. BOH areas in a typical hotel may look like shown in the below floor plan.



FIGURE 23: BACK OF HOUSE AREAS

### AP Locations

It is recommended to conduct a physical site survey to ensure that AP locations will provide the required signal strength. In most hospitality brand standards, the minimum signal strength is planned at -65 dBm. If a building is still under construction or when a physical survey is not possible, an offline predictive heat map tool, such as Air Magnet by NetAlly can be used to plan out AP locations.



Designing for Hospitality

One way to ensure continuous coverage in hallways is to place APs at intersection points. that way APs can cover multiple directions of the hallway, reducing the quantity of APs required and enhancing roaming experience, example below:

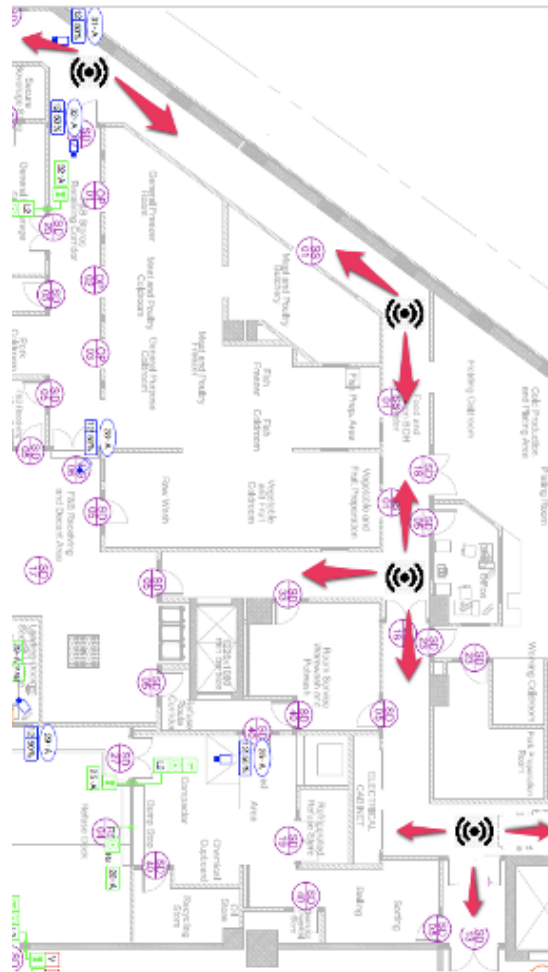


FIGURE 24: AP PLACEMENT FOR ROAMING COVERAGE

Plan hallways first as a starting point then identify remaining coverage areas. Once APs are well placed in hallways, other areas within BOH should be planned carefully, taking into consideration any high-density areas such as a staff cafeteria. Other considerations are places with thick or tiled walls, which may need more APs. Areas with temperature extremes like laundry rooms and freezers need the proper AP models. AP model positioning is discussed in the next section.

**Key Points:**

- Minimum RSSI -65 dBm
- Physical site survey and testing is key
- Offline planning using a recommended heat map tool in case a site survey is not possible
- Start with hallways, use intersection points
- Identify other key areas

**AP Positioning**

CommScope has engineered multiple series of RUCKUS APs that fit different areas depending on purpose, density, orientation, and environment.

It is also important to identify if IoT is required in BOH areas for non-Wi-Fi services and applications that run over Zigbee or BLE.

BOH areas will usually deploy a mix of R3xx series, R5xx series, and possibly a specialty E5xx series.

E5xx APs can be used in areas of temperature extremes such as laundry rooms or cold rooms. The E5xx is an AP with external BeamFlex antennas, allowing the active unit (AP) to be placed above the ceiling in an area with a normal room temperature and the antenna portion to be extended inside the cold room, for example.



FIGURE 25: E510 SERIES WITH BEAMFLEX ANTENNAS

The table below provides a guideline for AP models suitable in various locations.

Area	R3xx <sup>4</sup>	R5xx	E5xx	T3xx
Pathways	X			
Kitchens	X			
Admin Offices		X		
Cold Rooms			X	
Laundry	X		X	
Housekeeping	X			
Unloading			X	X
BOH Outdoor areas			X	X
Parking	X		X	X
Staircases	X			
Workshops	X			

TABLE 3: AP MODEL GUIDELINES

<sup>4</sup> R5xx / R350 must be used if IoT (Zigbee/BLE) is required

**Outdoor**

As with indoor public spaces, work with the customer to define the scope of coverage within the outdoor area.

For example, in a large resort in the forest, the customer may want Wi-Fi coverage within the paved pathways but not deep inside the forest. It is important to understand where the customer expects to have Wi-Fi coverage.

**Factor in Trees and Foliage**

Trees and other foliage are great at providing oxygen and shade, but unfortunately, they are just as great at attenuating Wi-Fi. When designing outdoor RF networks, **avoid placing APs behind trees, plants and bushes.** When trees are dry or dead, they are virtually invisible to Wi-Fi, but when they are alive (full of water), they can attenuate Wi-Fi RF signals by as much as 10-30dB<sup>5</sup>. **If an AP must be placed behind seasonal foliage, factor in a 20dB seasonal variation.**

Outdoor coverage in the hospitality world is almost always obtained using the T3xx series APs. As of this writing, the current T310 AP has 4 variants, differentiated by the letter suffixed at the end of the product name.

Model	Antenna Type	Operating Temp	USB Port	DC Power In
T310c	Omni (360°)	-20°C to +65°C	No	No
T310d	Omni (360°)	-40°C to +65°C	Yes	Yes
T310s	Wide Sector (120°)	-40°C to +65°C	Yes	Yes
T310n	Narrow Sector (30°)	-40°C to +65°C	Yes	Yes

TABLE 4: OUTDOOR AP MODELS

All AP models use a standard 1Gbps Ethernet uplink and are powered by standard 802.3af PoE. Models having a DC Power In option support direct 12v DC nominal (8V – 20V) power wired into the AP, which is normally used for mesh support since the Ethernet port will not be used in this case.

<sup>5</sup> See [https://www.itu.int/dms\\_pubrec/itu-r/rec/p/R-REC-P.833-9-201609-I!!PDF-E.pdf](https://www.itu.int/dms_pubrec/itu-r/rec/p/R-REC-P.833-9-201609-I!!PDF-E.pdf) for more info.

Designing for Hospitality

**Fiber Uplink for Outdoor APs**

In cases where the outdoor AP is installed in a location that is more than 90m away from an IDF, a fiber cable is required for uplink connectivity.

Avoid building an external mini IDF to house a standard fiber media converter, as this will require a high voltage power source, a power supply and associated cooling, and patch cabling. All of which are prone to fail especially if installed in areas with extreme temperatures.

Instead, use the CommScope PFCS system to carry power and data over a single wire right up to the AP, where an outdoor grade converter will convert it back to 1 or 2 ports of copper 1Gbps Ethernet + PoE. For more information about PFCS, the [PFCS section](#).



Media Converter, PoE Injector, Power Outlets, Power Supplies... and a complete mess of wiring

**Don't do this!**



CommScope PFCS hybrid cable + CommScope PFCS POE Extender + RUCKUS T3xx AP

**Do this!**

**FIGURE 26: COMMSCOPE PFCS SOLUTION**

### Mesh Uplink for Outdoor APs

Mesh and outdoor mesh considerations are covered in depth in separate Best Practice Design Guides (BPDG). See the [Mesh BPDG](#) and [Outdoor Mesh BPDG](#). Both are available on the Ruckus support site.

### Mobile Hotspot (Chauffeur Cars / Golf Carts)

The RUCKUS M510 mobile-wireless AP is designed to leverage LTE networks as a backhaul and connect wirelessly back to any network without the need for an Ethernet cable connection.

Because of the wireless LTE backhaul capability, the M510 addresses multiple deployment scenarios in hospitality, including:

- Mobile “in-vehicle” Wi-Fi (“mobile AP”) for hotel operated chauffeur vehicles and golf carts
- Rapid Wi-Fi deployment for temporary events, or a beach bar and other facilities where cabling is not possible.
- M510’s LTE backhaul can serve as a failover or redundancy for the WAN connectivity too.

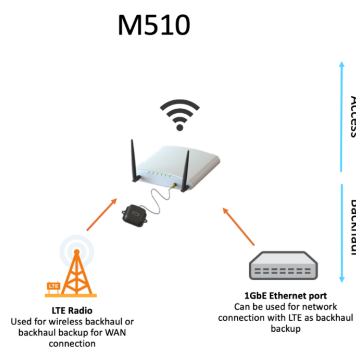


FIGURE 27: RUCKUS M510 WITH LTE BACKHAUL

### Benefits:

- Use existing management platform (Controller) for all APs
- Supported in Standalone mode, Unleashed, and SZ managed
- Resiliency, Geo Redundancy, Advanced WLAN management



FIGURE 28: RUCKUS APs ACROSS MULTIPLE MANAGEMENT PLATFORMS



**Things to know:**

- For SZ management, SZ must have Public facing IP address to enable connection over LTE
- Option 43 is not supported over LTE backhaul due to LTE limitations
- Pure Local-Breakout Mode is not supported directly over LTE
  - Need to enable NAT/DHCP on M510 if using LTE Backhaul without tunneling
  - If using tunneling, NAT/DHCP need not be enabled on M510
- AP to AP communication over LTE is not supported
- 802.11r, Bonjour Fencing, Auto Cell Sizing will not be supported

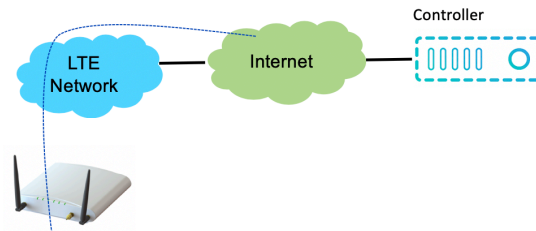


FIGURE 29: RUCKUS M510 CONSIDERATIONS

**Before You Order**

When placing an order for an M510, make sure the right SKU is selected to ensure the LTE domain is supported by the carrier in your region. Here is a list of SKU options, check datasheet for updates:

ORDERING INFORMATION	
901-M510-ATT0	<ul style="list-style-type: none"> <li>• Ruckus M510, USA (AT&amp;T)</li> </ul>
901-M510-D100	<ul style="list-style-type: none"> <li>• Ruckus M510, Domain 1 (All Carriers in below countries)</li> <li>• (India, Singapore, Malaysia, Philippines, Thailand, Vietnam, Hong Kong, Europe, Turkey)</li> </ul>
901-M510-D200	<ul style="list-style-type: none"> <li>• Ruckus M510, Domain 2 (All Carriers in below countries)</li> <li>• (Australia, New Zealand, Mexico, Brazil, Taiwan)</li> </ul>

Designing for Hospitality

**M510 Deployment:**

- Buy a SIM Card or two (micro SIM) & a Data Plan
- Attach the black LTE antennas (included in box) to the AP
- Note down IMEI number of the M510 (available on the box or on the back of the AP)
  - Please do this before you mount the AP
  - You can use SWIPE app to save this information
  - Your carrier may need the IMEI number to activate data plan



**Onboarding M510 onto SZ Controller:**

The following are supported M510 to SZ controller onboarding methods:

The SWIPE app	AP Registrar	Manual onboarding
<ul style="list-style-type: none"> <li>• Installer downloads app onto phone</li> <li>• Log into the desired SZ on SWIPE</li> <li>• Connect to M510 wirelessly</li> <li>• AP automatically <u>onboards</u> onto SZ</li> <li>• You can also save IMEI number of M510</li> </ul>	<ul style="list-style-type: none"> <li>• Enter AP Serial number and SZ IP address into AP registrar beforehand</li> <li>• Power up M510 with SIM</li> <li>• M510 <u>onboards</u> onto SZ</li> </ul>	<ul style="list-style-type: none"> <li>• Physically log into M510 over Ethernet</li> <li>• Optionally use CLI</li> <li>• Set SCG IP address</li> <li>• Disconnect the Ethernet</li> <li>• Mount the AP</li> <li>• Confirm AP is connected to SZ</li> <li>• Tedious, error prone and slow</li> </ul>

FIGURE 30: ONBOARDING THE M510

Topology Examples

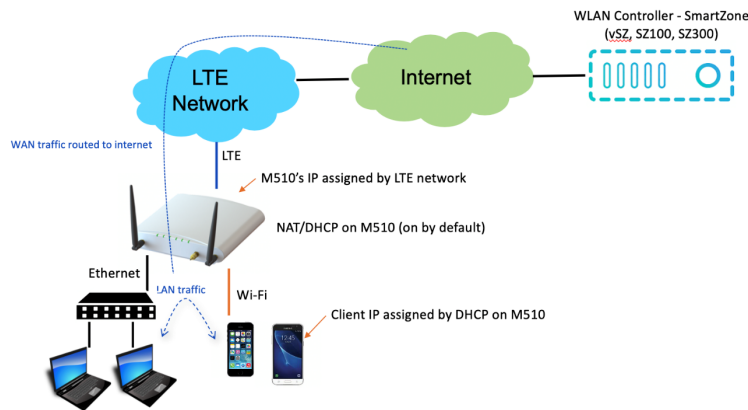


FIGURE 31: TOPOLOGY 1 (LTE AS PRIMARY BACKHAUL)

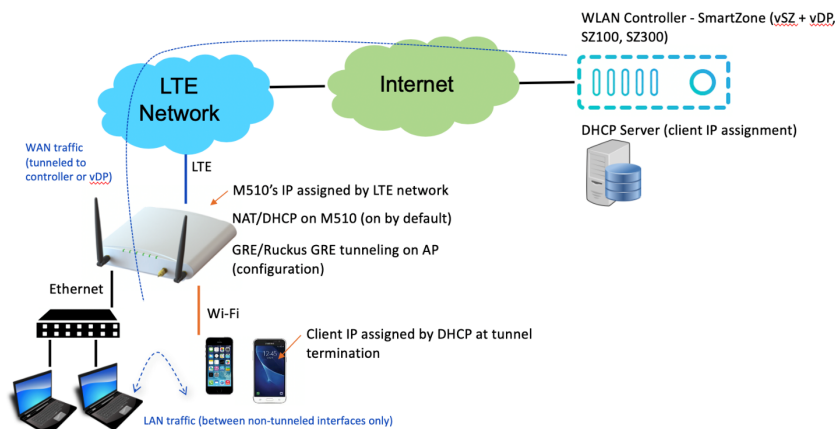


FIGURE 32: TOPOLOGY 2 (TUNNELED TRAFFIC – REMOTE CONTROLLER)

In the above two topologies:

- Off-premises SmartZone controller
- M510 shall support all the controller Discovery methods including AP Registrar (in this case Manual or AP Registrar will be used)
- NAT on the AP Management IP Address
- Assumption is that the Controller is reachable on the AP's Management IP (Over the LTE network) i.e., in the DMZ with appropriate port forwarding setup.

Designing for Hospitality

Dual SIM LTE-LTE Failover

BEFORE FAILOVER

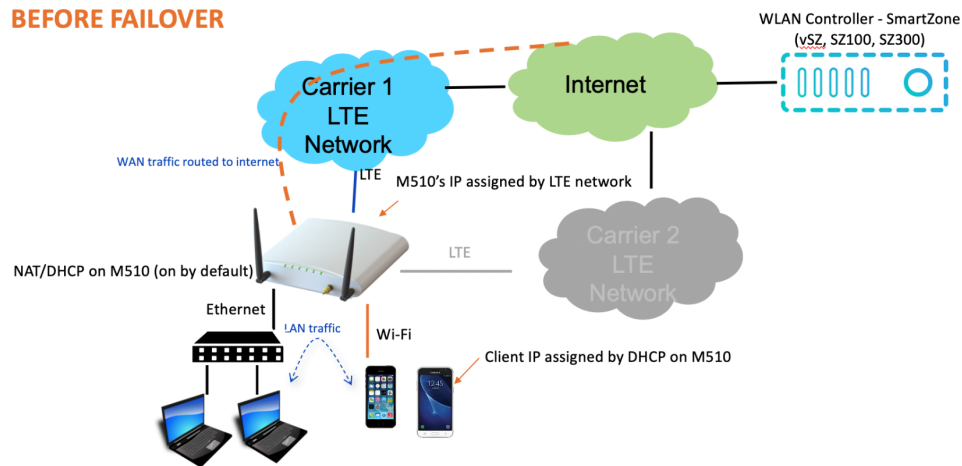


FIGURE 33: DUAL SIM LTE BEFORE FAILOVER

AFTER FAILOVER

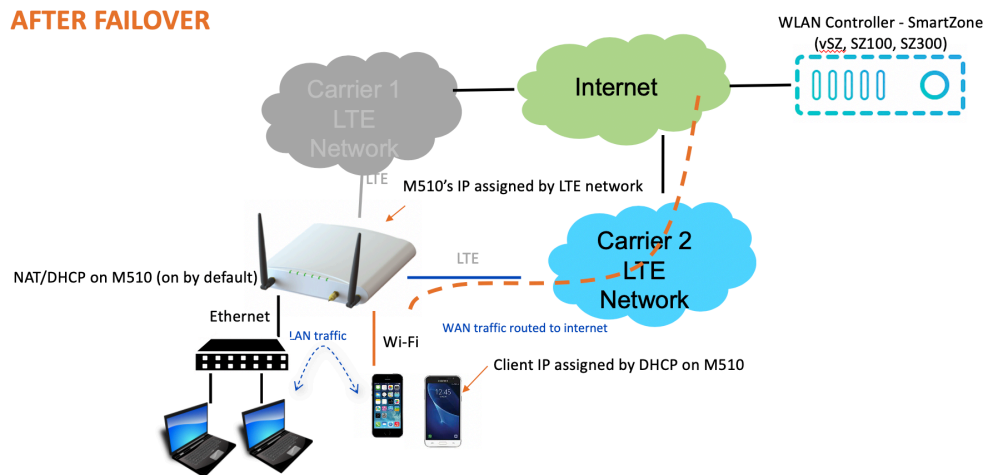


FIGURE 34: DUAL SIM LTE AFTER FAILOVER

- M510 fails over to the 2<sup>nd</sup> SIM if first SIM signal is non-existent
- M510 will remain on the 2<sup>nd</sup> SIM until it's signal drops & then will fail back to original SIM
- Applicable to tunneled & non-tunneled mode
- LTE-Backhaul AP is used to provide Wi-Fi connectivity over LTE backhaul
- Use cases in hotels include transportation vehicles, golf cart, and areas where pulling a cable is impossible
- It can run as standalone or be managed by SZ controller, supports Unleashed too
- Before ordering, check proper SKU for carrier support
- Can be onboarded onto SZ using multiple ways
- Use 2 SIM cards for LTE redundancy

## Switching Design

### Access (IDF) Switches

The RUCKUS ICX 7150-24P (“P” stands for PoE-enabled switch) or RUCKUS ICX 7150-48PF switches are ideal choices for the IDF. There are a few instances, such as if there are R7x0 series access points installed and/or strict requirements for redundant power supplies, in which a different ICX switch should be used. In general, however, the RUCKUS ICX 7150 provides the performance and features required at the IDF. Determining which ICX 7150 variant of switch to deploy largely depends on how many ports are needed.

<b>ICX 7150-24P</b>	24-port, PoE-enabled switch. Choose this switch if less than 24 ports are needed to connect access points (APs) or other end devices. 370 Watts POE budget
<b>ICX 7150-48PF</b>	48-port switch with a 740-watt PoE budget. This switch is ideal if more than 24 ports will be needed to connect APs or other end devices.
<b>ICX 7150-48P</b>	48-port switch with a lower 370 Watts PoE budget. Only use this switch if not all ports will be used for POE (E.g., In the case of alternating AP and IPTV ports)

TABLE 5: RUCKUS ICX 7150 VARIANTS

If more than 48 ports are needed, stacking multiple ICX 7150 switches is the optimal choice. This will be discussed in the stacks and uplinks section.



### Power (POE) Requirements

One advantage of the RUCKUS ICX switching family is the comprehensive PoE support. For more information about the different types of POE, consult the Glossary.

Learn more about PoE support and design with CommScope’s PoE Implementation Guide.

All RUCKUS ICX “P” switches are PoE+ capable (30 watts). In addition, the ICX 7150 Z-Series, ICX 7450, and ICX 7650 are PoH (90 watts), PoE++ (60 watts, UPoE) and PoE/PoE+ capable. Determining power requirements to ensure the switch can provide sufficient power is critical.

Power requirements depend on the devices connected to the switch and can vary significantly. The following table provides information on the maximum PoE budget for each ICX switch. It’s imperative that the total power budget not be exceeded. The table also includes information on each RUCKUS AP and the total number of APs each switch can safely support. It is important to take into consideration cable loss when calculating power requirements.

Switch Model	Max PoE budget	H320 15W	H510 15W	R310 15W	R510 15W	R720 30W	R720 45W
ICX 7150-12C	124W	8	8	8	8	4	—
ICX 7150-24P	370W	24	24	24	24	12	—
ICX 7150-48P	370W	24	24	24	24	12	—
ICX 7150-48PF	740W	48	48	48	48	24	—
ICX 7150-48ZP single ps	740W	48	48	48	48	24	16
ICX 7150-48ZP dual ps	1480W	48	48	48	48	48	16
ICX 7250-24P no eps	370W	24	24	24	24	12	—
ICX 7250-48P no eps	740W	48	48	48	48	24	—
ICX 7450-24P single ps	748W	24	24	24	24	24	8
ICX 7450-48P single ps	748W	48	48	48	48	24	8
ICX 7650-48P single ps	748W	48	48	48	48	24	8
ICX 7650-48P double ps	1496W	48	48	48	48	48	8
ICX 7650-48ZP single ps	748W	48	48	48	48	24	16
ICX 7650-48ZP double ps	1496W	48	48	48	48	48	24

TABLE 6: POE BUDGET CONSIDERATIONS

## ICX Power Supply Options

The ICX switch family includes switches that utilize the following power supplies:

- Embedded single power supply: ICX 7150 and ICX 7150C
- Dual power supplies: ICX 7150 Z-Series, ICX 7450 and ICX 7650
- External power shelf (EPS) with DC connectors: ICX 7250



## Stacking vs Uplinks

Stacking is the recommended approach when two or more switches need to be connected. Stacking provides the following benefits:

- Single point of management for multiple switches
- No spanning tree issues between switches
- In-Service Software Upgrade (ISSU) for hitless image upgrades

There are a few things to keep in mind when stacking ICX switches:

- 10 GbE links must be used, as stacking will not work over 1GbE links. On the other hand, Uplinks will operate at any available speed.
- Trunks from multiple uplinks that are bound together must operate at the same speed.
- 10 GbE ports can be used for stacking, uplinks, and server connectivity since they are universal ports. This is a unique feature of RUCKUS ICX switches. ICX switches do not need dedicated modules or proprietary cables.
- The maximum number of switches in a single stack is 12.
- ICX switches support long-distance stacking up to 10 km over standard Ethernet cables and optics. This allows switches to be stacked together even if they are in different wiring closets or on different floors.

Different switch models can be mixed within one stack (port count, PoE/non-PoE). However, they must be from the same family. For example:

- Stack 1: ICX 7150C-12, 7150-24, 7150-48PF, 7150-48ZP
- Stack 2: ICX 7250-24, 7250-48P
- Stack 3: ICX 7450-24, 7450-48P, 7450-48F
- Stack 4: ICX 7650-48F, 7650-48P, 7650-48ZP
- Stack 5: ICX 7750-26Q, 7750-48F, 7750-48C

### Stacking Cables and Optics

The distance between switches depends on distance and the complexity of the design. The following options are available for Twinax cables for in-rack stacking.

- ICX 7150 and ICX 7250 families: 10 GbE Twinax
- ICX 7450: Either 10 GbE or 40 GbE Twinax cables
- ICX 7750: 40 GbE Twinax cables
- ICX 7650: Either 40 GbE or 100 GbE Twinax cables

Twinax cables are available in lengths of 1, 3, 5, 7, or 10 meters.

Short-range (SR) optics should be used for up to 300 meters and the long-range (LR) optics for distances up to 10 kilometers.

### Part Numbers for ICX 7150 Switches

Most of the ICX 7150 product range can be ordered with several options. Let’s look at the options available.

SKU	10Gbps SFP+	Stacking	Routing <sup>6</sup>	Remote Support
7150-xx-4X1G	0	No	Basic	90 days 8x5
7150-xx-2X10G	2	Yes	Basic	90 days 8x5
7150-xx-4x10GR	All	Yes	Advanced	90 days 8x5
7150-xx-4x10GR-RMT3	All	Yes	Advanced	3 Years (see below)

<sup>6</sup> Basic = Static Routes and RIP. Advanced = OSPF, VRRP, PIM, PBR

Warranty

	ICX 7150 / 7450 / 7650 / 7750	ICX 7250
Included Support	Advanced hardware replacement (next business day), Includes power supplies & fans	
	Lifetime software updates	
Optional Bundle SKUs with 3 Year Support	For the life of the product (initial registered end user only)	
	90 days 8x5 remote phone support	3 years 24x7 remote phone support
Optional Bundle SKUs with 3 Year Support	4 hour parts only support	
	Next business day parts only support	
	Remote phone support	
	Secure uplift support	
	3 years 24x7 remote phone support ICX7x50-xxx-yyy-RMT3	n/a (3 year support is already included in base SKU)

## Infrastructure Design

This section will discuss two different scenarios, a new construction and a refurbish.

### New Construction

In new construction there is an opportunity to influence the design of the infrastructure. With new construction it is important to conduct a Needs Analysis and review the brand's standards. Ask if they have an existing Division 27 Standard. The Construction Specifications Institute (CSI) developed MasterFormat and it is the most widely used specification for commercial buildings. Division 27 is the Communications subgroup.

A Division 27 Standard will tell you all that you need to know about their cabling requirements. If the standard has not been updated in a while; this is a good opportunity to work with a CommScope Infrastructure Systems Engineer to update the document. An outdated standard will have outdated cabling. This is important because N-Base-T, Wi-Fi 6, and core switches demand the latest high-quality cabling plant. Updating the standard now is more cost effective than finding out after the fact that an updated network is running across an antiquated cabling plant.

If the customer does not have a Division 27 Standard at all, this is a good time to engage with a CommScope Infrastructure Systems Engineer to create a standard.

While working on the Division 27 Specification with the client, it is important to meet with the consultant who is designing the Structured Cabling System. They may use a generic Division 27 standard. If CommScope is developing a Division 27 Standard, then the client should ask the consultant to use this document for their construction documents. At this time, convey the power, space and cabling requirements of the equipment to be installed.

### Refresh

The second scenario is an existing building with existing pathways, spaces and cabling. Before anything else is done, ask to see documentation of the existing cabling plant. Test results, As Built Drawings, and conducting a site survey (refer to the CommScope Site Survey document for more details) will help in developing a plan. A qualified infrastructure specialist such as a CommScope Infrastructure Systems Engineer or PartnerPro contractor will be able to assist ([PartnerPro lookup](#)).

If the property is an existing building, the pathways, spaces, and cabling plant may have been there for years. One of the challenges with an existing building is using the latest equipment on an old cabling plant. Category 5, Category 5e and Category 6 may not be able to support every N-BaseT design.

- You may be specifying or confirming cable locations for installers to later use.
- All cabling should be installed to standard the latest version of:
- ANSI/TIA 568 Generic Telecommunications Cabling for Customer Premises
- ANSI/TIA 568 Commercial Building Telecommunications Cabling Standard
- TSB-162-A Telecommunications Cabling Guidelines for Wireless Access Points a
- A report should be available showing the cabling plant passed the latest:
- ANSI/TIA Balanced Twisted-Pair Telecommunication Components Standard
- ANSI/TIA Optical Fiber Cabling Components Standard



Designing for Hospitality

- You may be making use of existing cabling. It is a best practice to ask to for a copy of the structured cabling manufacturer’s warranty. If the cabling plant is not certified to Category 6A, a qualified cabling technician should verify performance. Many Access Points use N-BaseT and the only way to ensure performance is to test per:
- TIA TSB-5021 Guidelines for the Use of Installed Category 5e and Category 6 Cabling to support 2.5GBase-T and 5GBase-T.

Although internal electrical performance of Category 6 can support 2.5GBase-T and 5GBase-T, noise from adjacent cables can cause a link to fail.

- If a Category 5e or Category 6 link fails, the TSB-5021 test there are some mitigation techniques:
- Replace equipment cords and patch cords with Category 6A cords
- Reconfigure cross-connect cabling to more direct interconnection
- Replace connections with Category 6A connections
- Replace the horizontal cable with Category 6A horizontal cable

	2.5GBase-T	5GBase-T
Installed Cat 5e		Extended frequencies required
Installed Cat 6		
Installed Cat 6A		

Bundled cabling length 0m-50m	Category 5e	Category 6	Category 6A
2.5GBase-T			Assured
5GBase-T			Assured

Bundled cabling length 50m – 75m	Category 5e	Category 6	Category 6A
2.5GBase-T			Assured
5GBase-T			Assured

Designing for Hospitality

Bundled cabling length 75m – 100m	Category 5e	Category 6	Category 6A
2.5GBase-T			Assured
5GBase-T			Assured

ALSNR Risk	High	Medium	Low
------------	------	--------	-----

Before deploying fiber circuits, it is important to verify performance. The table below will give guidelines about supportable distances of various types of fiber:

Application Supported	OM5 50μ	OM4 50μ	OM3 50μ	OM2 50μ	OM1 62.5μ
40GBase-SR4	150m	150m			
10GBase-S	550m	300m	150m	32m	82m
10GBase-LX4	300m	300m	300m	300m	300m*
1000Base-SX	1100m	1000m	800m	300m	550m
1000Base-LX	500m	550m	550m	550m*	550m*
Singlemode	OS2				
40G FR	2km				
40G LR4	10km				
40G ER4	40km				

- Fiber optic cabling links can be adversely affected by dirt and debris on the end face of the connector. It is a best practice that a qualified cabling technician use a video inspection probe to inspect the end face before you connect. If there is dirt or debris on the end face refer to CommScope’s *Inspection and Cleaning instructions 412-19087* for detailed recommendations.
- Only use industry recommended fiber optic cleaning supplies

## Network Management (Controller)

CommScope RUCKUS wireless solutions are not restricted to a single type of management. Almost all of RUCKUS switching and Wi-Fi hardware can be managed by any of several different management platforms. The hardware is not locked to one platform and can be migrated between platforms through a simple firmware change as network needs evolve.

There are 3 main types of controller to choose from:

	SmartZone	Ruckus Unleashed	Ruckus Cloud
<b>Customer Type</b>	Centralized, mid-to-large organizations or service provider with capable IT	Small organizations with little to no IT	Distributed, small-to-large organizations with centralized or outsourced IT
<b>Customer Needs</b>	Flexible architecture Deep features and tools AP and Switch unified management	Low cost Deploys simply	Multiple sites Cloud management Deploys simply at scale
<b>Deployment Type</b>	1 or more large sites On-premises Private Cloud	1 or more small sites On-premises	2 or more sites
<b>IT Fit</b>	IT management IT staff	Some IT staff	Centralized IT staff Outsourced IT
<b>Control Type</b>	Dedicated physical or virtual appliance	AP only	Cloud
<b>IoT Support</b>	Full	No	Upcoming Release
<b>Management</b>	WebUI SNMP RESTful API	WebUI Mobile app	WebUI Mobile app
<b>Maximum Devices</b>	Up to 30,000 APs Up to 6,000 switches	128 APs 8 switches	Unlimited APs Unlimited Switches
<b>Maximum Clients</b>	450,000 WiFi Unlimited Wired	2,048 WiFi Unlimited Wired	Unlimited WiFi Unlimited Wired
<b>Supported Models</b>	All APs, except P300 All ICX 7xxx switches	Most current APs <sup>7</sup> All ICX 7xxx switches	Refer to link in footnote <sup>8</sup>

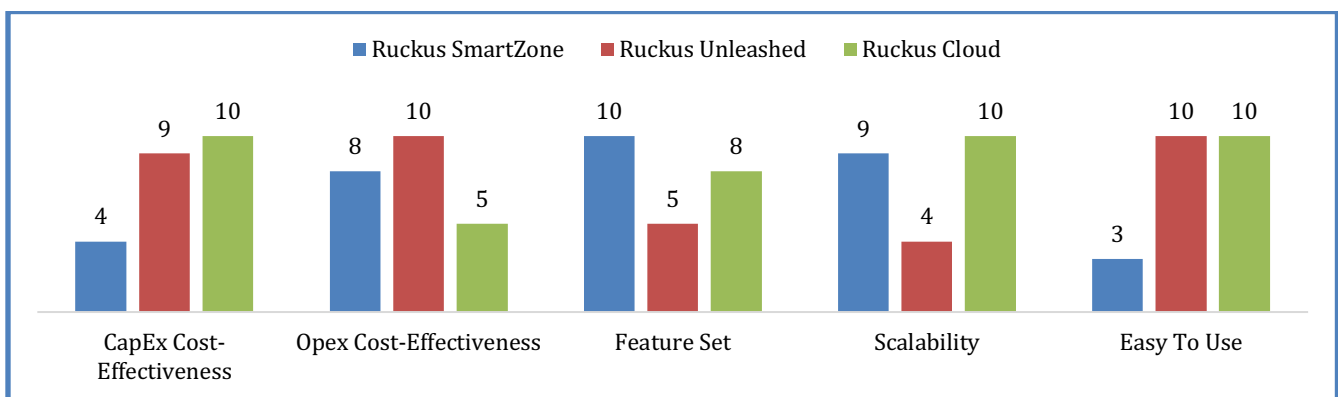
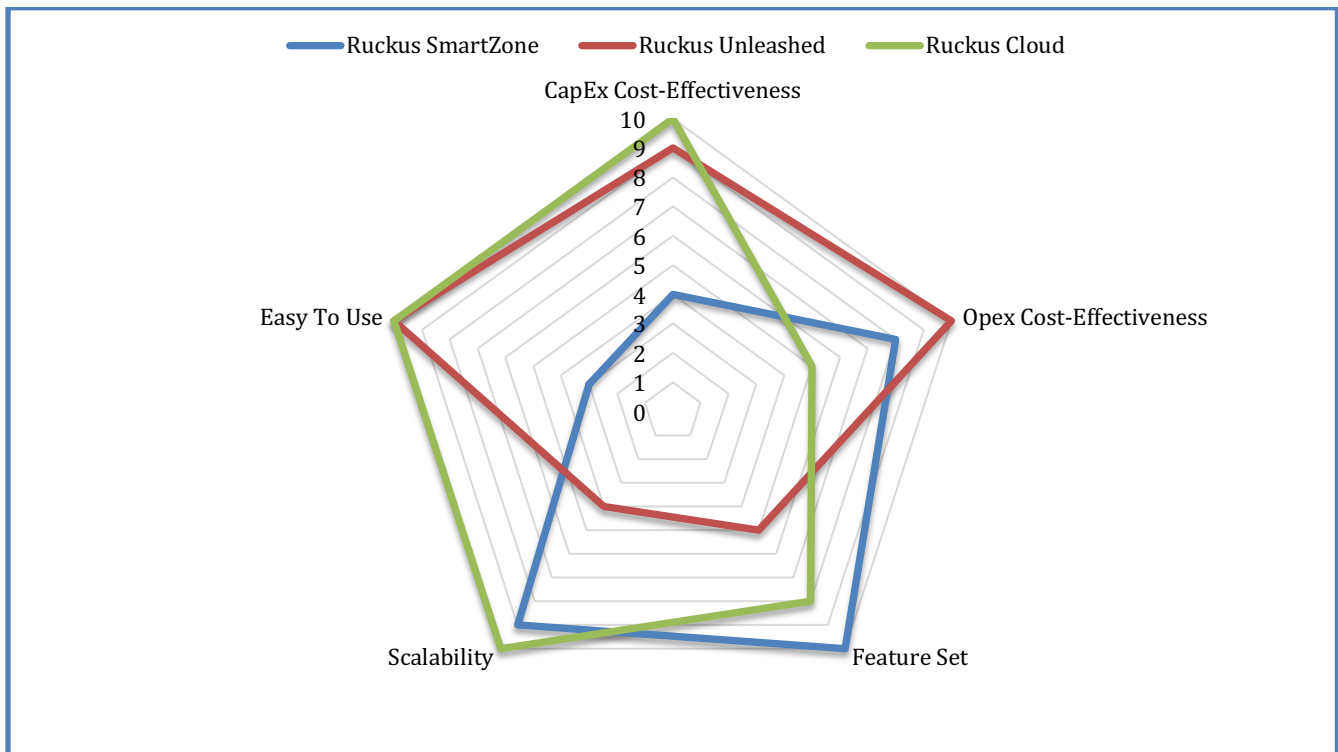
<sup>7</sup> Refer to *Release Notes* documents on the <http://support.ruckuswireless.com> for a complete list of supported AP models

<sup>8</sup> A complete list is maintained at <https://www.commscope.com/cloud-supported-network-devices>

### Choosing the Right Management (Controller) Platform

All management platforms offer basic Wi-Fi and Wired management functionality, but they do differ in subtle ways, which means there is no single answer to this conundrum. This is exactly why CommScope RUCKUS provides various management platforms. The aim is to strike a balance between what functionality is needed from the controller, versus the level of expertise of who will be managing the network, versus cost.

In the charts below we have rated different aspects of each management platform. A lower rating doesn't necessarily make it *bad* in the traditional sense, but rather it means it's not as capable in that department as its brethren.



## Examples

When designing a network for a small, 25-room boutique hotel where the owner is also the general manager, the bartender, and the receptionist, the last thing they would want is a Wi-Fi controller loaded with knobs and buttons that they don't understand. They just want a simple Wi-Fi network for their guests that they can quickly check with their mobile device if a guest has an issue. In this case, Ruckus Unleashed is the perfect platform since there is no central 'box' or reliance on internet connectivity. It also has virtually no CapEx nor OpEx since there is no other 'box' to buy or annual subscription to pay to keep the network active<sup>9</sup>.

On the other hand, a large national chain of 400 motorway hotels offering basic motel-style room+breakfast+WiFi service with no on-site IT staff would want a way for their IT team at headquarters to centrally monitor and manage all their properties in bulk. Similar to the boutique example above, their technical needs are minimal. They need to provide simple, reliable Guest Wi-Fi connectivity consistently throughout their properties. Here, Ruckus Cloud fits the bill perfectly since it is very easy to ensure service consistency across thousands of APs spread throughout hundreds of properties.

In a final example, the design for a large single property with 600 guest rooms annexed to a large conferencing venue holding 10,000 attendees, their internal IT team or their chosen managed service provider will need to have as much control into and visibility of the network as possible as they will need to fine tune the Wi-Fi network down to the smallest details, troubleshoot issues in real-time, integrate with 3<sup>rd</sup> party conference management systems and other entertainment services, etc. In-depth control and scale are the key and therefore Ruckus SmartZone is the best choice here.

Always keep in mind that RUCKUS networking solutions can very easily migrate from one platform to the other without changing AP and switch hardware. The national chain example above could start with 1 or 2 sites running Ruckus Unleashed and as their rollout expands, they can migrate existing sites to RUCKUS Cloud. Later, if they need to have more in-depth control, a greater feature set, and lower OpEx costs, they can easily migrate their entire estate to Ruckus SmartZone. All this can be done remotely and in bulk.

---

<sup>9</sup> On average, each AP needs ~1-4 kbps and each ICX switch needs XXXX kbps during normal operation. When triggering a firmware upgrade, the devices will individually pull their firmware from the RUCKUS SmartZone using HTTPS.



### Ruckus SmartZone

While the details of a SmartZone configuration are beyond the scope of this guide, the mode being used is required in order to calculate the quantity and type of nodes, licenses, and Watchdog support contracts to order.

When designing for SmartZone, the first decision is whether to go for a centralized vs. distributed approach. Then, choose between using a *physical* rackmount appliance vs *virtual* private cloud hosted. As you can see, RUCKUS SmartZone is very flexible in that respect.

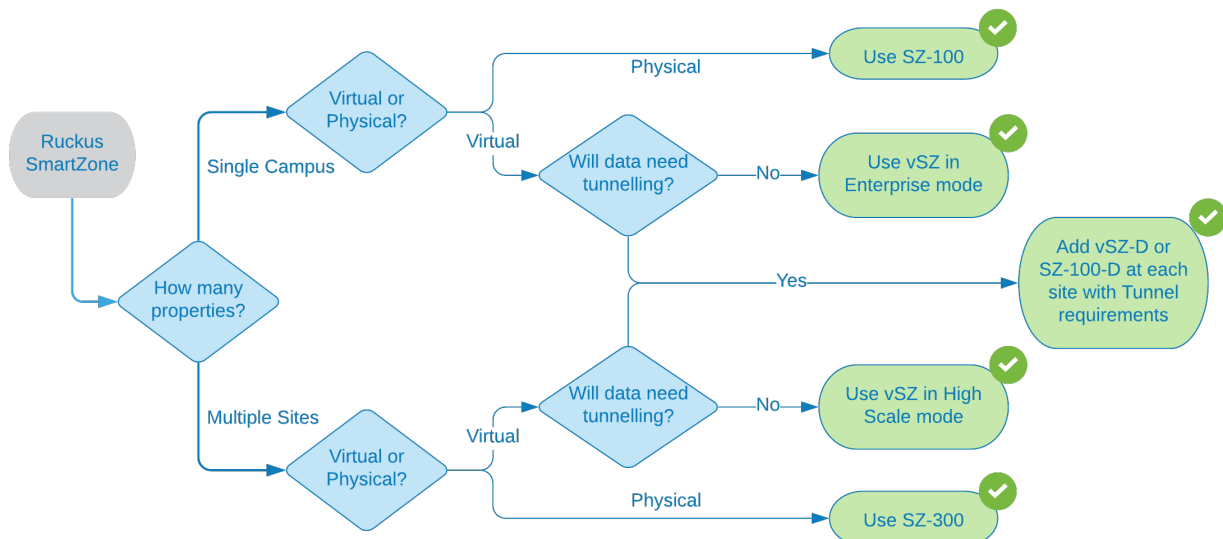


FIGURE 35: VIRTUAL VS. APPLIANCE SMARTZONE

Start by deciding whether the customer wants to host the controller as a virtual machine in their own private cloud environment or if prefers a physical rackmount unit as a controller.

Once that decision is made, the next deciding factor is scale. Will the controller be managing a single site or many sites?

Note: The RUCKUS SmartZone is equally at home managing a few hundred APs at a single site as it is managing thousands of APs across hundreds of sites distributed globally. There is no functional difference between having the controller on site, or halfway across the world in a datacenter.

First, keep in mind that RUCKUS SmartZone *software* has 2 modes of operation:

- A slimmed down -E(enterprise) mode provides simplicity and 14-day log storage and is limited to 6,000 APs. The SZ-100 hardware controller is locked to this mode.
- A full-featured -H(igh Scale) mode provides complete management flexibility and scale supporting 24-hour log storage while supporting 30,000 APs. The SZ-300 hardware controller is locked to this mode.

Both options are available as a physical device or a virtual machine, so the choice needs to be made as follows:

Preferred Architecture		Controller Type	Management slots available per node
Centralized	Physical	SZ-144	2,000
	Virtual	vSZ (in -Enterprise mode)	1,000
Distributed	Physical	SZ-300	10,000
	Virtual	vSZ (in -High Scale mode)	10,000

TABLE 7: HIGH-SCALE VS. ENTERPRISE (VIRTUAL) SMARTZONE

**Scalability – AP and ICX Switch Management Slots**

When designing a controller setup for both AP and ICX switch management, keep in mind that each one ICX switch added to the controller consumes five management slots, while one AP consumes only one management slot.

Use the following table to calculate how many Management Slots are needed.

Total quantities in your design		Multiply by		Result
Switches =		x 5	=	
APs =		x 1	=	
Total Management Slots needed			=	

TABLE 8: MANAGEMENT SLOT CALCULATION

**Scalability - Clustering**

Did the number of Total Management Slots needed result in more than is supported by your preferred platform? Don't worry. With Ruckus SmartZone, AP and ICX Switch capacity is added by simply adding more nodes to a SmartZone Cluster, which can have up to 4 nodes. For redundancy purposes, in clusters having 2-4 nodes CommScope recommends that the AP and ICX Switch capacity is limited to N-1. In other words, the capacity needs to be calculated as though there is one less node. For example, in a cluster having 3 nodes, the Management Slot capacity will be that of 2 nodes.

# of Nodes	Node Capacity	Redundancy
1	1x	No Redundancy (node failure will result in cluster failure)
2	1x	Can tolerate 1 node failure
2	2x	No Redundancy (node failure will result in cluster failure)
3	2x	Can tolerate 1 node failure
3	3x	No Redundancy (node failure will result in cluster failure)
4	3x	Can tolerate 1 node failure
4	4x	NOT SUPPORTED

TABLE 9: SCALABILITY IN CLUSTERING

### Scalability – Multi-Site Clustering for Geographical Redundancy

RUCKUS SmartZone supports a “cluster of clusters” spread across multiple geographical sites for geographical redundancy and distribution. This topic is too vast for this guide so in such cases we recommend reaching out to CommScope Ruckus for guidance.

### Scalability – Calculating Management Bandwidth

RUCKUS SmartZone is designed to allow managing APs and ICX switches remotely. In fact, RUCKUS SmartZone uses standard secure internet protocols such as SSH and HTTPS to communicate with the APs and ICX Switches. This means network management is unaffected by latency, packet loss, and jitter and can be run over any IP public or private network.

When bandwidth is in short supply (such as in very remote locations with limited internet bandwidth or in the case of expensive bandwidth such as satellite connectivity on cruise ships), ensure there is enough bandwidth available to avoid saturating the link with management traffic.

Each AP and ICX switch establishes and maintains an SSH tunnel with RUCKUS SmartZone, through which it receives any configuration changes and periodically<sup>10</sup> sends back status messages and logs.

On average, each AP needs ~1-4 kbps and each ICX switch needs ~2-8 kbps during normal operation. When triggering a firmware upgrade, the devices will individually pull their firmware from the RUCKUS SmartZone using HTTPS.

- Packet Loss/Latency/Jitter not an issue
- On average, each AP needs ~16kbps and each ICX switch needs XXXX kbps
- Firmware upgrades will download a ~12MB file to every AP and a ~XXMB file to each ICX switch

---

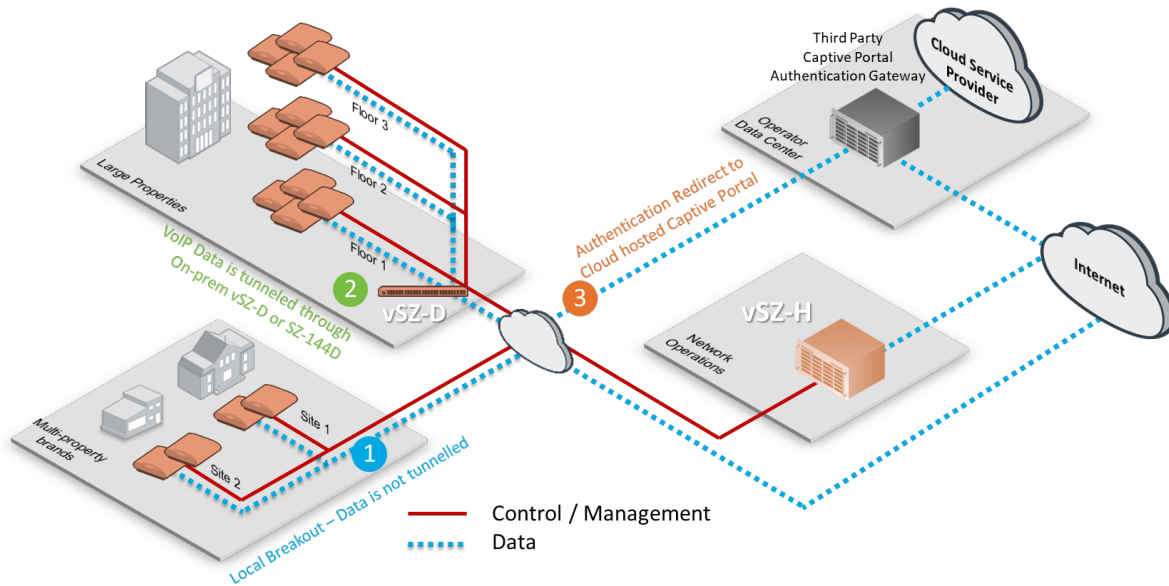
<sup>10</sup> The “period” depends on mode of operation. vSZ-E/SZ-100 = 5 minutes, vSZ-H/SZ-300 = 15 minutes.

**Tunneling**

In some environments, data traffic needs to be tunneled to a central concentrator (referred to as the dataplane) before it is ‘exposed’ to the underlying network. Tunneling can be enabled or disabled on a per-WLAN basis, so the same AP can tunnel *some* traffic while *not* tunneling other traffic.

All CommScope Ruckus AP models support tunneling.

The SZ-100 and SZ-300 already include a physical dataplane, no additional software, hardware or licenses are needed in this case.



**FIGURE 36: TRAFFIC FLOW FOR TUNNELED AND NON-TUNNELED DATA**

The vSZ does not have any tunneling support built-in. When tunneling is needed in a vSZ environment, a separate VM called vSZ-D or a physical unit called SZ-100-D is required.

Each vSZ node supports up to 10x vSZ-D or SZ-100-D dataplanes, for a total of 30x dataplanes per cluster.

Note: CommScope recommends tunnelling in the following environments:

- Any WLANs used for clients that are sensitive to roaming sensitive such as SIP VoIP handsets or payment terminals.
- All WLANs on APs that are running on a non-Ethernet underlying network ([GPON](#), DOCSIS, LTE, etc).

Note:

- SZ-100 and SZ-300 already include dataplane. No extra components or licenses are needed.
- For vSZ, a vSZ-D VM (licensed by bandwidth) or SZ-100-D physical appliance is required.
- Keep the dataplane within the same local LAN as the APs. Any latency will affect clients.

**Building the SmartZone Bill of Materials**

Once the platform for the controller is determined, create the component list for the controller.

Although there are 3 period options for support, the recommendation is to opt for at least 3 years of support to ensure support is maintained throughout the lifespan of the system.

As SKUs might change over time, always confirm the SKUs via the latest CommScope Ruckus Price List

**Virtual SmartZone (vSZ) Architecture**

SKU	Description	Quantity
L09-VSCG-WW00	Virtual SmartZone software virtual appliance, 1 Node, includes 1 AP license  (No built-in tunnelling support! See below)	1 - 4
L09-0001-SG00	AP management license, 1 Ruckus AP access point.	[number of managed Ruckus APs]
L09-0001-SGCX	Switch management license, 1 Ruckus ICX switch.	[number of managed Ruckus ICX switches]

TABLE 10: VIRTUAL SMARTZONE SKUS

Support Options	Qty	1 Year	3 Years	5 Years
Virtual SmartZone	1 - 4	S02-VSCG-1L00	S02-VSCG-3L00	S02-VSCG-5L00
AP License Support	[number of Ruckus AP licenses]	S02-0001-1LSG	S02-0001-3LSG	S02-0001-5LSG
ICX License Support	Not needed. ICX Support is purchased with the <u>switch</u> , not the <u>controller</u> .			

TABLE 11: VIRTUAL SMARTZONE SUPPORT SKUS



**Virtual SmartZone (vSZ) Optional Tunneling Support**

The following Dataplane nodes are needed to add Tunneling support only when using Virtual SmartZone.

The Virtual and Physical Dataplane Nodes can be mixed up to the total supported by the cluster.

Virtual Dataplane Node	SKU	Description	Quantity		
	L09-vSZD-WW00	Virtual Data Plane software virtual appliance, Base License (includes 1Gbps throughput)	1		
	L09-vSZD-BW10	Virtual Data Plane Bandwidth Upgrade – 10 Gbps Upgrade	(Optional)		
	Support Options	Qty	1 Year	3 Years	5 Years
	Virtual DataPlane (Base)	1	S02-VSZD-1L00	S02-VSZD-3L00	S02-VSZD-5L00
	Virtual DataPlane (10Gbps Upgrade)	1	S02-VSZD-1LBW	S02-VSZD-3LBW	S02-VSZD-5LBW
Physical Dataplane Node	SKU	Description	Quantity		
	P01-D144-XX00	SmartZone Data Plane Appliance, with 4x10GigE and 4 GigE ports (10Gbps throughput)	1		
	902-S110-0000	Spare/Secondary AC Power Supply	(Optional)		
	Support Options	Qty	1 Year	3 Years	5 Years
	SZ-144D SZ Dataplane Appliance	1	S02-D144-1000	S02-D144-1000	S02-D144-1000

TABLE 12: SKUs FOR TUNNELING SUPPORT

**SZ-100 Architecture**

SKU	Description	Quantity
<b>P01-S144-XX00</b>	SmartZone 144 Controller Appliance with 4x10GigE SFP+ and 4 1G Copper ports. Includes all fans. Includes 1 PSU.  (Includes Tunneling support, no additional components or licenses needed)	1 - 4
<b>902-S110-0000</b>	Spare/Secondary AC Power Supply	(Optional)
<b>L09-0001-SG00</b>	AP management license, 1 Ruckus AP access point.	[number of managed Ruckus APs]
<b>L09-0001-SGCX</b>	Switch management license, 1 Ruckus ICX switch.	[number of managed Ruckus ICX switches]

TABLE 13: SZ 100 SKUS

Support Options	Qty	1 Year	3 Years	5 Years
<b>SZ-144 Base Unit</b>	1 - 4	S02-S144-1000	S02-S144-3000	S02-S144-5000
<b>AP License Support</b>	[number of Ruckus AP licenses]	S02-0001-1LSG	S02-0001-3LSG	S02-0001-5LSG
<b>ICX License Support</b>	Not needed. ICX Support is purchased with the <u>switch</u> , not the <u>controller</u> .			

TABLE 14: SZ SUPPORT SKUS

SZ-300 architecture

SKU	Description	Quantity
<b>P01-S300-WW10</b>	SmartZone 300 (SZ 300) with redundant AC power, six (6) Fans, two (2) 10 Gbps data cards, and six (6) 1 GigE ports.  Doesn't include power cords.  (Includes Tunnelling support, no additional components or licenses needed)	1 - 4
<b>902-0174-XX00</b>	IEC Power Cord. Change "XX" in SKU to country code to determine plug type (US/AU/BR/CN/EU/IN/JP/KR/SA/UK)	2 per node
<b>L09-0001-SG00</b>	AP management license, 1 Ruckus AP access point.	[number of managed Ruckus APs]
<b>L09-0001-SGCX</b>	Switch management license, 1 Ruckus ICX switch.	[number of managed Ruckus ICX switches]

TABLE 15: SZ 300 SKUS

Support Options	Qty	1 Year	3 Years	5 Years
<b>SZ-300 Base Unit</b>	1 - 4	S02-S300-1012	S02-S300-3012	S02-S300-5012
<b>AP License Support</b>	[number of Ruckus AP licenses]	S02-0001-1LSG	S02-0001-3LSG	S02-0001-5LSG
<b>ICX License Support</b>	Not needed. ICX Support is purchased with the <u>switch</u> , not the <u>controller</u> .			

TABLE 16: SZ 300 SUPPORT SKUS

### Ruckus Unleashed

Unleashed is very easy to design – in fact there is nothing to design! Simply pick the APs and ICX switches you would like to use in a property, and that is it. There are no other components to pick.

A few key points to keep in mind with Unleashed are:

- Unleashed supports:
  - up to 128 APs
  - up to 2048 WiFi Clients
  - up to 8 ICX Switches
- Master AP is automatically elected by default, but this can be overridden.
- Master AP can serve up to 100 WiFi Clients.
- All non-Master APs can serve their respective maximum number of clients depending on model.
- Tunnelling is not supported.
- All APs and ICX Switches must be on the same Layer 2 network.
- Multi-SSID/Multi-VLAN is fully supported for WiFi clients and wired devices.

Unlike RUCKUS SmartZone or Cloud, AP or ICX Switch licenses are not needed for an Unleashed system to work.

Watchdog support is needed for each Unleashed network and for each AP over 25 APs. This entitles you to support from the CommScope RUCKUS Support Team, as well as access to all support documentation and firmware upgrades.

Support Options	Qty	1 Year	3 Years	5 Years
First 25 APs	1 per site	806-RUNL-1U00	806-RUNL-3U00	806-RUNL-5U00
26-128 APs	1 per AP	806-0001-1U00	806-0001-3U00	806-0001-5U00

TABLE 17: UNLEASHED SKUS

### Ruckus Unleashed Multi Site Manager (UMM)

If your customer is managing multiple small sites running Unleashed, they should consider deploying Unleashed Multi Site Manger (UMM) which allows them to manage multiple Unleashed systems centrally. For more information about UMM, please contact CommScope.

	Small Deployment (Up to 10 sites)	Large Deployment (Up to 300 sites)
<b>System Requirements</b>	Unleashed APs and ICX switches	Unleashed APs and ICX switches
<b>Additional Software</b>	None	UMM Software License UMM AP/ICX Management License
<b>Management</b>	Via WebUI or free mobile app	Centrally via UMM
<b>Support</b>	Unleashed Site Watchdog Support	UMM Software License Support UMM AP Management Support

### RUCKUS Cloud

RUCKUS Cloud offers a worry-free large-scale management platform. In fact, there is no limit to the number of APs and ICX switches that can be added.

It also has very powerful multi-site functionality that lets customers ensure consistent configuration across multiple sites without having to manually or programmatically touch every single site individual.

Finally, it provides a simple, high-level view of the network which instantly shows the network administrator any problems.

Note: RUCKUS Cloud only supports ICX model ranges 7150, 7650 and 7850. Other switch models can be used within the same network but in standalone mode.

Licensing for RUCKUS Cloud is a very simple annual subscription.

	1 Year	3 Years	5 Years
<b>Any Ruckus AP Model</b>	CLD-RKWF-1001	CLD-RKWF-3001	CLD-RKWF-5001
<b>ICX 7150-C08P</b>	CLD-S08M-1001	CLD-S08M-3001	CLD-S08M-5001
<b>ICX 7150 (any other)</b>	CLD-S71M-1001	CLD-S71M-3001	CLD-S71M-5001
<b>ICX 7650 (any)</b>	CLD-S76M-1001	CLD-S76M-3001	CLD-S76M-5001
<b>ICX 7850 (any)</b>	CLD-S78M-1001	CLD-S78M-3001	CLD-S78M-5001

TABLE 18: RUCKUS CLOUD SKUS

APs and switches managed by RUCKUS Cloud can be installed behind a NAT router. All management traffic is initiated by the AP or ICX Switch towards the RUCKUS Cloud servers, therefore no inbound NAT rules need to be configured.

The management protocols for RUCKUS Cloud are very similar to those of RUCKUS SmartZone. To learn more about the bandwidth consumption and latency requirements, please refer to the Scalability – Calculating Management Bandwidth section.

## Appendix – Miscellaneous Topics

### Painting Access Points

In some situations, there may be requests from interior designers, building owners, or even legal requirements to blend any components into the general look and feel of the existing wall or ceiling.

The official position of Commscope is that any physical modification to the hardware will void the warranty, so the normal recommendation recommend is to avoid painting the AP and instead use a non-ferrous enclosure or an existing visual barrier (E.g., furniture) to hide the AP. If this is not possible and the customer accepts voiding the warranty, the following describes how APs should be painted.

#### Painting an Indoor Access Point

In general, painting an indoor access point with common vinyl resin-based paints (latex or polyester), which are free of ceramic and metallic additives will not affect the wireless performance of the access point. Care should be given to mask connectors and product labeling before spray painting any product.



FIGURE 37: PAINTED INDOOR AP

An alternative to spray painting is vinyl wrap. Tested and recommended are 3M's 1080 line of vinyl wraps (including black); they do not interfere with RF performance.

[https://www.3m.com/3M/en\\_US/graphics-signage-us/1080-wrap-film-series/](https://www.3m.com/3M/en_US/graphics-signage-us/1080-wrap-film-series/)

#### Painting an Outdoor Access Point

In general, painting an outdoor access point will alter the thermal characteristics and the assured product specifications of the product. Specifically, the operating temperature range of the product may be significantly impacted when subjected to solar loading effects of outdoor installations. It is therefore recommended to avoid using dark colors in hot regions or any location where the AP will be exposed to continuous direct sunlight as this will shorten the lifespan of the product.

**Official CommScope Warranty Statement**

Altering Ruckus Wireless products in any way, including painting, voids the existing product warranty.

**Why Does the Warranty Not Cover Painted Products?**

Paints, primers, and common painting preparation techniques and painting application practices may subject the product to harmful chemicals that may damage or alter the plastics, circuit assemblies, gaskets or other materials used in the access point. CommScope cannot qualify or make assurances that the vast majority of paint products, painting processes, and workmanship quality will be compatible with or will be harmless to or will not impact the performance or reliability of Ruckus wireless products.



### CommScope Powered Fiber Cable System (PFCS)

The CommScope Powered Fiber Cable System is designed to mimic PoE in a fiber-deep environment and in long distance outdoor infrastructures.

Installation becomes like a POE application, in that the technician can place a single cable between the IDF/MDF and the network device location. Once the cable is terminated, connections to the device are made with a simple copper patch cord. The difference being that the channel lengths are greatly extended. Depending on the power delivery, distances can range from 600 meters / 2000 feet to 3,000 meters / 10,000 feet.

The Powered Fiber Cable System is composed of three main elements:

- Hybrid copper and fiber cable (indoor/outdoor)
- Fiber Backpack for indoor, PoE Extender or Power Extender for outdoor
- Power Supply / Power Distribution

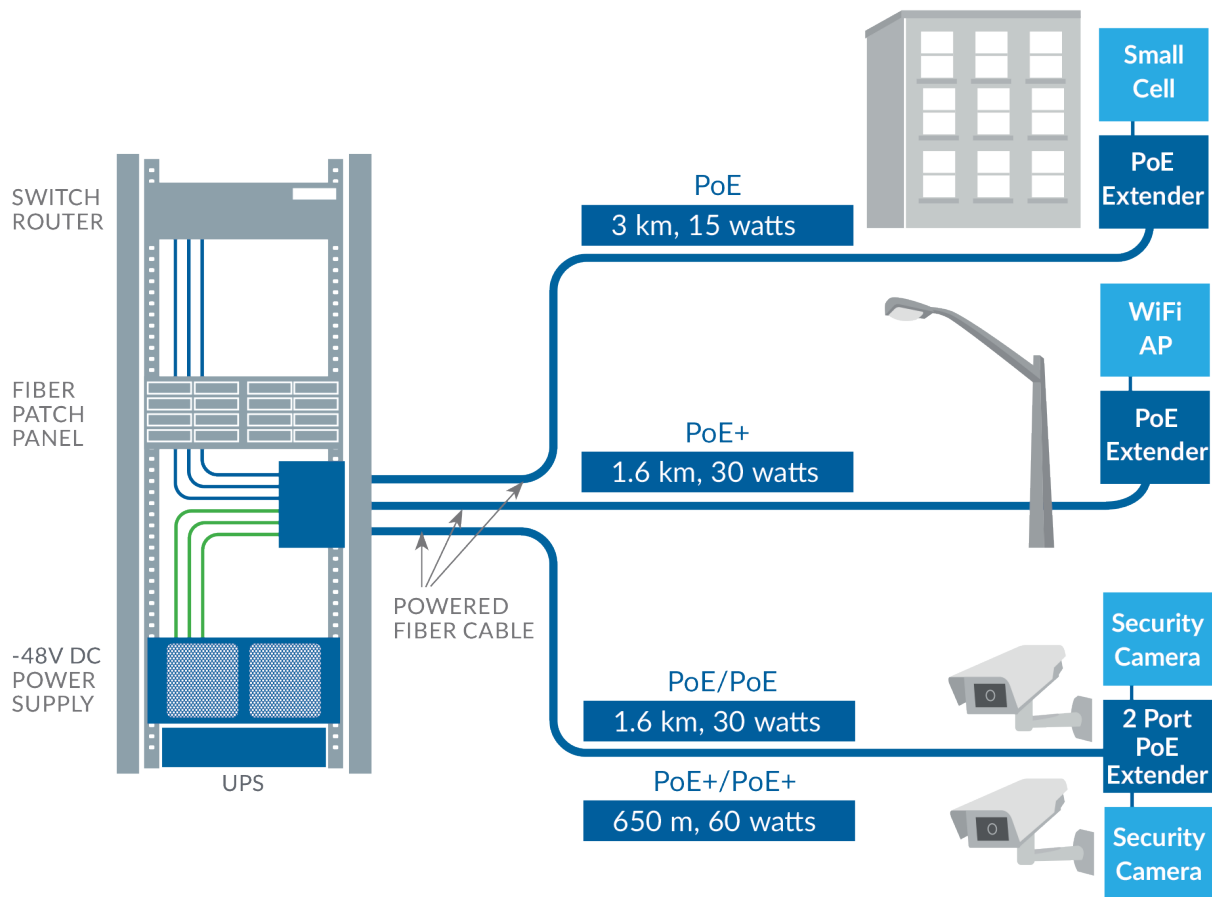


FIGURE 38: COMMSCOPE POWERED FIBER CABLE

The PoE and Power Extenders are the main component in the solution. This unit combines all the elements that would normally be required in the remote IDF into a single hardened and electrically protected device.

The PFCS hybrid cable will enter the Extender through a weather sealed grommet. The copper conductors are screwed down on a terminal strip. Note that there are several variants of the PFCS Extender unit but all variants are IP67 weather rated.

Product Name	Input Data Ports	Power Output Type
<b>1-port POE Extender</b>	2x SFP 1Gbps 1x RJ45 1Gbps POE	Max 60W POE Budget (depends on distance)
<b>2-port POE Extender</b>	2x SFP 1Gbps 2x RJ45 1Gbps POE	Max 60W shared PoE Budget (depends on distance)
<b>12V Power Extender</b>	LC-LC Passive Passthrough	Conditioned 12V DC on 2 wire terminals
<b>48V Power Extender</b>	LC-LC Passive Passthrough	Conditioned 48V DC on 2 wire terminals

TABLE 19: COMMScope POWERED FIBER CABLE

Since the PFCS cable can reach distances of up to 3Km / 1.8miles, the cable can be terminated in the MDF or an existing IDF rather than having to build an outdoor or dedicated IDF for your outdoor hardware.

In the MDF/IDF, the cable splits into a set of fiber strands and a pair of copper DC wiring. The fiber strands can be terminated and plugged into a standard Fiber port as you would a normal fiber cable. The DC pair is plugged into a power supply.

CommScope offers a power supply for use in the IDF/MDF. *However, it is important to note that our system does not require the use of this power supply. Any NEC Class 2 low voltage power supply which can supply 48VDC can be used with our system.*



Power Express Class 2  
shown here “fully loaded” with  
four 8 port modules



SPS Bulk DC Rectifier  
shown here “fully loaded” with 3 Rectifier  
modules and PSU controller

CommScope has partnered with ABB Industrial Supply to offer the Power Express DC Power Distribution solution. This power supply is modular and can easily accommodate expansion as the deployment grows. In a basic installation, one Power Express chassis will be coupled with 1 Slimline Power System rectifier chassis.

## Designing for Hospitality

The Power Express chassis can be populated with 4 DC distribution modules, each providing 8 individual DC output channels. When fully populated, the system can service 32x Extenders. Additional device support is available in more complex installations.

The Slimline Power System rectifier can be populated with 3 rectifier modules with each module delivering 1200 Watts of DC power. With the optional SPS controller, the Power Supply can be put on the Building Automation System Network, with remote monitoring and control. This may be desirable for larger installations.

## Why (not) PON/GPON/GEPON?

EPON, GPON, GEPON... these are all variants of the same technology architecture. While they all have their benefits, history and application, for the purposes of this document we will group them all together and call them xPON.

Let's make one thing clear. Commscope Ruckus does officially support running APs over a xPON network and we have several deployments using this architecture. If it is an absolute must that your infrastructure must run over a xPON network, don't worry, this is fully supported by Ruckus.

However, the main challenge is that xPON technologies are not designed for the flat Layer 2 network architecture in which we normally run our networks. For example, APs expect to be able to directly communicate with their neighbouring APs over their Ethernet backhaul. WiFi clients are constantly roaming from one AP to another and they expect that roam process to take less than 100ms. Client MAC addresses are constantly appearing and disappearing on different switchports upstream as clients roam.

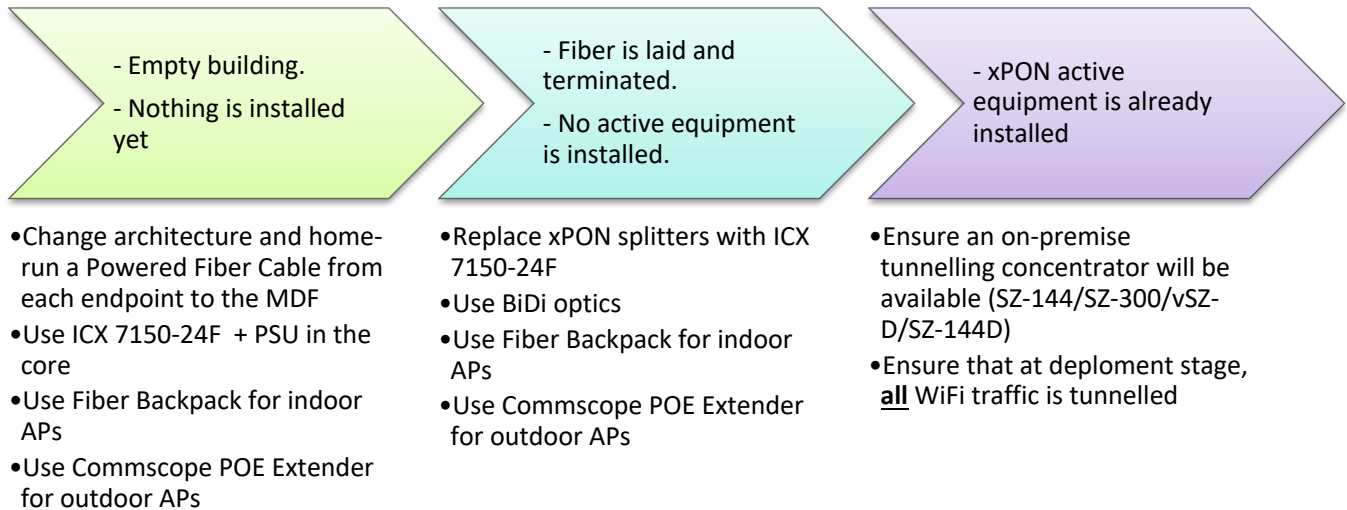
On the other hand, xPON is designed for the carrier market, where subscribers do not "roam" from their own home router/ONT to their neighbour's router/ONT. Roaming and peer-to-peer traffic commonly seen in WiFi and Wired Ethernet networks is often either simply not allowed by the ONT/OLT, or the high roaming rates overwhelms the ONTs or the OLT, whereas an Ethernet switch is designed to support this as it is designed to expect WiFi clients.

In our experience, we have seen all kinds of strange behaviours when a WiFi deployment is done on top of a xPON infrastructure. The symptoms usually are:

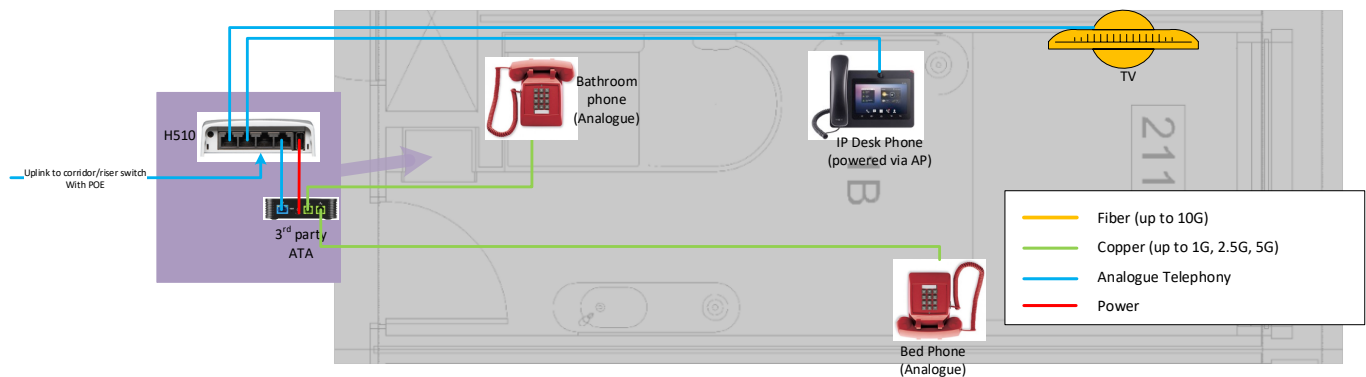
- Very high CPU utilization of the OLT – due to the frequent and rapid roaming of WiFi clients.
- Very, very long roaming delays - one particular case took 15 minutes to roam!
- High jitter – due to the shared access nature of xPON.
- ONT unreliability – ONTs are usually designed for the consumer market.
- ONT instability – ONTs are powered by a local PSU, which can fail or be unplugged.

Designing for Hospitality

Instead of xPON, we propose several different solutions. The choice depends on the stage of the deployment and the possibility of changing the architecture. Take a look at the following chart.



One argument in favor of xPON is the availability of ONTs with built in switch, analogue phone port and TV RF connection. The reality is that this is still possible even without xPON.



An H510 can be installed inside each guest room, replacing the ONT.

The H510 delivers WiFi, Wired connectivity to TV, and 1x POE IP Phone.

For additional analogue telephony, a 3rd party ATA can be powered by the H510's USB port for 2x analogue telephones.

## Glossary

Term	Description
<b>IDF</b>	Intermediate Distribution Frame. Distribution rack for one or more floors. For high-scale buildings there can be two (or more) IDFs per floor. This is the point where all the cables (copper-based) concentrate from a given floor.
<b>MDF</b>	Main Distribution Frame. Main rack for the building (or group of buildings), where all the cables (fibers usually) coming from IDFs concentrate. This is where servers and/or firewalls are connected.
<b>POE</b>	Power Over Ethernet: provides power up to 15.4 watts (802.3af) per port
<b>PoE+</b>	Power Over Ethernet: provides power up to 30 watts (802.3at) per port
<b>PoH</b>	Power over HDbaseT: can provide power up to 90 watts (802.3bt)



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

We encourage you to visit [commscope.com](https://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®**

**RUCKUS®**

---

[commscope.com](https://commscope.com)

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

© 2020 CommScope, Inc. All rights reserved.

Unless otherwise noted, all trademarks identified by ® or ™ are registered trademarks, respectively, of CommScope, Inc. This document is for planning purposes only and is not intended to modify or supplement any specifications or warranties relating to CommScope products or services. CommScope is committed to the highest standards of business integrity and environmental sustainability with a number of CommScope's facilities across the globe certified in accordance with international standards, including ISO9001, TL9000, ISO14001 and ISO45001. Further information regarding CommScope's commitment can be found at [www.commscope.com/About-Us/Corporate-Responsibility-and-Sustainability](https://www.commscope.com/About-Us/Corporate-Responsibility-and-Sustainability).