

Global Guest Internet Access Standards



Version 2.1

Global Network Engineering

1. Document Version Control

Date	History	Version
08/07/2014	First Release – Duane Larson	1.0
11/06/2014	Updated – Michelle Robson	1.1
12/19/2014	Finalized – Duane Larson	1.2
01/27/2015	Updated with Tom/Neil comments	1.3
06/04/2015	Made Global – Duane/Neil comments	1.4
05/20/2016	Updated – Phil Jackson	1.5
10/20/2016	Updated – Phil Jackson -Added hardware references	1.6
2/15/2018	Updated – Phil Jackson UnoNet	2.0 DRAFT
6/27/2018	Reviewed Draft and Published – Phil Jackson	2.0
10/12/2018	Updated references Pwr and BTU calcs – Phil Jackson	2.1

1.1 Approval for Distribution

Date	Approval Name	Version
01/30/2015	Duane Larson	1.3
06/04/2015	Duane Larson	1.4
06/01/2016	Duane Larson	1.5
10/20/2016	Phil Jackson	1.6
2/15/2018	Phil Jackson	2.0 DRAFT
6/27/2018	Phil Jackson	2.0
10/12/2018	Phil Jackson	2.1

Contents

1. Document Version Control	2
1.1 Approval for Distribution	2
2. Scope	5
2.1 What Are The Changes?	5
2.2 Effective Date	5
3. General	7
3.1 Removal of End of Life Technology	7
3.2 Power Requirements	7
3.3 Circuit Standards and Rate Caps	7
3.4 Cabling Standards	7
3.5 Approved Hardware Manufacturer	8
3.6 Guest Gateway Device	8
3.7 Physical Security and Labelling	8
3.8 Wi-Fi Alliance Certification	9
3.9 In Room Wireless Access Points & Survey	9
3.10 Outdoor Coverage	10
3.11 Required Switches	11
3.12 Required Controllers	11
3.13 Required Access Points	12
3.14 Wireless APs with External Antennas	12
3.15 Access Point Accessories	13
3.16 RF Signal Strength (-65dBm Concurrent on 5GHz and 2.4 GHz Bands)	15
3.17 Data Rates	15
3.18 Wireless SNR (Signal to Noise Ratio 30dB)	16
3.19 Wireless Channel Bonding	16
3.20 Dual Band AP's	16
3.21 Port Security/Port Isolation	17
3.22 Power & BTU Calculations	19
3.23 UPS Requirements	19
3.24 3 rd Party Devices & Applications	20
3.25 Circuit Monitoring	20
3.26 AP Installation Best Practices	20
3.27 Ekahau Site Survey Pro & Ekahau Sidekick	21
4. SSIDs	25
4.1 Application of the StayConnected SSID's	25
4.2 Single Brand Hotels: SSID Naming Conventions	25
4.3 Dual-Branded Hotels: SSID Naming Conventions	26
4.4 Dual-Branded Hotels	26
4.5 Preconfigured SSID Matrix slots	27
5.1 Circuit Standards - Requirements	28

1. Introduction

This document sets out the standard network and device standards, which are to be used when deploying Internet Access Networks, globally, within any Hilton Family of Brands hotel.

There are many systems and components involved in a successful deployment. This includes LAN and AP/controller configurations, site surveys and AP implementations. Each element needs to be planned for carefully.

The goal of this standard is to ensure the delivery of the guest and staff services enabled on the network meets the modern demands of an evolving technology environment.

2. Scope

This document is applicable to any Hilton Family of Brands hotel deploying a new wireless network or modifying an existing wireless guest network. This includes managed and unmanaged locations and franchises at all Hilton Family of Brands globally. The standards that will be documented in the following sections have been communicated to our preferred Guest Internet Access vendors who are required to uphold our standards. For Hilton to continue to be the leader in guest wireless in the hospitality market we need to make sure that our standards provide our guests with the best user experience possible. In order to do this we need to make sure our hotels continue to have strong signal coverage with best in class equipment that meets the ever-growing needs of our guest's devices.

2.1 What Are The Changes?

- All equipment will come from a single OEM, and that OEM is Cisco. Specifically, utilizing Cisco's 100% cloud based and controlled Meraki line.
- **Wireless fundamentals remain largely the same. However you should review this document in its entirety.**
- Migration to new yard stick, Ekahau Site Survey Pro with Ekahau Sidekick minimum v9.2.2 This gear replaces the previous yard stick of AirMagnet Survey Pro and the Proxim 8494's
- Hotels will need a dedicated Cat6 cable for each guest room installed behind the TV at a mid-height at each guest room TV location. This cable may be shared with our currently prescribed WallPlate AP model, Meraki MR30H
 - If you have an existing Cat5e or Cat 6 cable in the guest room at the desk you can move the cable or elect to use a patch cord to get the wired connection behind the TV.
- All APs must be fed with a minimum of 30W of power (PoE+, 802.3at). No exceptions.

Return to [In Room Wireless Access Points & Survey](#)

Note: This document will contain external links to other documents maintained by other departments. Non-Hilton teams may not have access to these links. In such cases, you will need to request this document from your Hilton sponsor.

2.2 Effective Date

This document goes into effect, globally on 10/12/2018.

(This page intentionally left blank)

3. General

3.1 Removal of End of Life Technology

DSL - DSL deployments or “upgrading” of existing DSL of any type is strictly prohibited, it must be replaced with dedicated and home ran Cat6 cabling to each guest room TV within the property.

Mesh - This prohibition also applies to wireless point to point or wireless point to multipoint backhubs. Wireless mesh in any form is prohibited from being used in the delivery of GIA services.

- If wireless mesh is present, it must be replaced with dedicated and home ran cabling to each guest room TV within the property.
- If wireless point to point or wireless point to multipoint backhubs are present they must be replaced with proper fiber backhubs.

CMTS – CMTS deployments or “upgrading” of existing CMTS of any type is strictly prohibited. CMTS installs must be replaced with dedicated and home ran Cat6 cabling to each guest room TV within the property.

Load Balancers - Third party load balancing devices and solutions are not supported.

3.2 Power Requirements

In general, each Guest Internet Access (GIA) MDF and IDF locations requires a separate and dedicated 20A quad-gang outlet with an isolated ground. GIA outlet must be located within 2 feet and on the same wall as the rack where the GIA equipment will be installed. Each GIA closet must have an appropriately sized UPS for power conditioning. Large UPS units, may require the installation of larger amperage circuit(s). All electrical for GIA must meet Hilton standards and comply with the host country’s jurisdictional electrical and building codes. Note: Some closets may require 30A circuits. UPS units must be rack mounted in the GIA Racks. Do not use consumer grade or desk type UPS systems.

3.3 Circuit Standards and Rate Caps

It is vital that you strictly adhere to the minimum circuit standards for all installations. Refer to Hilton’s publication, entitled [Bandwidth and Circuit Guidance](#) for full circuit standard requirements.

Note: Non-Hilton teams will not have access to these links. They will need to request this document from Hilton.

3.4 Cabling Standards

Hotel cabling for Guest Internet Access must comply with Hilton’s [Global Design & Construction Standards for Technology](#) documents, which are listed by brand on The Lobby. Sometimes you may hear reference to “2518”; this refers to the cabling section number in the above linked standards.

Note: Non-Hilton teams may not have access to The Lobby. They will need to request this document from Hilton.

3.5 Approved Hardware Manufacturer

All wireless access points, antennae, switches, associated peripherals, and licensing will be sourced and manufactured from Cisco's Meraki line. Each AP is required to have dedicated WIDS/WIPS and BLE radios and secure mounting brackets. Return to [Required Switches](#)

All Cisco Meraki hardware used must comply with the requirements set forth in this document and all pieces must be sourced and covered by a 5 year initial license.

All switching infrastructure used must comply with [Corporate and Hotel Meraki Network Hardware Standards](#) document, which is linked above.

Approved AP Table is located in [Required Access Points](#)

Approved AP External Antenna Table is located in [Wireless APs with External Antennas](#)

Approved AP Mounting Accessories Table is located in [Access Point Accessories](#).

Note: Non-Hilton teams may not have access to some or all of these links. If that's the case, they will need to request the materials via their Hilton Sponsor.

3.6 Guest Gateway Device

Refer to [Corporate and Hotel Meraki Network Hardware Standards](#) document for gateway model and information.

3.7 Physical Security and Labelling

All network gear deployed within a hotel must be secured so that no one can remove or tamper with the equipment and its cabling. GIA network closets (MDF and IDF's) must be physically secured with locks and only be accessible by authorized personnel. If an IDF must be located in a guest accessible area then all equipment, patch panels, terminations, electrical, UPS etc. must be fully contained within an appropriately rated, locking, and properly ventilated enclosure. If wireless AP's are accessible to non-hotel personnel then they should be properly mounted to the wall or ceiling using manufacturer provided secure mounting brackets. All AP's must be physically secured to their individual mounting bracket with an appropriate physical security mechanism that is not plainly visible and that Hilton deems is aesthetically pleasing. All AP's will be labeled as describe below. Host country's jurisdictional electrical and building codes must be strictly followed.

All Guest Internet Access equipment, including UPS units, must be rack mounted, and clearly and discretely labelled with their respective designations. All labels for GIA equipment must be made using a white background label. The label must be machine printed in black, with all capital text onto plastic, self-adhesive, thermal, or laser printed labels. Label height must be between 1/4" and 1/2". This standardized labelling ensures all equipment is easily identifiable for maintenance and support purposes. Example **MEMHQ-MR30H-MDF-AP001**, **MEMHQ-MS350-IDF01-SW001**, **MEMHQ-2902-MDF-**

RTR001, MEMHQ-MX250-MDF-MX01. Failure to comply with racking and labelling requirements will mean a revisit at vendor's expense to make corrections.

3.8 Wi-Fi Alliance Certification

Hilton requires the exclusive use of Cisco's Meraki AP's. Cisco has an unmatched record of Wi-Fi Alliance certification and leads the industry in ensuring its products are Wi-Fi CERTIFIED™. This certification reduces support costs and ensures a product has met industry-agreed requirements and standards.

The Wi-Fi CERTIFIED™ logo is an internationally recognized seal of approval for products indicating that they have met industry-agreed standards for interoperability, security, and a range of application specific protocols.



Wi-Fi CERTIFIED™ products have undergone rigorous testing by an independent Authorized Test Laboratory. When a product successfully passes testing, the manufacturer or vendor is granted the right to use the Wi-Fi CERTIFIED logo. Certification means that a product has been tested in numerous configurations with a diverse sampling of other devices to validate interoperability with other Wi-Fi CERTIFIED™ equipment operating in the same frequency band(s).

Certification is available for a wide range of consumer, enterprise, and operator-specific products, including smartphones, appliances, computers and peripherals, networking infrastructure, and consumer electronics. The Wi-Fi CERTIFIED logo gives consumers confidence that a product will deliver a good user experience and meet industry standards.

3.9 In Room Wireless Access Points & Survey

Hilton requires Guest Internet Access (GIA) vendors to survey with and deploy Cisco Meraki's 100% cloud managed and controlled wireless access points inside guestrooms. In all cases, vendors will conduct physical onsite "AP on a stick" (APoS) Site Surveys utilizing the software and hardware detailed in [What are the Changes?](#) & [Ekahau Site Survey Pro & Ekahau Sidekick](#). This "click and go" or "sample on click" physical survey will dictate RF design and AP density. All "wall plate" style AP mounting locations in guest rooms will generally be indicated by a room's individual TV location(s). DO NOT USE HALLWAY BASED AP's FOR IN ROOM GUEST COVERAGE.

There are two possible AP mounting scenarios. Legacy Wall Plate and Greenfield. Each will be described below.

1. **Legacy Wall Plate Locations** are defined as those locations that may have a previously low or high mounted Wall Plate style access point from Cisco, Aruba or Ruckus. It is ok to reuse some or all of these AP mounting locations with the new Meraki MR30H's if all of the following is true:
 - a. Post installation Wireless signal on 2.4 and 5GHz meets Hilton's minimum requirements as set forth in this document.
 - b. A patch cord can be ran from the wall plate's PoE out port "Eth1" to the back of the television set. Patch cord must be easily concealable within the junction where the flooring and baseboard meet the wall, completely concealed within the cavity of the wall, OR left neatly in open at brand and GM's discretion. Note: ***If an AP endpoint location is left in open or at desk level or above built in case goods the cabling may have to be concealed or relocated to meet brand's specific aesthetic requirements.***
2. **Greenfield Location**, in this context, applies to physical rooms which are newly built (new construction) **and existing room locations where a cable has not been previously ran.** If you encounter a room without an existing hardwired gigabit certified Ethernet run, then a new run must be installed centered midway up the wall and behind EACH TV within the guest room. Certain case goods and case goods with integral TV mount types may require mounting the AP (if present) off to one side or the other. In these cases, an AP surface mounted security bracket will be required. The idea is that if needed an AP could easily be installed, if needed, at a future time.

Future revisions of this document will include diagrams.

3.10 Outdoor Coverage

All outdoor coverage locations or areas that are exposed to the elements where weather, water, and/or dust ingress is a concern, must utilize Cisco Meraki outdoor specific ruggedized AP's that are purpose built for the demanding environmental requirements of the physical and geographical location in which they will be installed. All Cisco Meraki outdoor APs are IP67 rated and tested to protect against dust ingress, shock, vibration, and moisture ingress. Example outdoor /ruggedized locations, but not limited to- kitchens, food prep areas, garages, pool areas etc... DO NOT INSTALL INDOOR AP's OUTSIDE

Outdoor AP models are listed within [Required Access Points](#) and mentioned in [AP Installation Best Practices](#)

Outdoor AP locations with exposed cabling must use Outside Plant-Shielded Twisted Pair (OSP-STP) cabling and/or OSP rated patch cords with appropriate cable glands that maintain the AP's IP rating. All outdoor AP's must be grounded/bonded using a dedicated earth ground and utilize manufacturer (Meraki) approved and appropriately rated antennae with proper lightning arrestors. All host country jurisdictional electrical and building codes will be strictly adhered to and followed.

If the Meraki outdoor AP is installed and exposed to the elements, it must be properly grounded to prevent damage to the AP, connected networking equipment, and the mounting structure. The outdoor AP can suffer several types of failure in the field due to a lack of grounding.

Protecting the Antenna(s) - A direct strike will destroy any antenna. The best chance of avoiding damage to an antenna from a lightning strike is to prevent a strike from occurring. Structures can be equipped with structural "lightning-rods" in accordance with building codes and recommendations for the area.

Protecting the Access Point - The best way to protect the AP itself from direct strike is to avoid a strike. However, in the event of a strike, some protection for the hardware and most importantly the structure, can be achieved through the use of a surge arrestor. A lightning surge arrestor generally installs on the base of the antenna, between the antenna and the RF connector on the AP housing. It contains a fuse device (generally a fast acting gas discharge fuse) that triggers during a strike and channels the energy to a dedicated local grounding point. Surge arrestors have a small amount of signal loss, but are a worthwhile investment for access points installed in hard to reach areas or high up and likely to attract strikes.

Protect the Structure -The ground structure for the access point, the antennas, and the cables must be built in accordance with building codes. On any given mounting structure, a protection system typically includes a rooftop network of conductors, multiple paths to the ground, connections to the metallic portion of the structure and a grounding network.

Static Build-up - Static build-up can cause slow and irreversible damage to the access point. This may present itself as a reduction in Transmit Power and Receive sensitivity over time, or may show as a sudden death of Ethernet communication on the active port(s). Excess static in the environment builds up on the antenna element or system ground, damaging the sensitive components when the concentration is high.

Static is especially noticeable when conditions are suitable for thunderstorms. Warm, dry, and windy conditions dramatically increase the failure rate of unprotected equipment. Damage from static build-up can be prevented with proper grounding. It is suggested to install a grounding strap from the antenna ground to a well-designed local earth ground. A grounding strap can be made from a ring lug terminal (1/4" thin metal ring) and a medium length stranded copper wire (no more than 5 meters, suggested gauge AWG 14 or lower). It can be connected to the antennae connectors below the antennae. (There is 1-2mm of space below the bottom of the antenna and above the enclosure nut). The other end of the wire should be firmly attached to a grounding structure.

Protecting the interior network and electronics - In the event of a strike that damages or destroys the access point installed outside, it is important to isolate and protect any equipment inside. Excess energy on the access point that can't find its way to local earth ground will transfer to the interior equipment over the communication and power cable. A surge arrestor designed for use with Cat-6 cable must be used to prevent damage to equipment that is not directly exposed to the elements.

Note: When surveying with outdoor Aps with external antennae's you must make sure that your antennas have their lightening protection installed on each element to account for the slight signal loss they induce. It is never acceptable to survey for outdoor locations using an indoor AP.

3.11 Required Switches

Refer to section [Approved Hardware Manufacturer](#)

3.12 Required Controllers

A physical appliance is no longer required on premise. The next logical evolution is here, and that evolution is the Meraki Cloud Controller which features centralized management and eliminates the

need for costly on-site hardware controllers which constantly require upgrades, power, and rack space. The Meraki Cloud Controller offers superior network-wide visibility, control and is massively scalable. The wireless network traffic does not pass through the cloud controller, so the network stays up even if the connection to the cloud is lost. Some of its key features include automatic RF optimization, network monitoring and alerting, along with seamless firmware and security updates that protect our guests, our hoteliers, and Hilton.

3.13 Required Access Points

In combination with the wireless cloud controller mentioned previously, Hilton requires the exclusive use of Cisco Meraki 802.11ac Wave 2 AP's in all areas that are covered by Wi-Fi. This requirement is applicable to Hilton's Family of brands globally, without exception, for all areas including, but not limited to, all public, indoor, outdoor, Heart of Hilton, and meeting space/areas indoors and/or outdoors.

Suitable AP models are limited to the models shown below:

Return to [Approved Hardware Manufacturer](#) or [Outdoor Coverage](#)

Device Type	Model	Purpose
AP, Wall Plate, Indoor use	MR30H	In-Room Wireless
AP, Traditional Style, Indoor use, Low Density	MR42/42E**	Hallway Coverage and low capacity areas only
AP, Traditional Style, Indoor use, High Density	MR52/53/53E**	Lobbies Public Space and Gathering areas
AP, Traditional Style, Indoor use, High Density	MR52/53/53E	Conference facilities
AP, Traditional Style, Outside use, High Density	MR84*	High-density outdoor, garages, etc.
AP, Traditional Style, Outside use, Low Density	MR74*	Low-density outdoor, garages, etc.

* MR74 and MR84 use external antennae for Ruggedized APs.

** MR42E and MR53E use external antennae for indoor and are to be used as indicated in table above in areas where directional coverage is needed.

3.14 Wireless APs with External Antennas

External antennas are to be used indoors and outdoors when needed. It is up to the Guest Internet Access vendor to determine how to use them. All external antennae must be AP manufacturer approved. External Antennas must be manufactured for the specific Cisco Meraki AP model and not violate any AP's manufacturer's compliance with FCC statutes or affect AP's, FCC, or host country's local regulatory compliance. Return to [Approved Hardware Manufacturer](#)

Indoor Models	Link	For use with:
MA-ANT-3-A1, A5, & A6*	Data Sheet	MR42E & MR53E
MA-ANT-3-B1, B5, & B6*	Data Sheet	MR42E & MR53E
MA-ANT-3-C5 & C6	Data Sheet	C5 MR42E C6 MR53E
MA-ANT-3-D5 & 6	Data Sheet	D5: MR42E D6: MR53E
MA-ANT-3-E5 & 6	Data Sheet	E5: MR42E E6: MR53E
MA-ANT-3-F5 & 6	Data Sheet	F5: MR42E F6: MR53E

Outdoor Models	Link	For use with:
MA-ANT-20	Data Sheet	MR74 & MR84
MA-ANT-21	Data Sheet	MR74 & MR84
MA-ANT-23	Data Sheet	MR74
MA-ANT-25	Data Sheet	MR74 & MR84
MA-ANT-27	Data Sheet	MR74 & MR84
AIR- ANT2513P4M-N	Data Sheet	MR84

3.15 Access Point Accessories.

All newly purchased AP's will ship with their standard mounting brackets and accessories. However for various reasons it may be necessary to purchase additional mounting hardware and accessories. Use the accessories below when needed for mounting AP's and external AP antennas. Return to [Approved Hardware Manufacturer](#).

Mount Kits	Description	Info	link	For use with:
MA-MNT-ANT-3	Fixed Mounting Bracket	MA-MNT-ANT-3 (Horizontal Mounting Bracket)	Data Sheet	MA-ANT-3-C5 & C6
MA-MNT-ANT-4	Fixed Mounting Bracket	MA-MNT-ANT-4 (Vertical Mounting Bracket)	Data Sheet	MA-ANT-3-D5 & D6
MA-MNT-ANT-1	Articulating Arm Mount	MA-MNT-ANT-1 (Standard Mounting Arm)	Data Sheet	MA-ANT-3-E5 & 6
MA-MNT-ANT-2	Articulating Arm Mount	MA-MNT-ANT-2 (Long Mounting Arm)	Data Sheet	MA-ANT-3-F5 & 6
MA-MNT-MR-H1	Replacement Accessories	Indoor Use	Data Sheet	MR30H
MA-MNT-MR-H2	Wall Plate Surface Mounting Bracket	Use to relocate AP on the wall where no dedicated single-gang surface mount box is installed or over single gang boxes with shared service to allow physical pass-through of connections.	Data Sheet	MR30H
MA-MNT-MR-H3	Wall Plate Mounting Bracket w/ Integral Wired Switch Port Security	Cannot be used without a single-gang flush mounted opening	Data Sheet	MR30H
MA-MNT-CLG-1	Ceiling Mount, DEEP	Indoor Use	Data Sheet	ALL MR and MV except MR30H
MA-MNT-MR-7	Replacement Accessories	Outdoor Use	Data Sheet	MR74
MA-MNT-MR-8	Replacement Accessories	Indoor Use	Data Sheet	MR42
MA-MNT-MR-9	Replacement Accessories	Indoor Use	Data Sheet	MR52 and MR53
MA-MNT-MR-10	Replacement Accessories	Outdoor Use	Data Sheet	MR84

(This page intentionally left blank)

3.16 RF Signal Strength (-65dBm Concurrent on 5GHz and 2.4 GHz Bands)

Return to [Ekahau Site Survey Pro & Ekahau Sidekick](#)

Hilton's wireless RF (Radio Frequency) standard is continually evolving to meet the needs of future technology. The overwhelming majority of devices today can communicate on, and actually prefer the 5GHz spectrum. Dual band concurrent use AP's directly allow for more clients to connect to a single AP and not contend for valuable airtime. Modern clients can use the 5GHz spectrum while the others can use the 2.4GHz spectrum. A strong RF signal allows and enables clients to receive a more stable connection. The more stable the connection, the less retransmits. The less retransmits, the greater the download speeds. All of these combined enables an enhanced guest/user experience.

It is not a good idea to crank the AP broadcast/transmit power to its highest level. Just because the AP is broadcasting at the max doesn't mean the wireless clients will get better performance. In fact, doing this often causes issues that will severely degrade wireless performance, as Wi-Fi is a two-way radio transmission. Mobility centric devices like smartphones and tablets still need to have adequate power to transmit back to the Access Point; even though the AP's transmitted signal to the endpoint is strong doesn't necessarily mean the guest user performance is going to be good. To make sure client devices don't have this issue, we need to survey with an RF signal that is at less than full power. **All site surveys will be taken with survey Access Points' transmit power set no higher than 14dB on both bands.** A key advantage of surveying at lower power levels is that it allows for a "self-healing" network. As the noise floor increases over time this allows for power to be dynamically adjusted to compensate for interference and environmental variables that are out of anyone's control. In general, the closer your APs are to your actual user's devices, the faster their device will perform and the more enhanced their experience will be.

Hilton requires all wireless designs and implementations to deliver no less than -65dBm on the 5GHz and 2.4GHz frequency bands, simultaneously, to the target areas with minimum modulation of 64-QAM 2/3 @ 30dB SNR or greater. Recall that you are surveying and planning for an SNR that is considerably higher than 30dB on 5GHz with a 40MHz wide signal. Coverage areas include the "four corners" of a guest room including the guest bathroom and all other guest facing areas within the boundaries of the hotel. Any additional hotel designated coverage areas (garages, shops, balconies, back office etc.) must also conform to these requirements. Hilton's survey standards and methodologies will be managed and dictated by our preferred Guest Internet Access vendors. Vendors are required to completely remove 802.11b rates and adjust 2.4GHz OFDM rates and/or completely remove 2.4GHz OFDM completely from select AP's/AP groups/profiles to eliminate and/or mitigate co-channel interference (CCI) and adjacent channel interference (ACI) to within industry acceptable norms. Although CCI and ACI is less likely on the 5GHz band, it is the vendor responsibility to continually monitor, and eliminate if either are present on any 2.4 or 5GHz channel in use.

3.17 Data Rates

Hilton requires the disablement of HR/ DSSS 802.11b rates (1, 2, 5.5 and 11Mbps). We also recommend that the base OFDM data rates no lower than 24Mbps on both 2.4 and 5GHz bands to control roaming and cell sizes

802.11ac only operates in the 5GHz band, so it should come as no surprise that the overwhelming majority of your bandwidth and raw speed is realized by using 5GHz. The original 2.4GHz 802.11 DSSS standard was approved in July 1999 at 1 and 2 Mbps; subsequently it was amended in 2003 to add 5.5 and 11Mbps. The modulation and data rates used by this archaic standard are stone aged when compared to today's MIMO and MU-MIMO wireless standards. 802.11b severely hampers the channel use and actually slows the entire wireless network, impacting all devices that use the 2.4GHz band.

3.18 Wireless SNR (Signal to Noise Ratio 30dB)

When a wireless signal is received, the amplitude of the signal is important. However, the usefulness of that Wi-Fi signal is determined by its distinction/measurement relative to the amount of noise (noise floor) and other RF interference that may be present. SNR is the ratio between the maximum signal strength that a wireless connection can achieve and the ambient noise present in the connection. Noise is defined as any overlapping frequency that cannot be demodulated by the AP's radios. It can be other stray frequencies like malfunctioning wireless networks in the area, Bluetooth, wireless cameras, DECT phones, electrical wiring, and microwaves or even added by natural phenomenon. For example, if signal level is measured from an AP @ -65dBm and the noise floor is at -95dBm we have an SNR of 30dB. If the same AP gives the same signal level of -65dBm but our noise floor has elevated to -75dB, the signal quality would be worse by 20dB (SNR of 10). These differences will cause transmission errors, resulting in rate shifts that decrease the wireless data connection speeds which will degrade the wireless network. SNR of the wireless network needs to be as high as possible in order to allow higher data throughput which reduces a client's airtime. (Reduced airtime is good) Technology has evolved and people expect to be able to stream high quality video, which requires higher throughput than casual web browsing. If a hotel has a low SNR, AP placement is critical and more AP's (higher density) are usually needed with appropriately managed power settings.

Hilton requires all vendors to survey for 40MHz wide 5GHz and to deploy 802.11abgnac networks with a minimum SNR of 30dB or higher at install date utilizing the minimum in-band power for each frequency required to achieve the desired signal and SNR results. Subsequent diagnostics will need to be performed during the life of the install to validate the SNR.

3.19 Wireless Channel Bonding

Channel bonding allows clients to have higher throughput. Channel bonding requires adequate RF signals (See Wireless RF Signal Strength section for minimum standard). If the RF signal is weak the use of channel bonding becomes much less effective in providing a throughput boost.

With a 40MHz wide channel a 2x2:2 ac radio, allows for the data rate range to increase from 300Mbps to 400Mbps on dual stream capable devices and from 72Mbps to 200Mbps on single stream 802.11abgnac devices. Clients that are transmitting faster and clearing the air faster allows more devices to send more data in a much shorter time frame. This is analogous to a highway in a metropolitan area. If we have heavy traffic on a free-way (channel) all traffic (your users data) has to slow down to accommodate the overuse. Sometimes traffic (data) must come to a complete stop, when the traffic (data) stops and starts each time, the speed (data rate) gets slower and slower (part of the 802.11abgnac standard) until its destination (the AP) is reached or until you give up and exit the free- way. Adding an additional lane to our existing highway (channel) allows us to increase the size of path travelled to move the traffic (data) more quickly and efficiently.

Hilton requires all surveys to be conducted at 40MHz wide on the 5GHz frequency with the required signal strength and minimum SNR stated within [Wireless SNR](#). Channel Bonding is for 5GHz only.

3.20 Dual Band AP's

Dual band (2.4GHz and 5GHz) concurrent use radios allow for more client capacity on a single AP. Hilton requires an AP's Wi-Fi Alliance Interoperability Certificate be listed as:

Frequency Band(s) 2.4 GHz, 5 GHz – Concurrent

3.21 Port Security/Port Isolation

It is imperative that guest devices should not be able to reach one another over the GIA network, to prevent possible security breaches between clients.

Port security and port isolation will be used to protect guest devices across the Guest Internet Access network. Protected ports provide a form of security by not forwarding ANY traffic to any other port that is also protected on the same switch. All traffic passing between protected ports must be forwarded through a layer 3 device, such as a router.

Meraki APs feature a firewall on each AP and they establish their layer2 isolation a little differently than the previous generation of legacy AP's. Navigate here for a full description of the Wireless Client Isolation feature (aka Layer 2 LAN Isolation) documentation: [Wireless Client Isolation](#)

Note that the doc says that this feature is available in 25.8, which is true but Hilton is requiring a newer version. **Please ensure that all Meraki AP's have at least 25.9 firmware.** Once you have upgraded the APs to 25.9, you will see the Layer 2 isolation feature. You can enable this feature via the Meraki Dashboard: **Wireless>Configuration>Firewall & traffic shaping**. Below is a screenshot of what it looks like, including an additional firewall rule to allow ping to the gateway.

Firewall & traffic shaping

SSID: G6iso

Block IPs and ports

Layer 2 LAN isolation Enabled (bridge mode only)

Layer 3 firewall rules ⓘ

#	Policy	Protocol	Destination ⓘ	Port ⓘ	Comment	Actions
1	Allow	ICMP	192.168.100.1/32	Any	Allow Gateway Pings	⊕ ×
	Deny	Any	Local LAN	Any	Wireless clients accessing LAN	
	Allow	Any	Any	Any	Default rule	

[Add a layer 3 firewall rule](#)

In the example, you can see that there is a rule, the “Local LAN” firewall rule which is set to Deny. This rule prevents wireless clients, on this SSID, from reaching any private IP addresses (RFC 1918); only public IP address. **Note: DNS and DHCP traffic is exempt from this rule.** Also, this feature can be used in both Bridge Mode and NAT Mode. Here’s the KB on this feature: [Deny Local LAN](#)

Even though the client traffic is dropped at the AP edge, Port Protection mechanisms must still be set on all switches just as it always has been done. Note that the Meraki Cloud Controller is not shown on the diagram below. Future release of this document will contain a newer diagram.

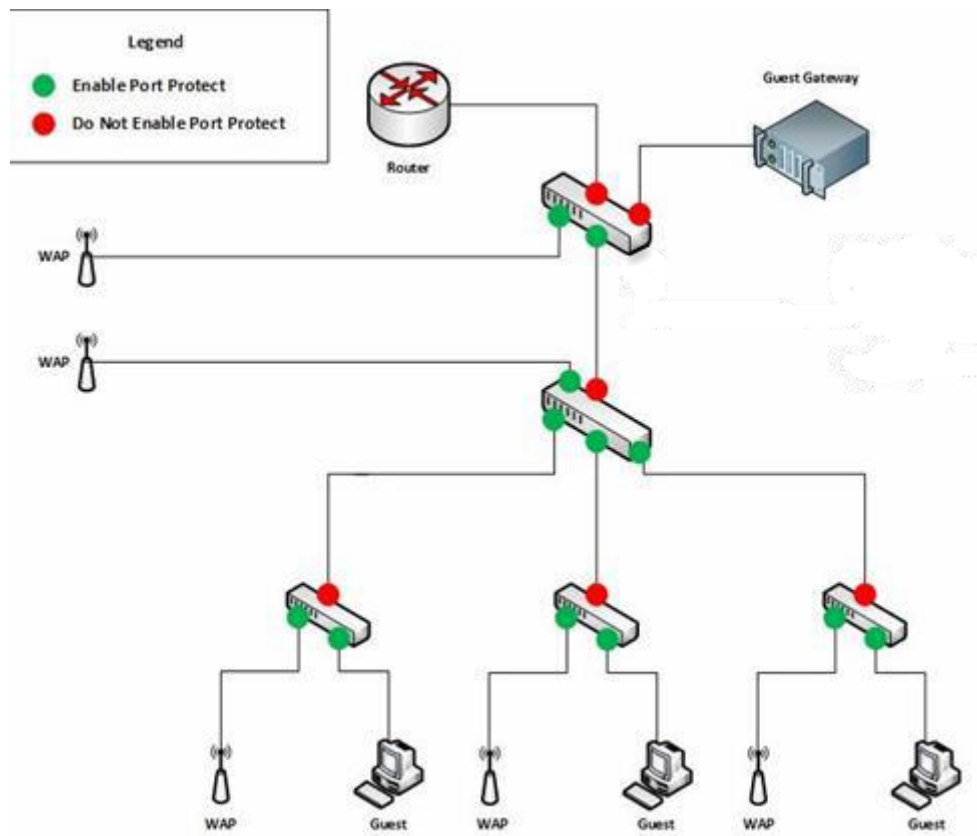
Where to enable switchport protected

- Enable on trunk ports to downstream switches
- Enable on access ports to wired guestrooms
- Enable on trunk ports to Access Points

- Enable on ALL guest facing WLANS
- Enable on Parent Etherchannel trunk ports on Meraki switches

Where not to enable switchport protected

- Do not enable on trunk ports to switches that are closer to the Guest Gateway
- Do not enable on Guest Gateway or Internet router ports



Standard Switchport Protected Diagram 1

3.22 Power & BTU Calculations

Common units of electricity include volts, amps, VoltAmps, watts, and British Thermal Units (BTUs). This section will address Kilo-Volt-Amps (kVA), Kilowatts (kW) and BTUs. IT professionals should be conversant in the correct use of these terms. Most if not all of this information can be obtained from the equipment's data sheet. If you can't find the information on the data sheet you should call the manufacturer's help desk and open a ticket to get the answer you need to make your calculations. Google is your friend. Order of precedence for data is in this manner:

1. Datasheet
2. Manufacturer's FAQ's

3.23 UPS Requirements

Make sure that the UPS can handle the total electrical load of the equipment that you want to connect to it. Create a spreadsheet to determine your total load, and then choose a UPS with an Output Wattage Capacity 20-25% higher than that total.

Reputable UPS Manufacturers include, but are not limited to, TrippLite, APC, Eaton, and CyberPower.

UPS units must be supplied with each IT closet. ALL UPS units used must be 19 inch, rack mounted Line Interactive-for Networks or On-Line type or better units. A single closet may have multiple rack units of UPS and battery packs. UPS UNITS ARE HEAVY, so you must plan for and accommodate for this weight and use 4 post to 2 post rack conversion kits to spread UPS weight evenly or use 4 post racks and rail kits. As mentioned above, UPS must be loaded to no more than 80% of their stated output wattage. Be advised that whole building generator sites still require UPS units for power conditioning during and after power transfer.

DO NOT USE STANDBY UPS UNITS!

Standby UPS units are made expressly for desktop computers and home networks. They are cheap consumer grade quality with very low output wattage, this is why you can find them at Big Box retail or Club Warehouses. They are easily identifiable by their low cost and small rectangular or small tower foot print. They are not rack mountable.

3.24 3rd Party Devices & Applications

It is technically possible to run 3rd party devices and applications over the Guest Internet Access network. **For each device and/or application it is necessary to gain Hilton and GIA vendor approval prior to installation.** When approval is granted for the installation of 3rd party devices and/or applications, this will always be on a best effort basis. In accordance with [section 3.16](#), 3rd Party devices/applications are prohibited from using HR and DSSS rates they must also be able to communicate at a required minimum data rate of 24Mbps

3.25 Circuit Monitoring

Circuit monitoring must take place with the GIA vendor in order to ensure a seamless and stable connection for all client connections.

When bandwidth utilization of the GIA circuit reaches 80% of the available capacity of the connection, during three or more consecutive days in any calendar month, the hotel circuit will be considered saturated and non-compliant. Upon such an occurrence, the Hotel will be required to upgrade the circuit. Circuit(s) must be upgraded by contract within 45 days of the hotel being notified as having a “saturated circuit”.

Circuit uptime should also be monitored, however contractual SLAs will determine the maximum deliverable before further investigation can be requested by the Guest Internet Access Vendor.

3.26 AP Installation Best Practices

It is important to locate AP's close enough to each other to provide ample wireless coverage but far enough apart so they do not cause CCI or ACI with one another. The actual distance needed between any two APs depends upon a combination of factors, including, but not limited to, AP type and type of AP antenna, the construction of the building, sources of signal degradation, shielding, and reflection.

- Model your installation using Ekahau Site Survey Pro with the model specific APs and antennae orientations.
- For Meeting space and public space AP's the best signal coverage it is recommended to place the AP no higher than 18ft and below the ceiling since there will be less obstructions.
- In room APs must be of the Wall Plate Style and adhere to mounting practices described previously in this document.
- Mount the antennae to utilize its engineered antennae propagation characteristics. Internal antenna models, non-wall plate (traditional), AP's should be mounted horizontally (logo to the ground), not on the wall. In Wi-Fi, consistency in AP and antennae, placements is one of the hallmarks of a successful design, implementation, and Wi-Fi turn up. If you must use the wall make sure you have surveyed and modelled for this. Use the antennae “splat” patterns provided.
- Keep the antennae away from metal obstructions such as heating and air-conditioning ducts, large ceiling trusses, building superstructures, and major power cabling runs. If necessary, use a rigid conduit to lower the antenna away from these obstructions.
- The density of the materials used in a building's construction determines the number of walls

the signal must pass through and still maintain adequate coverage. Consider the following before choosing the location to install your antenna:

- Paper and vinyl walls have very little effect on signal penetration.
- Solid and pre-cast concrete walls will limit signal penetration.
- Concrete and wood block walls will limit signal penetration.
- Any metal clad walls/mirrors causes signals to reflect off, causing poor penetration.
- Signals will likely reflect off a chain link fence or wire mesh spaced between 1 and 1 1/2 in. (2.5 and 3.8 cm). The fence acts as a harmonic reflector that blocks the signal. Likewise metal lathe/mesh, of all sizes, will severely degrade signal.
- Install the antennae /AP away from microwave ovens and 2.4-GHz & 5GHz cordless phones. These products can cause signal interference because they operate in the same frequency range as the device your antenna is connected to.
- Outdoor Coverage AP's must comply with [Outdoor Coverage](#) section so that they can withstand the environmental conditions for a given location.

3.27 Ekahau Site Survey Pro & Ekahau Sidekick

Return to [In Room Wireless Access Points & Survey](#)

For years our yardstick has been the Proxim 8494 802.11abgnac dongle in conjunction with AirMagnet Survey Pro. Unfortunately AirMagnet has been in decline and is no longer the industry preferred tool for wireless site survey and spectrum analysis. Couple this with the fact that Proxim killed off the 8494 product line some time ago and the time is right for a change that is long overdue.

Effective immediately, all GIA vendors must acquire and train it's teams to perform site surveys with Ekahau Site Survey Pro with the Ekahau Sidekick and survey for 2.4 GHz, 5 GHz and spectrum analysis concurrently using the latest version ESS Pro which was at v9.2.2 at the time the document was updated. Vendors that do not have the required survey hardware and software will have until March 31st, 2019 to become compliant. In the interim, preference will be given to vendors who meet the new requirements.

The first step in a wireless LAN (WLAN) deployment is to ensure that desired operation begins with a site survey to ascertain the Radio Frequency behavior in the environment. Many guest issues can arise in a wireless network due to poor planning and coverage. **As stated in *RF Signal Strength*, all survey AP's transmit power on each band must be set to no higher than 14dB (half-power) while conducting the site survey to determine AP locations.**

Hilton requires that each band be given a unique SSID for APoS survey purposes:

- [UnoNet-2.4GHz](#)
- [UnoNet-5GHz](#)

Hilton requires a physical Passive and/or Active Site Survey with Spectrum Analysis prior to any wireless installation, remediation, refresh, or MACD (Move, Add, Change, or Delete). Although not a requirement for legacy sites, a predictive site survey can save you lots of time and headache if properly completed. Predictive site surveys using ESS Pro are required in 100% of new construction and renovations.

Physical Site Surveys (APoS) required if

- New Install existing structure
- Refresh
- AP location changes / MACD
- Structural changes to building / MACD
- When Troubleshooting RF related issues

Predictive Surveys with ESS Pro are required for:

- New construction or renovations /additions.

Post installation validation surveys are required for ALL installations.

In all instances, the hotel must provide a complete, accurate, scaled, and properly labelled digital floor plans for each floor and desired coverage area to the GIA vendor. No plans = no design, no survey. Better results are achieved with Ekahau when using .dwg CAD files. Using .dwg files will save you time, particularly, with predictive modelling surveys. **DO NOT USE FIRE ESCAPE PLANS OR ANY OTHER UNSCALED OR INACCURATE DRAWINGS.**

Basic Setup of ESS Pro for a Survey

1. Open ESS Pro
2. Connect Sidekick
 - a. Power on Sidekick.
 - b. Sidekick should be worn on user hip at the beltline. Ensure cooling fins face outward and remember to always wear Sidekick in same location from floor to floor.
 - c. Fully charged sidekick should last you between 7 and 8 hours.
3. Insert the maps (a.k.a. floor plans)
4. Verify the scale on your maps (.dwg files should scale automatically)
5. Choose continuous or Stop-and-Go Survey (Stop-and-Go is preferred)
6. Left click on map at your current location, walk at a steady pace and move mouse cursor as you move (green halo will appear around dotted line as data is collected), left click at every stop or turn.
7. Right click (or click survey icon) to stop the survey
8. If multiple surveys are performed on the same project they can be displayed simultaneously by checking "Primary" or "Secondary" on the survey tab. Unwanted surveys can also be deleted from the survey tab.
9. Define coverage/capacity requirements.
10. Review network performance based on defined requirements.

Basic Setup of ESS Pro for a Predictive Survey

1. Insert the maps (a.k.a. floor plans)
2. Scale the maps
 - a. When all maps are imported:
 - i. Add them to a building
 - ii. Select three alignment points on all maps so the tool can visualize the data in three dimension
3. Draw the wall and/or attenuation areas
4. Draw Coverage Areas
5. Define Coverage/capacity requirements
6. Place Access Points (APs) – Manually or using Auto-planner
 - a. Define AP make and model from AP library.
 - b. Remember to set AP height
7. Optimize the design (Adjust AP placement, channels, power levels etc.)

Analyze

1. Verify coverage/capacity requirements
2. Review each visualization to conform performance meets or exceeds requirements.
3. If a particular requirement fails, modify the design to optimize performance. This could require any number of things, including but not limited to, moving APs, changing channel plans, power levels, antennae types, channel bandwidth, disabling radios, and other methods to improve Wi-Fi performance. Ensuring the wireless network is functioning properly is often an iterative process and it may take several attempts tweaking various settings to achieve the desired results. **PLAN ACCORDINGLY.**

NOTE: For Post Installation Surveys you must allow adequate time for the network to converge. Allow at least 3 hours between last AP install and power adjustment start of survey. If you have surveyed and modelled properly

Generate Report.

Reports are available in the default format or an extensive templated format with many customizations available to the vendor.

The items below relate to ESS Pro settings and are included for reference.

Channels and Scan Interval – This is handled automatically by the ESS Pro Software and Sidekick

Calibration – Define the correct distance between either two x or y axis points on each floor plan map. If the map is not properly calibrated the heat maps generated from the AP do not represent the correct distance.

Signal Propagation – This calculation is handled automatically by the use of ESS Pro and the Sidekick

Survey Path – It is important to verify the survey path on which the data points were taken. The survey path should follow a valid walking path and should not have paths that go through walls. The survey path should also have a walking path that shows data points collected inside rooms and offices where there is desired coverage. It is possible that you do not have proper coverage in a room or area that shows coverage but does not have a walking path or data point. You should also verify that the doors

to the rooms and offices were closed when the data points were collected. Assess the survey path in order to verify how often data points are collected.

Post installation RF survey is required for all installations. This post install survey must include a minimum of three consecutive guest floors in each unique “tower”, lodge, building, cabin, casita bungalow, etc. Post install survey must include 100% of all restaurants, public gathering places and meeting space and any back of house coverage and all property specifically requested areas.

Later versions of this document will include more details on the ESS Pro Settings.

4. SSIDs

This section sets out the UnoNet/StayConnected (SC) standards for deploying SSID naming conventions in both single and dual-branded Hilton hotels. The SSID standard is global and required for all UnoNet installs. It applies to all future Hilton brands, until further notice in writing by Hilton's designated program manager. Compliance with the SSID standard set forth in this document is mandatory and will be strictly enforced. Hilton will maintain tight control over the names numbers of SSIDs used. All SSIDs, including Wall Plate Ethernet ports will be distributed to APs utilizing Cisco's Meraki Tag system. No SSID will be used without prior written approval from Hilton's Global Network Engineering team.

With UnoNet/Meraki we are able to standardize on what SSID's will be used at hotels and preconfigure the SSID's with Meraki's Config Templates. At the end of this section we will provide a list of SSID's that will be pre-configured on the UnoNet/Meraki platform. **No more than 4 SSIDs can be broadcast on any single AP at any given time. This count is not inclusive or wired port enablement on multi-Ethernet port AP's.**

Each SSID can be thought of as virtual AP, operating on the same channels on which the physical AP is set. Therefore, enabling 'x' SSID's on a single AP is nearly identical to deploying 'x' physical AP's with one SSID each. The downside to multiple SSID's is that it creates additional channel utilization due to overhead and can cause latency and bandwidth degradation for users.

4.1 Application of the StayConnected SSID's

- UnoNet/Meraki installs only

4.2 Single Brand Hotels: SSID Naming Conventions

- 'Hilton Honors' is the convention covering guest rooms and public spaces. ***There is a space between each word.*** If there is bleed over from guest rooms to the public space, the convention <Hilton Honors Lobby> is permissible.
- 'Hilton Honors Meeting' is the convention covering the meeting space. ***There is a space between each word.***
- Vanity SSID's are permissible in the meeting space at the client's request. In these cases, flexibility should be exercised if the client insists on a SSID outside of the aforementioned naming convention e.g. 'Google' is acceptable. Use of vanity SSID is governed by the understanding they are temporary and must be removed from broadcasting at conclusion of the event.
- SSID's are case-sensitive, therefore, be sure the 1st letter in each word of the SSID is **Capitalized**. (Example, Hilton Honors).

4.3 Dual-Branded Hotels: SSID Naming Conventions

Hilton Honors Hampton
Hilton Honors Homewood
Hilton Honors HGI
Hilton Honors Tru
Hilton Honors Doubletree
Hilton Honors Home2
Hilton Honors Hilton
Hilton Honors Tapestry
Hilton Honors Conrad
Hilton Honors Curio
Hilton Honors Waldorf-Astoria
Hilton Honors Canopy
Hilton Honors Embassy

- 'Hilton Honors <Brand Name>' is the convention covering guest rooms and public spaces. (Example, Hilton Honors Hampton.) ***There is a space between each word.***
- 'Hilton Honors <Brand Name Meeting>' is the convention covering the meeting space. (Example, Hilton Honors Hampton Meeting) ***There is a space between each word.***
- Vanity SSID's are permissible in the meeting space at the client's request. In these cases, flexibility should be exercised if the client insists on a SSID outside of the aforementioned naming convention e.g. 'Google' is acceptable. Use of vanity SSID is governed by the understanding they are temporary and must be removed from broadcasting at conclusion of the event.
- SSID's are case-sensitive, therefore, be sure the 1st letter in each word of the SSID is **capitalized**. (Example, **Hilton Honors Tru**). Note, for Hilton Garden Inn, use HGI as listed under Single Hotels and with each letter in HGI capitalized. (Example, **Hilton, Honors HGI**).

4.4 Dual-Branded Hotels

Installations involving **dual-branded** hotels you have one option:

- Shared circuit, split at the router
- Use dedicated VLANs to direct the appropriate SSID to the correct Gateway (shared APs, switches and controllers)
- Two SSIDs on each AP (example: Hilton Honors Hampton & Hilton Honors HGI)
- Each brand has its own separate landing page.

4.5 Preconfigured SSID Matrix slots

Number	Type	Name/SSID	Use
0	Standard	Hilton Honors	Guest
1	Standard	Hilton Honors Lobby	Lobby
2	Standard	Hilton Honors Meeting	Meeting
3	Standard	Hilton	PEP/Corp Travel
4	Utility	TBD	Dual Brand, POS, Vanity, 3rd Party Apps
5	Utility	TBD	Dual Brand, POS, Vanity, 3rd Party Apps
6	Utility	TBD	Dual Brand, POS, Vanity, 3rd Party Apps
7	Utility	TBD	Dual Brand, POS, Vanity, 3rd Party Apps
8	Utility	TBD	Dual Brand, POS, Vanity, 3rd Party Apps
9	Utility	TBD	Dual Brand, POS, Vanity, 3rd Party Apps
10	Utility	TBD	Dual Brand, POS, Vanity, 3rd Party Apps
11	Utility	TBD	Dual Brand, POS, Vanity, 3rd Party Apps
12	Utility	TBD	Dual Brand, POS, Vanity, 3rd Party Apps
13	Utility	TBD	Dual Brand, POS, Vanity, 3rd Party Apps
14	Utility	TBD	Dual Brand, POS, Vanity, 3rd Party Apps

5. Appendix

5.1 Circuit Standards - Requirements

Please ensure any vendor you contact understands the Internet circuit must follow the below listed requirements in order to meet Hilton Standards:

- Bandwidth requirements must meet or exceed Hilton Internet Circuit Matrix for the GIA Program (Your Guest Internet Access VENDOR Service Executive will alert you to the bandwidth requirement per property)
- Viable Circuit Types include Fiber, DS3, OC3, and Ethernet and any fractional offerings of those types. No DSL/cable/wireless - a.k.a. microwave). Circuits must provide synchronous up/down speeds.
- LOA-Letter of Authorization from ISP
- Availability SLA must be 99.9% annually and a MTTR of 4 hours or less and stated in the contract
- Must provide at least a /28 (16 IPs / 14 Usable IPs) or a number of public IP addresses sufficient to meet needs for hotel's back office or other systems.
- SNMP protocol enabled for monitoring (Hilton GIA will need IP Port 162 open past the ISP hardware/router for SMNP access to GIA equipment)
- SNMP protocol enabled for monitoring of Internet router via a read-only community string (exceptions considered on an individual basis)
- Vendor support and escalation contact information. 24 x 7 live person support for circuit and equipment if managed by ISP.
- Hotel will provide a letter of agency so that Guest Internet Access VENDOR can act on behalf of the hotel to report troubles and make changes to the circuit.

No MAC BINDING, DHCP, NAT, PAT, firewalls, filtering, shaping, or throttling by the ISP IS ALLOWED.

Routers are recommended but NOT a requirement. However, if provided and/or required then the Hardware/router that terminates circuit at customer premise must be managed, maintained and supported by ISP in total or by approved 3rd Party Vendor. Hardware must have current maintenance agreement that provides for repair/replacement within 24 hours.

What is required for Hilton to approve this 3rd party solution?

1. Must provide circuit vendor's SLA (service level agreement) to Guest Internet Access VENDOR for Hilton approval
2. Must complete existing circuit worksheet with all needed information on the Potential New Internet circuit
3. Must approve LOA (Letter of Agency) in order for Hilton GIA Program to call the provider in the event of circuit trouble
4. Must submit all documents for Hilton's approval