

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of)
)
Petition of American Hotel & Lodging)
Association, Marriott International, Inc., and) RM-11737
Ryman Hospitality Properties for a)
Declaratory Ruling to Interpret 47 U.S.C. §)
333, or, in the Alternative, for Rulemaking)

**JOINT COMMENTS OF
ARUBA NETWORKS, INC. AND
RUCKUS WIRELESS, INC.**

Marta Beckwith
Vice President, Legal
Aruba Networks
1344 Crossman Ave.
Sunnyvale, CA 94089

Scott Maples
Vice President, General Counsel
Ruckus Wireless, Inc.
350 West Java Drive
Sunnyvale CA 94089

December 19, 2014

TABLE OF CONTENTS

I.	INTRODUCTION	2
II.	SECTION 333 IS NOT IMPLICATED WHEN A WI-FI NETWORK OPERATOR USES DEAUTHENTICATION TO CONTAIN PART 15 DEVICES	6
A.	The Transmission of Deauthentication Frames Does Not Result In Interference.	6
B.	Section 333 Only Protects “Stations” And Does Not Protect Part 15 Devices.	8
III.	THE COMMISSION SHOULD CLARIFY ITS RULES AND POLICIES REGARDING THE MANAGEMENT OF UNLICENSED SPECTRUM	11
IV.	CONCLUSION	13

EXECUTIVE SUMMARY

The Commission should use the AHLA Petition as its vehicle for resolving the tension some see between Section 333 of the Act, which prohibits “willful and malicious” interference to “stations”, and Part 15 of the Commission’s Rules, which provides that unlicensed “devices” have no expectation of protection from interference in most circumstances.

In response to the AHLA Petition, the Commission should acknowledge the important role that network management systems play in assuring that networks (wired and wireless) are safe and secure and that the information of network operators and the public is protected. Today, network operators are faced with a wide variety of cybersecurity challenges. While the Joint Commenters support the Commission’s long-standing efforts to promote the use of unlicensed spectrum and generally support the right of individuals acting lawfully to use their Wi-Fi devices, the Commission can and should assure that those charged with maintaining cybersecurity or protecting important policies are not hamstrung in battling the serious threats they face.

We agree with the AHLA Petition that Section 333 of the Act does not provide protection to Part 15 devices. Section 333 is, by its terms, only protective of “stations” and the Commission has never subjected Part 15 “devices” to the other provisions of the Act applicable to “stations.” Moreover, the transmission of 802.11 network management frames, does not constitute “interference” under the Act or the Commission’s rules. An access point that transmits an 802.11 Layer 2 deauthentication frame to contain a Wi-Fi device does not increase the undesired signal level or otherwise cause electromagnetic interference. From an RF perspective, the deauthentication frame’s characteristics are identical to those of any other frame transmitted by the 802.11 device. It is the way the 802.11 device interprets the deauthentication frame, not the RF characteristics of the signal that leads the device to discontinue communications.

Concluding that Section 333 does not apply to Part 15 devices has the added benefit of allowing the Commission to establish for the first time Part 15 rules and policies that distinguish between management practices that are acceptable, and those that are not. In doing so, the Commission will be taking on an obligation to engage in a careful balancing act, continuing to promote the widest possible use of Wi-Fi devices, while at the same time assuring that network administrators can protect their networks, data and customers from cybersecurity threats and from attempts to violate important network policies. Doing so will require a dialog between the Commission and the 802.11 industry, and the Joint Commenters look forward to participating.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of)
)
Petition of American Hotel & Lodging)
Association, Marriott International, Inc., and) RM-11737
Ryman Hospitality Properties for a)
Declaratory Ruling to Interpret 47 U.S.C. §)
333, or, in the Alternative, for Rulemaking)

**JOINT COMMENTS OF
ARUBA NETWORKS, INC. AND
RUCKUS WIRELESS, INC.**

Aruba Networks, Inc. (“Aruba”) and Ruckus Wireless, Inc. (“Ruckus”) (collectively, the “Joint Commenters”) hereby respond to the Commission’s November 19, 2014 *Public Notice*¹ seeking comment on the August 25, 2014 petition by the American Hotel & Lodging Association, Marriott International, Inc., and Ryman Hospitality Properties for a declaratory ruling “that the operation of FCC-authorized equipment by a Wi-Fi operator in managing its network on its premises does not violate 47 U.S.C. § 333, even though it may result in ‘interference with or cause interference to’ a Part 15 device being used by a guest on the operator’s property.”² In the alternative, the AHLA Petition urges the Commission to commence a rulemaking proceeding to amend Part 15 to “specify the interference to Part 15 devices that Section 333 prohibits.”³

¹ See “Consumer & Governmental Affairs Bureau Reference Information Center Petition for Rulemaking Filed,” *Public Notice*, Report No. 3012 (rel. Nov. 19, 2014).

² See Petition of American Hotel & Lodging Association, Marriott International, Inc., and Ryman Hospitality Properties for a Declaratory Ruling to Interpret 47 U.S.C. § 333, or, in the Alternative, for Rulemaking, RM-11737, at 13-19 (filed April 25, 2014)(“AHLA Petition”).

³ See *id.* at 19-21.

I. INTRODUCTION

Aruba is a leading global provider of wireless (“Wi-Fi”) mobility solutions. Aruba develops, markets and sells products and services to enterprises, state, local and federal government bodies and educational institutions that enable its customers to quickly, securely and cost-effectively meet their mobility and bring-your-own-device (“BYOD”) needs. Ruckus is a global supplier of carrier-class 802.11 compliant Wi-Fi products and technologies for mobile Internet infrastructure and enterprise wireless LAN (“WLAN”) systems. Ruckus provides both advanced indoor and outdoor wireless systems for service provider and enterprise customers to support applications such as WLAN access, mobile data offload, public access, and WLAN services.

For the reasons discussed in more detail below, the Commission should use the AHLA Petition as its vehicle for resolving the tension some see between Section 333 of the Act, which prohibits “willful and malicious” interference to “stations”, and Part 15 of the Commission’s Rules, which provides that unlicensed “devices” have no expectation of protection from interference in most circumstances. Section 1.2 of the Commission’s Rules provides that a declaratory ruling is appropriate for “terminating a controversy or removing uncertainty.”⁴ The

⁴ 47 C.F. R. §1.2. The uncertainty addressed in the AHLA Petition is compounded by the fact that on the October 3, 2013, after the AHLA Petition was filed, the Enforcement Bureau and Marriott International, Inc., and Marriott Hotel Services, Inc. (collectively, “Marriott”) entered into a Consent Decree that expresses the Enforcement Bureau’s belief that Section 333 is violated when a Wi-Fi network operator utilizes network management software to “contain” Wi-Fi use on its premises in the absence of a direct threat to the security of the network or the operator’s guests. *See* Marriott Int’l, Inc., *et al*, *Consent Decree*, File No. EB-IHD-13-00011303, at ¶ 6 (rel. Oct. 3, 2014)(the “Marriott Consent Decree”). Marriott did not admit that it had violated Section 333. *See id.* at ¶ 10. Indeed, in a press release issued in connection with the Marriott Consent Decree, Marriott noted that “Marriott has a strong interest in ensuring that when our guests use our Wi-Fi service, they will be protected from rogue wireless hotspots that can cause degraded service, insidious cyber-attacks and identity theft” and stressed that “[w]e believe that [our] actions were lawful.”[cite to come] *available at* <http://news.marriott.com/2014/10/marriott-internationals-statement-on-fcc-ruling.html>

AHLA Petition sets forth in detail the uncertainty that presently exists as to whether Section 333 of the Act can be invoked to protect unlicensed devices operating under Part 15 and what, if any, protection the Commission affords to Part 15 operations.⁵ In the interest of brevity, that discussion need not be repeated here. Suffice it to say that the Joint Commenters, as providers of equipment used to build 802.11 Wi-Fi networks and the technologies used by governmental, educational, hospitality, enterprise and other customers, have an interest in making their Wi-Fi networks more secure and reliable, and in obtaining certainty regarding these issues.

In response to the AHLA Petition, the Commission should acknowledge the important role that network management systems play in protecting networks (wired and wireless) and the information of network operators and the public. As noted in the AHLA Petition⁶ and discussed below, network operators today are faced with a wide variety of cybersecurity challenges. While the Joint Commenters support the Commission's long-standing efforts to promote the use of unlicensed spectrum and, as discussed in detail below, generally support the right of individuals acting lawfully to use their Wi-Fi devices, the Commission can and should assure that those charged with maintaining cybersecurity or protecting important policies are not hamstrung in battling the serious threats they face.

Some examples of the threats facing network operators that we believe justify the use of network management technology to contain unauthorized Part 15 devices include the following:

- **Protect One's Own Network from Attack** – An unmanaged access point (“AP”) may attempt to access a network for any number of bad purposes. We understand that the Enforcement Bureau agrees that a network operator should be permitted to prevent this type of unmanaged access using containment technology. But even when the unmanaged AP is not attempting to access the network, there may be reasons to prevent them from operating for various reasons whether in public, quasi-public, corporate or government environments.

⁵ See AHLA Petition at 4-6, 20-21.

⁶ See *id.* at 6-8.

- **Prevent “Evil Twins”** – An evil twin is an attack in which an unauthorized AP is set up to spoof a network AP (to pretend to be a legitimate AP belonging to the network) in order to steal passwords and other data. The evil twin AP does not try to access the operator’s network in these attacks. Containing unauthorized APs prevents such attacks against a company’s employees, guests and customers. This type of attack is generally done in public or quasi-public spaces where it is (a) easy to set up a hidden AP and (b) guests/customers don’t know the exact name or SSID of the legitimate network.
- **To maintain a “G” rated airspace** – K-12 schools, libraries and certain other facilities are required to comply with the Children’s Internet Protection Act. In order to do so, these facilities usually set up Internet filtering software on their own networks to prevent minors from viewing adult content and other unauthorized Internet sites while on their premises. Without containment, individuals can set up their own unauthorized APs in these locations and get around content filtering. This can also happen in the enterprise environment, potentially subjecting an employer who does not prevent such access in its work space to discrimination or harassment claims. AP containment can address this problem.
- **To maintain data security and enforce network use policies** – Many government agencies and companies have specific policies on what can come into and go out on their networks. This is true even for guests – many entities set up guest networks with guest wireless access to ensure compliance with their network policies while guests are on their premises. By setting up an unauthorized AP that is unconnected to the network, employees and guests can circumvent the policies set up on the network. In other words, people can specifically set up unauthorized APs not on the network in order to circumvent data security and other policies. For example, in a corporate or government setting, deauthentication and disassociation are tools that are used to prevent corporate, military or government espionage by allowing a network administrator to prevent a rogue access point from collecting data from corporate clients or from allowing an individual to circumvent network protections regarding what type of information can be transferred out of the organization.

Note that we offer this list not as an exhaustive catalog of legitimate uses of wireless network management technology to contain unauthorized devices, but to illustrate the problem. Just as cyber threats and the demand for reliable wireless networks will continue to evolve, the use of network management technology to protect legitimate interests will also evolve.

A wide range of companies, some of whom are identified in the AHLA Petition, provide network managers with tools for protecting against these security risks and to otherwise manage

access to their networks.⁷ Although implemented somewhat differently by each vendor, they generally are designed to enhance the ability of these network managers to establish and enforce policies that protect networks, data and devices. The network management tool that led to the Marriott Consent Decree uses one of the most common techniques for managing Wi-Fi use -- the transmission of standards-based IEEE 802.11 Layer 2 deauthentication frames that can be used to “contain” potentially harmful APs.⁸

Layer 2 network management frames, including disassociation and deauthentication frames, are an integral part of the 802.11 standard and are used by 802.11 compliant devices as connections between APs and client devices are formed and dissolved. These are essential network management tools that have been an integral part of in Wi-Fi networks from the initial adoption of the 802.11 standard. For example, these types of frames are used when a client device travels from one location to another and requires transition from one access point to another in order to maintain connectivity. They are also used in certain types of Wi-Fi management and containment technology. For example, they are part of the mechanism by which load balancing is achieved, e.g. they are used to help direct a wireless client device away from a busy access point to a less busy access point.

As will be discussed below, we agree with the AHLA Petition that the use of Layer 2 network management security technologies to contain Part 15 devices does not constitute

⁷ *See id.* at 8-9.

⁸ Under the 802.11 standard, before a client device can access the resources of a Wi-Fi network, it engages in a process of authentication and association with the relevant AP by exchanging a series of management frames that provide a technical “hand shake” between the two devices and allow the AP to reject a connection based on policies set by the network operator. During this process, and thereafter, either device can send the other a disassociation or deauthentication frame to terminate the connection. These management frames are required by the 802.11 standard and are critical to the management of an APs resources and to a client’s ability to associate with and disassociate from a particular AP as it moves location.

interference under Section 333. Section 333 cannot reasonably be interpreted to protect unlicensed Part 15 devices and, in any event, Section 333 applies to electromagnetic interference, which is not present here. However, that does not mean that the Commission has no authority to regulate interference with Part 15 devices or cannot adopt rules or policies designed to allow access to the unlicensed spectrum consistent with legitimate security, legal, policy and other needs.

II. SECTION 333 IS NOT IMPLICATED WHEN A WI-FI NETWORK OPERATOR USES DEAUTHENTICATION TO CONTAIN PART 15 DEVICES

A. *THE TRANSMISSION OF DEAUTHENTICATION FRAMES DOES NOT RESULT IN INTERFERENCE.*

Section 333 states that “[n]o person shall willfully or maliciously interfere with or cause interference to any radio communications of any station licensed or authorized by or under this Act or operated by the United States Government.”⁹ While the AHLA Petition uses the phrase “interference” to describe how Wi-Fi network operators contain unauthorized or unmanaged Wi-Fi operations on their premises, the use of Layer 2 management frames does not constitute “interference” as that term is used in Section 333, and the Joint Commenters are unaware of any comparable situation in which the Commission has found interference to have occurred or Section 333 violated.¹⁰

The Commission defines “interference” as “[t]he effect of unwanted energy due to one or a combination of emissions, radiations, or inductions upon reception in a radiocommunication

⁹ 47 C.F.R. § 333.

¹⁰ *See, e.g.* AHLA Petition at 1. The Joint Commenters are aware that the Enforcement Bureau has stated that Section 333 makes it unlawful to use devices that jam Wi-Fi use by others. *See, e.g.* FCC Enforcement Advisory, Cell Jammers, GPS Jammers, and other Jamming Devices, 26 FCC Rcd 1329 (Enf. Bur. 2011). However, the Bureau has provided no legal analysis supporting its assertion that Section 333 applies to Part 15 devices and, as discussed below, its view is contrary to law. Moreover, as noted in the following discussion, the use of network management techniques does not constitute signal jamming.

system, manifested by any performance degradation, misinterpretation, or loss of information which could be extracted in the absence of such unwanted energy.”¹¹ It occurs when a receiver is adversely impacted by an electromagnetic field emitted by another device, such as when a jammer transmits “powerful radio signals that overpower, jam, or interfere with authorized communications.”¹² In other words, interference is caused by an increase in the unwanted electromagnetic (including radio frequency) “energy” being received by the receiver. As noted in the AHLA Petition, most cases in which the Commission has found Section 333 violated involve the use of jamming devices designed for the sole purpose of overpowering the desired signal with an undesired radio frequency signal.¹³

In contrast, an AP that transmits an 802.11 Layer 2 deauthentication frame to contain a Wi-Fi device does not increase the undesired signal level or otherwise cause electromagnetic interference. From an RF perspective, the deauthentication frame’s characteristics are identical to those of any other frame transmitted by the 802.11 device. All that is happening is a standards-based exchange of network management information using defined protocols – protocols that the recipient interprets as a termination of its connection. It is the way the 802.11 device interprets the deauthentication frame, not the RF characteristics of the signal that leads the device to discontinue communications. Section 333 simply does not apply to the type of network management technology used here.

¹¹ 47 C.F.R. § 2.1.

¹² See *C.T.S. Technology Co., Limited*, Notice of Apparent Liability for Forfeiture and Order, 29 FCC Rcd 8107, 8107-08 (2014) (“*C.T.S. NAL*”). See also “FCC Enforcement Advisory: Cell Jammers, GPS Jammers and Other Jamming Devices,” *Public Notice*, DA 11-250 (Enf. Bur. 2011). Although the Marriott Consent Decree references that the initial informal complaint against Marriott alleged jamming, there is no evidence that the Enforcement Bureau believes that transmitting deauthentication frames constitutes jamming.

¹³ See AHLA Petition at 13-14.

B. SECTION 333 ONLY PROTECTS “STATIONS” AND DOES NOT PROTECT PART 15 DEVICES.

Turning again to the specific language of the statute, Section 333 provides that “[n]o person shall willfully or maliciously interfere with or cause interference to any radio communications of any *station* licensed or authorized by or under this Act or operated by the United States Government.”¹⁴ Section 333 protects only “stations” and, as discussed below, unlicensed devices operating pursuant to Part 15 are not “stations” for purposes of the Act. Thus, Section 333 simply does not apply to the Part 15 devices at issue here.

This limitation on the scope of Section 333 is appropriate. Were Section 333 to apply here, it would presumably bar network operators from using deauthentication and other association and deassociation techniques **required** by the 802.11 standard and **necessary** to the proper functioning of 802.11 compliant devices.¹⁵ Section 333 prevents all willful interference without exception – it does not distinguish between conduct undertaken for laudable purposes and that undertaken with bad intent. As a policy matter, Section 333 would be an extremely blunt instrument for regulating Wi-Fi, as it would not permit use of 802.11 required Layer 2 management techniques. Even if the Commission were to find that the uses of these network management packets that are required to be compliant with the 802.11 standard were permitted, it would impede the ability of network managers to secure their networks, data and customers against the threats that even the Enforcement Bureau has acknowledged are appropriately

¹⁴ 47 C.F.R. § 333 (emphasis added)

¹⁵ As noted in the AHLA Petition, because of the expansive definition “willful” under Section 312(f)(1) of the Act, if Section 333 were to apply, a network operator could be considered to be acting “willfully” in transmitting a deauthentication frame, even if its intent in doing so is to allow the client device to associate with another access point, to request the client to associate with an access point with more available bandwidth, or to protect its network against intrusion, defeat an Evil Twin attack, or otherwise achieve a legitimate objection. *See* AHLA Petition at 17 n. 34.

addressed with network management. Thus, the Commission can and should declare that because Part 15 unlicensed devices are not “stations” for purposes of Section 333 and that Section 333 does not apply to the transmission of network management frames to Part 15 devices. Such a declaration does not, and should not, preclude the Commission from addressing electromagnetic interference to Part 15 devices or to address improper uses of network management technology under other provisions of the Act, but it avoids the draconian results that applying Section 333 could result in.

Although Section 333 does not define what constitutes a “station,” other provisions of the Act and the Commission’s rules support the interpretation that Part 15 devices are not covered.¹⁶ Most notably, Sections 307 through 310 address in detail the process for obtaining a license for a “station” and modifications, renewals and transfers thereof.¹⁷ The Commission has recognized that not all radiofrequency devices are “stations” and has never imposed the licensing requirements under these provisions of Title III to Part 15 unlicensed devices.¹⁸ Rather, consistent with Section 302 of the Act,¹⁹ the Commission has drawn a distinction between “radio

¹⁶ Section 3 (35) of the Act defines the terms “radio station” or “station” as “a station equipped to engage in radio communication or radio transmission of energy.” 46 U.S.C. §147(35). This circular definition (for equipment to constitute a station, it must be a station) does not shed any light on the scope of Section 333.

¹⁷ 47 U.S.C. §§ 307, 308 (setting out the requirements for “station” applications, licenses, modifications, and renewals); § 309 (establishing processes for Commission action on applications for a “station” license, modification, or renewal under Section 308); § 310 (includes certain ownership limitations on, and requirements for the assignment of license and transfer of control of, “station” licenses.).

¹⁸ While Section 307(e) of the Act allows for “radio stations” to operate without individual licenses in certain specified radio services (the citizens band radio service; the radio control service; the aviation radio service; and the maritime radio service), 47 U.S.C. § 307(e), this limited exemption from the station licensing requirement is not extended to Part 15 wireless devices.

¹⁹ Under Section 302, “[t]he Commission may, consistent with the public interest, convenience, and necessity, make reasonable regulations (1) governing the interference potential of *devices*

stations” or “stations” subject to Title III licensing and other provisions (including Section 333), and unlicensed “devices”.

The distinction between unlicensed “devices” and licensed “radio stations” or “stations” is engrained in the Commission’s own rules. Part 15 establishes the “regulations under which an intentional, unintentional, or incidental radiator may be operated without an individual license”²⁰ and devices not falling within the scope of Part 15 “must be licensed pursuant to the provisions of section 301 of the Communications Act of 1934, as amended, unless otherwise exempted”²¹ Indeed, as the AHLA Petition rightly notes, were Part 15 devices to be deemed “stations” for purposes of Section 333, then the provision of Section 15.5(b) obligating Part 15 devices to accept interference from each other would contravene Section 333. It is impossible to square the provision of Section 15.5(b) requiring a Part 15 device to accept all interference with an interpretation of Section 333 that forbids any willful or malicious interference to a Part 15 device. Part 15 of the Commission’s Rules can only be harmonized with Section 333 of the Act by acknowledging that “radio stations” or “stations” are distinct from Part 15 Wi-Fi “devices” and that each category has its own set of rights and obligations. To interpret Section 333 otherwise runs the risk of undermining the Commission’s unlicensed regulatory paradigm.

which in their operation are capable of emitting radio frequency energy by radiation, conduction, or other means in sufficient degree to cause harmful interference to radio communications” 47 U.S.C. § 302 (emphasis added).

²⁰ 47 C.F.R. § 15.1.

²¹ 47 C.F.R. § 15.5(b). The Part 15 rules do not purport to authorize the operation of any “radio station” or “station. The only exception is with respect to the Citizen’s Band Service “stations” which Congress specifically exempted from individual licensing requirements under Section 307(e) of the Act.

III. THE COMMISSION SHOULD CLARIFY ITS RULES AND POLICIES REGARDING THE MANAGEMENT OF UNLICENSED SPECTRUM

As noted above, concluding that Section 333 does not apply to Part 15 devices has the added benefit of allowing the Commission to establish rules and policies for Part 15 devices that distinguish between management practices that are acceptable, and those that are not. In doing so, the Commission will be taking on an obligation to engage in a careful balancing act, continuing to promote the widest possible use of Wi-Fi devices, while at the same time assuring that network administrators can protect their networks, data and customers from cybersecurity threats and from attempts to violate important network policies. Doing so will require a dialog between the Commission and the 802.11 industry, and the Joint Commenters look forward to participating.

The Commission should not lose sight of the fact that the 802.11 standard has been developed to accommodate the operation of multiple Wi-Fi networks and multiple client device connections in close proximity. Wi-Fi has a long and successful history of operating and flourishing in this environment. Consumers generally benefit when they have access to multiple Wi-Fi networks. And, consumers benefit from personal, portable Wi-Fi hotspots when used appropriately. But, there also are benefits to consumers and network users when their data and these relatively open Wi-Fi and IP networks are protected by network operators using network management and other techniques from data thieves, cybercriminals and those trying to circumvent important network policies such as those for “G” rated airspace.

The Joint Commenters urge the Commission to use this proceeding to adopt rules and guidelines regarding the appropriate use of network management techniques that afford consumers broad access to Wi-Fi networks, but that are consistent with the legitimate network and other security, legal and policy needs of the network operator. We identified in Section I

above several examples of scenarios where we believe network management and security concerns outweigh the individual rights of Part 15 users.²² And, the record developed in response to the AHLA Petition is likely to identify additional scenarios. By declaring that Section 333 is inapplicable to Part 15 devices and to this type of network management technology, and starting the process of explaining when such network management techniques can be used, the Commission can provide the 802.11 community (vendors, network operators, and users alike) clarity as to what network management is permitted and what is not.²³

²² *See supra* at 3-4.

²³ The Joint Commenters must take issue with the aspect of the AHLA Petition that appears to suggest that the permissibility of network management is related to property ownership and the relationship of the property owner to the owner of the device being contained. *See* AHLA Petition at 4. This relationship should have nothing to do with either the applicability of Section 333 to Part 15 devices or the propriety of any Part 15 network management. Thus, as the Commission begins the process of providing additional clarity, there should be no dependency on property ownership or on a similar relationship between any parties using Part 15 stations in the same RF domain.

