Rules for Successful Hotel Wi-Fi

We all have experienced terrible Hotel Wi-Fi… the travel guide, or online research showed ‘Free Wi-Fi’ – and then we end up on site with a horrible experience.

Wi-Fi in hotels does not need to be a bad thing… if you follow some best practices any hotel can offer its guests a great Wi-Fi experience!

First, let me say this is one man’s opinion. Perhaps there are others who might like some of the things I despise, or have unique cases where some of these rules might not be the most effective. I freely agree there are times when all these rules might not apply. But for the most part, the following will help your guests have exactly what they want… *Fast, Free, and Easy Public Wi-Fi*!

All about guest expectations
The entire reason for a hotel offering Wi-Fi to the guests is to help with the bottom line. Free Wi-Fi has become a necessity in the industry. Not only to get first-time guests, but especially to have return guests, the Wi-Fi needs to meet the expectations of the guests.

So when reading this post – remember to think ‘What would my guests want’ – that should be the driving factor behind all your Wi-Fi decisions.

The following are in no particular order – as long as you keep the first rule, above, in mind – you can work on the following in any order you like.

Do what is Right vs Doing what is Easy
This should go without saying… but here I am saying it up front and as the lead-in to all the other rules. Think back on WHY you are putting in public Wi-Fi… for your guests. Refer to rule one above. Designing a WLAN that meeting your requirements must be grounded in those very requirements. What DO your guests expect? Your job is to design the Wi-Fi to meet those requirements. Plain and simple. So do what is right, not take some easy way out.

Wi-Fi is NOT a commodity – check out this blog on just this subject.
http://www.wlanpros.com/wi-fi-%e2%89%a0-commodity/

Channel Plans
We’ve all seen the terrible Hotel Wi-Fi where each adjacent AP is on the next available channel. As you walk down the hall you hit Channel 1, then Channel 2, then Channel 3, etc. This causes massive Adjacent Channel Interference (ACI), and greatly reduces the available throughput on the network.

By way of contrast, the current hotel I’m working from today has all its access points set to channel 6. All of them – all 150 of them are all on the exact same channel. This causes a different type of interference called Co-Channel Interference (CCI). The designer of this hotel’s Wi-Fi didn’t understand the basic fundamentals of how 802.11 works. It is a Shared Medium – whereby all devices that can ‘hear’ each other are in a contention domain and defer to each other. So in this hotel all client devices and Access Points are basically in one large contention domain.

Sure – each device gets a great RSSI… but the noise floor is also very high, and since all devices hear each other, the retransmission rates are high, CRC errors are high, and the resulting data rates drop to bare minimum in spite of having a high signal strength.

Use the appropriate channel plans, in most countries a 1, 6, and 11 channel plan will work fine. Some countries might be able to implement a 4-channel plan like 1, 5, 9, 13 – but just be aware if there is a Channel 6 or Channel 11 nearby you might be increasing your ACI to a point where the additional fourth channel isn’t worth the effort.
2.4GHz vs 5GHz
We all know there are devices still lurking around without 5GHz capabilities. But luckily these are dwindling rapidly. The 2.4GHz ‘garbage band’ is just that – junk. It is full of other devices, Microwave Ovens, Bluetooth, Portable Phones, Video Cameras, etc. All have an equal right to use the unlicensed frequency – and do so with abandon. Additionally, since there are only three available channels – we have a very limited ability to get frequency reuse in most facilities.

Thus 2.4GHz is crowded, over-saturated, and very difficult to design around. But still necessary. Just don’t expect good things in the 2.4GHz band.

On the other hand – we have a wide variety of channels available to use in the 5GHz band. As well as the physics of RF allow for 5GHz signals to work over a smaller range. This is a good thing – a great thing even. We want small, tight, controlled coverage patterns around our Access Points – 5GHz gives this to us much better than does 2.4GHz.

Design for 5GHz, and then turn off 2.4GHz radios – perhaps ½ or more in order to minimize CCI in the 2.4GHz band.

802.11ac Channel Allocation (N America)

20MHz Channel Width
In 2.4GHz you really must use only 20MHz channels. But in 5GHz you have options for 40MHz or wider channels. Please only use 20MHz channels. For a couple of good reasons. First, you can get more Transmit Power going into a smaller channel footprint, thus delivering stronger RSSI to your client devices. In turn that will allow for higher data rates and more efficient airtime. Second, since many devices can’t use the 40MHz
channels, much of your limited RF frequency might be wasted. And third, you’ll have less chance for 5GHz co-channel interference because you’ll have access to more 20MHz channels to choose from.

A blog by Andrew Von Nagy on the subject of wider channels.
http://www.revolutionwifi.net/2014/08/quick-take-wider-channel-widths-are.html

Use all DFS Channels
There has been quite a bit of debate over the use of DFS channels. There were times where many client devices couldn’t see all DFS channels. Thus if your WLAN design was limited and didn’t have proper overlap, you might have a perceived hole in coverage for certain devices. This can be compensated for by proper design with both primary and secondary coverage (Overlap) with 5GHz dual-radio coverage everywhere.

More importantly, more and more client devices no longer have a limitation on seeing DFS channels.

Turn Off Low Data Rates
Turn off supported data rates of 1, 2, 5.5, and 11 Mbps. Yes – this will automatically not allow any 802.11b-only devices to connect. That is a good thing. I seriously doubt people who can afford a night in a hotel room still are using B-only devices. You don’t want those on your network anyway – they cause havoc and slow down all other devices and require protection mechanisms to be implemented that devastate your potential data rates.

Now on to the slower OFDM rates. I’ve seen good results turning off 6Mbps and 12Mbps and allowing only 18Mbps or higher. Some sites we’ve moved that up to a minimum of 24Mbps and seen even better results. But be a bit careful and measure before and after changes to minimize errors and average data rates.

The more devices that communicate at faster data rates, the more total net capacity you’ll have on your network.
SNR more important than RSSI
Like I alluded to in the previous rule – just having RSSI isn’t sufficient. The way 802.11 works is more based on Signal to Noise Ratio – the difference between the received signal and the ambient noise floor. The higher the SNR, the higher the potential data rates. We’d like each device to connect and use the highest possible data rate. Each device gets on and off the limited radio frequency and uses less of the airtime.

When either SNR drops, or interference climbs, client devices will receive errors or timeouts. These in turn force the client to communicate at a lower data rate. Thus using up more and more airtime as the data rate continues to shift downward.

Our goal should be to keep Errors at a minimum and SNR at a maximum. This might mean having fewer Access Points… counter-intuitive I know… but that’s how it works.

SoHo vs Enterprise Gear
I know I’m going to get in trouble with folks who are infatuated with buying the cheapest possible gear. But I have no problem stating you should be using Enterprise-class gear and NOT SoHo-class gear. You’d think this would be obvious… but many want to ignore the fact that equipment manufacturers actually use different components that work better than others. Not to mention man-years of coding of firmware to get the most possible out of the hardware.

In the industry there is a term, CoGS… for Cost of Goods Sold. Usually in the order of 1/6th or 1/8th of the retail price of the device. So if your retail price is $1,200 – the CoGS might be $200. If you think of SoHo devices that retail for $120… their CoGS might be only $20 of actual hard costs for the chips, case, motherboard, installation, packaging, etc. Think for a minute – the CoGS of a top-of-the-line enterprise AP is nearly double the retail price of a SoHo AP. Let that sink in for a minute.

There IS a huge difference between the capabilities – RAM, CPU, antennas, and hardware quality between SoHo and Enterprise gear. That will effect the results, especially as we add more and more load to our Wireless networks.
SoHo gear is designed and tested for the market intended – that of a house with a handful of Wi-Fi devices. If that is where you are putting your Wi-Fi – then by all means use SoHo gear. But a hotel is NOT a home environment, and needs a much higher standard of quality.


Access Point Placement
Like other devices placed in your facility – fire sprinkler heads, smoke detectors, exit signs, etc. – Wireless Access Points work best with ‘line-of-sight’ with the fewest possible RF attenuators or RF reflectors in between the AP and the client devices.

Placing AP’s above the ceiling tiles is usually a big no-no. Installing access points amongst ductwork causes higher multi-path and a less consistent RF signal to client devices. Causing higher error rates, lower data rates, and lowering overall throughput capacity.

Refer back to doing it correctly vs doing it easy. I can’t imagine a building inspector allowing all fire sprinklers to be hidden above the ceiling tiles only in hallways – so why do you think placing AP’s there is a good idea?

Here is an excellent document on Antenna/AP placement and choices: http://go.7signal.com/download-wlan-antenna-guide

Captive Portals
The bain of Guest everywhere… No one LIKES Captive Portals. You know, the thing that pops up in your browser making you read something, click something, turn over personal information, etc. before you can access the Internet.
Perhaps these are caused by people who have anal personalities and want to control everything for everyone. Or perhaps they became popular because lawyers wanted to get paid to write the Terms of Service.

But they are NOT required. Perhaps by some misguided policy they are recommended. But since no one likes them, why do we still have them?

If large multi-billion-dollar corporations like Disney or LaQuinta have pulled all Captive Portals from their public Wi-Fi – and you know they have boatloads of lawyers on staff – why does your lawyer still think these are necessary?

Perhaps you live in a country where you have misguided politicians who have passed silly laws thinking capturing extra information in a captive portal will help save your society from crime or terrorism… I say ‘pahrump’! Sorry that you have to live under stupid laws.

But for the rest of us – a Captive Portal is a waste of our time and effort.

Referring to the first rule – what do the guests want? They want the same type of experience they have at home. When a guest returns to a Disney property – your Wi-Fi device just works. Plain, simple, easy. It just connects and works like you’d have at home! Why can’t hotel systems work that way? Well they can. LaQuinta’s management went to their IT staff and asked that very question. Now any returning guest’s device automatically joins the Wi-Fi and ‘just works’. Brilliant!

Time Outs
A dreaded by-product of Captive Portals is the ‘time-out’ – after logging in to the captive portal, a timer starts, and upon some arbitrary time, the Wi-Fi stops working. Usually without any warning. The guest’s computer just stops working when accessing the Internet. Forcing a guest to go through a variety of maneuvers trying to figure out what is wrong. Perhaps calling on Tech Support – only to realize they have to again close a browser and re-open one – so they can trigger the Captive Portal to reset the timer.

This is just plain stupid.
The hotel operator saves no money, is protecting nothing, it is only causing a great hassle on their guests with nothing in return. This is normally turned on because some salesmen wanted to sell a ‘service’ of the Captive Portal and showed of this ‘great feature’ designed to keep people who already know the code to just repeat it over and over.

Like I said – just plain stupid. Turn off timers once and for all!

Use building materials in your designs
One of the hardest things to do in WLAN Design is to get Frequency Reuse. The ability to re-use a channel in multiple places in your venue. The more times you can re-use a frequency, the more total capacity you’ll have. Thus this should be the goal.

Because of this goal – you should NOT be placing AP’s in hallways. Because, when using Omni Antennas in hallways, the signals shoot directly down the hall and will easily interfere with other AP’s on the same channel. Instead, you can use the rooms themselves, as well as the bathrooms and hallway walls to keep RF apart. Place the AP’s in the rooms – and then the RF signals will have an easier time moving from room to room, and the bathrooms near the hallways will help block the signals from interfering with other AP’s.

I have seen a hallway placement work – but only with alternating directional antennas, each facing away from the hall into the rooms at the side.

Remember – the goal isn’t to do this easy, but to do it RIGHT. Hallway placements are easy – but they give you sub-optimal performance.

Why don’t hotels only put their fire sprinkler heads in the hallways? For the exact same reasons. You want the water in the rooms to put out the fire in the room.

Why don’t hotels put smoke alarms only in the hallways? For the exact same reasons. You want to sense a fire/smoke in the rooms and not in the hallways.

Why do you want to put AP’s in the rooms? Because that’s where the guests are! Not to mention, you’ll have much smaller contention domains, lower co-channel interference, and lower error rates, resulting in higher data rates for clients – and thus adding capacity to the wireless network.
WLAN design is all about Frequency Reuse – check out this post for more details: http://www.wlanpros.com/frequency-reuse/

Allow VPNs
This is an easy one. Allow VPNs across your guest Wi-Fi. Done.

Don’t charge extra for it. Having a VPN doesn’t cost you any more, allows your guests to be more secure. And did I say it doesn’t cost you any more – so don’t charge for something that is free.

Have enough DHCP Addresses
Nothing is worse than having a Layer 1/Layer 2 connection to the Hotel Wi-Fi and then receiving the APIPA address of 169.x.x.x and failing to access the Internet. This is a simple failure of not providing enough scope to your DHCP pool. So fix it already!

Backhaul
Sorry to have to state the obvious – but many times the Wi-Fi in the hotel is fine. But guests complain because they are part of a pool of 250 users all sharing a T-1 out of the hotel to the Internet. In today’s society, watching Netflix, YouTube, or Hulu is a normal expectation of Hotel Wi-Fi. Take the simple 3Mbps of a Netflix stream and multiply it by the number of rooms in your facility. Then double that. You can never have too much upstream bandwidth.

You say ‘But Keith, that costs money!’ – that is true. But it also costs money to provide and elevator to your guests. It also costs money to provide daily room cleaning to your guests. It also costs money to staff the hotel front desk for your guests. It also costs money to launder the bedding and towels for your guests. It is part of the business of being a hotel. Meeting the expectations of your guests.

So don’t be a miser. Buy as much bandwidth as you can.

One of the very best Wi-Fi experiences I’ve ever had was in a small Super-8 motel in Warner-Robbins Georgia. The room was small, the bed uncomfortable, and the ‘breakfast’ consisted of pre-packaged small muffins. But the Internet speeds were fantastic! I asked the management why the dichotomy. They
answered, “We don’t have the capital to fix the other things – but our fast, fiber to the Internet is lower than the cost of a single maid. Why not make something memorable and get return customers because of fast Internet?” – Why not?

Why are you throttling bandwidth?
This is kind of a tie-in with the backhaul rule above. Give the customers what they want. They don’t WANT to be throttled. So don’t do it. The additional costs of slightly higher backhaul are easily offset by the lack of customers complaining. Remember RULE ONE – what do your guests expect?

More AP’s does NOT equal more capacity
Perhaps you’ve met a WLAN salesman who doesn’t really know how 802.11 works – and since they get paid on commission, they’ll try to sell you more access points under the guise of adding capacity. Don’t be fooled.

802.11 and Wi-Fi is a contention-based protocol. Adding more AP’s without getting frequency reuse will actually lower your throughput. The number of access points you can have in your property is based on proper placement – remember, not in hallways – a good design will go a long way toward getting maximum capacity in your venue.

Not to mention – you’ll actually save money by buying only the access points you need that maintain the highest possible throughput capacity. Spend the extra money for a proper design, and you’ll save more than enough to cover it. You’ll not only save on Access Points, but also switch ports, cabling costs, and installation costs.

Antennas
Who’s afraid of the big bad directional antenna? <You know you just hummed along with that line>

So many are defaulting to looking at only AP’s with built-in omni-directional antennas. Don’t be fooled into thinking you have to use only omni antennas. There are a wide variety of antenna choices available to help your WLAN designers meet your specific needs. Yes, they cost a bit more, but you’ll usually need fewer AP’s overall, and you’ll have better results when you target where you want the RF signals to go.
Analytics don’t have to be intrusive
You can always get user count information, even down to the types of devices used by your guests directly from your Wireless Network Management System (WNMS). You don’t need a captive portal to gather analytical information. Many see certain analytical options as intrusive and asking for too personal of information.

Try getting the data you need to manage your Wireless LAN directly from the WLAN itself. You do not need those extra add-ons that your customers don’t want or need.

Control your DNS
There are options available to augment your current DNS. Perhaps directly from your ISP or other third-party DNS outfits that might add some capabilities to help your guests get the best possible experience while on your Hotel Wi-Fi.

Validate Your WLAN
After installation, and before turning over the WLAN to users – you’ll need to validate the network meets your design criteria. This includes doing a survey and analysis of the data to verify not only primary and secondary coverage. But also throughput, error rates, retry rates, and average data rates.

Here’s some more information on the subject:

Thank you, for reading to the end of this long list of rules for providing Hotel Wi-Fi that meets the expectations of your guests.

You aren’t a hotel? Well you know what? This was actually written so Schools, Hospitals, Restaurants, or any facility that provides guest access can also follow all the same rules.
If you are having any difficulty trying to explain some of these concepts to a non-technical audience, here is a graphical document you might want to use to help with some analogies.

Keith R. Parsons
Managing Director
Wireless LAN Professionals, Inc.
Wireless LAN Training/Consulting
383 Ridge Road
Orem, UT 84057-2770

Personal keith@wlanpros.com
Twitter http://twitter.com/keithrparsons
Facebook http://facebook.com/keithrparsons
LinkedIn http://linkedin.com/in/keithrparsons
Website http://WirelessLANProfessionals.com