

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION**

STINGRAY IP SOLUTIONS LLC,

Plaintiff,

v.

HEWLETT PACKARD ENTERPRISE
COMPANY,

Defendant.

§
§
§
§
§
§
§
§
§
§

CASE NO. 2:24-cv-00868-JRG-RSP

JURY TRIAL DEMANDED

PLAINTIFF’S FIRST AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Stingray IP Solutions LLC (“Stingray”) files this First Amended Complaint in the Eastern District of Texas (the “District”) against Defendant Hewlett Packard Enterprise Company (“Defendant” or “HPE”) for infringement of U.S. Patent No. 7,224,678 (the “’678 patent”), U.S. Patent No. 7,440,572 (the “’572 patent”), and U.S. Patent No. 7,616,961 (“the “’961 patent”) (these patents collectively referred to as the “Asserted Patents”).

THE PARTIES

1. Stingray IP Solutions LLC (“Stingray” or “Plaintiff”) is a Texas limited liability company, located at 6136 Frisco Sq. Blvd., Suite 400, Frisco, TX 75034.

2. On information and belief, Defendant Hewlett Packard Enterprise Company is a company organized under the laws of Delaware, USA, with its principal place of business located at 1701 East Mossy Oaks Road, Spring, Texas, USA 77389. Hewlett Packard Enterprise Company may be served with process via its registered agents, including C T Corporation System, 1999 Bryan Street, Suite 900, Dallas, TX, USA 75201-3136.

3. The *HPE Annual Report* explains that HPE’s “operations are organized into six reportable business segments,” one of which is “Intelligent Edge.” HEWLETT PACKARD ENTERPRISE COMPANY, *Form 10-K Annual Report For the Fiscal Year Ended October 31, 2022*, 4, (Feb. 24, 2023), available for download at <https://www.sec.gov/Archives/edgar/data/1645590/000164559023000117/hpe-20231031.htm> [hereinafter “*HPE Annual Report*”]. HPE states that its “Intelligent Edge business is comprised of a portfolio of secure edge-to-cloud solutions operating under the Aruba brand that includes wired and wireless local area network (“LAN”), campus, branch, and data center switching, software-defined wide-area networking, network security, and associated services that enable secure connectivity for businesses of any size.” *Id.* at 5. According to HPE, “The primary business drivers for Intelligent Edge solutions are work from anywhere environments, mobility, and connectivity for internet-of-things (‘IoT’) devices.” *Id.* Via its “Intelligent Edge” segment, HPE’s states that its “wireless access portfolio” includes a “leadership position in Wi-Fi ... and Zigbee.” *Id.* at 10.

4. On information and belief, Hewlett Packard Enterprise Company is the owner of the Aruba brand and related companies, encompassing, but not limited to, Aruba, HPE Aruba Networking, Aruba ESP (or Aruba Edge Services Platform), and Aruba Networks, LLC (collectively, “Aruba”). *Id.* at 5-6, 10, 81, Ex. 21. The “HPE Aruba Networking product portfolio includes hardware products, such as Wi-Fi access points, switches, and gateways.” *Id.* at 5. “HPE Aruba Networking software and services portfolio includes cloud-based management, network management, network access control, software-defined wide-area networking, network security, analytics and assurance, location services software, and professional and support services, as well as aaS and consumption models through the HPE GreenLake edge-to-cloud platform for the Intelligent Edge portfolio of products.” *Id.*

5. In addition, HPE “offer[s] Aruba ESP (or Edge Services Platform), which takes a cloud-native approach to helping customers meet their connectivity, security, and financial requirements across campus, branch, data center, and remote worker environments, covering all aspects of wired, wireless LAN, and wide-area networking.” *Id.* at 6.

6. HPE’s Annual Report for the Fiscal year ending October 31, 2023, indicates that the “Intelligent Edge products” category “accounted for more than 10% of [HPE’s] consolidated net revenue” of \$28.496 billion for fiscal year 2022 and \$30.077 billion for fiscal year 2023 (in constant currency). *Id.* at 4, 37. During the same timeframe, HPE states that its net revenue in the United States was \$9.425 for fiscal year 2022 and \$10.369 billion for fiscal year 2023. *Id.* at 84. Additionally, HPE indicates that its Intelligent Edge total segment net revenue increased by \$1.530 billion or 41.6% from \$3.674 billion in fiscal year 2022 to \$5.204 billion in fiscal year 2023. *Id.* at 43, 46, 47, 82.

7. On information and belief, Hewlett Packard Enterprise Company, along with its subsidiaries, members, segments, companies, brands and/or related entities, for example, U.S.-based subsidiaries, members, segments, companies, brands and/or related entities, is engaged in making, using, selling, offering for sale, and importing Wi-Fi- and Zigbee-enabled products and services within the United States and Texas. *See, e.g., id.* at 10 (describing HPE’s “Research and Development,” including “investing in automation, machine learning, and AI-based network operations ... , as exemplified by [HPE’s] cloud-native Aruba Central cloud service that provides manageability for [HPE’s] entire portfolio, including Wireless LAN, Campus & Data Center Switches, and SD-Branch.”), 20 (indicating “[t]he manufacture of [HPE’s] product components, the final assembly of [HPE’s] products and other critical operations are concentrated in certain geographic locations, including the United States, Puerto Rico, ... [and] China”), 32 (stating that

HPE’s “major product development, services, manufacturing, and Hewlett Packard Labs facilities” are located in the United States, Puerto Rico and China, among other locations, with HPE’s “principal executive offices” and “global headquarters” being located in Texas, within the United States).

8. HPE’s products are manufactured outside the U.S. and then imported into the United States or manufactured inside the U.S., distributed, and sold to end-users via the internet, brick-and-mortar stores and/or via dealers in the U.S., in Texas and the Eastern District of Texas.

9. HPE maintains a corporate presence in the United States, including in Texas and in this District, including at least its global headquarters in Spring, Texas, and offices in this District, including, for example, those located at 3001 Dallas Parkway, Suite 200, Frisco, TX 75034 in Collin County, Texas; and/or 6080 Tennyson Parkway, Suite 400, Plano, Texas 75024 in Collin County, Texas. *See, e.g., 3001 Dallas Pkwy, Suite 200, Frisco, TX 75034*, COLLIN CAD, <https://www.collincad.org/propertysearch?prop=2805626&year=2024> (last visited Aug. 30, 2024); *6080 Tennyson Parkway, Suite 400, Plano, Texas 75024*, COLLIN CAD, <https://www.collincad.org/propertysearch?prop=2709682&year=2024> (last visited Aug. 30, 2024). On behalf and for the benefit of HPE and its subsidiaries, members, segments, companies, brands and/or related entities, HPE coordinates the importation, distribution, marketing, offers for sale, sale, and use of HPE’s products in the U.S. For example, HPE maintains distribution channels in the U.S. for HPE’s products, for example, via at least its own online stores, distribution partners, retailers, reseller partners, dealers, and/or other related service providers. *See, e.g., Wireless Devices*, HPE, <https://buy.hpe.com/us/en/networking/wireless-devices/c/1137927> (last visited Aug. 30, 2024) (website offering various Aruba Wi-Fi access points for sale); *HPE offices and executive briefing centers*, HPE, <https://www.hpe.com/us/en/contact-hpe.html#Office> (last visited

Sep. 3, 2024) (listing “WW Corporate Headquarters - Spring, TX - United States, 1701 E Mossy Oaks Rd, Spring, TX 77389;” “Frisco, TX Office 3001 Dallas Parkway, Frisco, TX 75034-8660;” and locations in New York, California, Georgia, Colorado and North Carolina”); *Partner Connect*, HPE, <https://partnerconnect.hpe.com/partners> (last visited Sep. 3, 2024) (listing “10004 result(s)” in the “United States,” including various states, and stating “[c]onnect with trusted HPE partners who sell, manage, integrate, support and deliver HPE solutions”); *How to Buy*, HPE, <https://www.hpe.com/us/en/buy-parts-products.html> (last visited Sep. 4, 2024) (stating, “We offer a variety of ways to purchase HPE products and services” and “Find a reseller, service provider, or authorized support partner near you.”).

10. As a result, via at least HPE’s established distribution channels operated and maintained by at least Defendant Hewlett Packard Enterprise Company and/or its U.S.-based subsidiaries, members, segments, companies, brands and/or related entities, HPE products are distributed, sold, advertised, and used nationwide, including being sold to consumers via physical stores and online HPE stores operating in Texas and this District. Thus, Defendant does business in the U.S., the state of Texas, and in this District.

JURISDICTION AND VENUE

11. This action arises under the patent laws of the United States, namely 35 U.S.C. §§ 271, 281, and 284-285, among others.

12. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

13. Defendant Hewlett Packard Enterprise Company is subject to this Court’s specific and general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this State and this District, including: (A) at least part of its infringing activities alleged herein which purposefully avail the Defendant of the privilege of

conducting those activities in this state and this District and, thus, submits itself to the jurisdiction of this court; and (B) regularly doing or soliciting business, engaging in other persistent conduct targeting residents of Texas and this District, and/or deriving substantial revenue from infringing goods offered for sale, sold, and imported and services provided to and targeting Texas residents and residents of this District vicariously through and/or in concert with its partners, alter egos, intermediaries, agents, related entities, distributors, importers, customers, subsidiaries, and/or consumers. For example, Hewlett Packard Enterprise Company and Hewlett Packard Enterprise Company's U.S.-based subsidiaries, members, segments, companies, brands and/or related entities manufacture, import, distribute, offer for sale, sell, and induce infringing use of HPE products to distribution partners, retailers (including national retailers), resellers, dealers, service providers, consumers, and other users.

14. This Court has personal jurisdiction over Hewlett Packard Enterprise Company, directly and/or indirectly via the activities of Hewlett Packard Enterprise Company's partners, alter egos, intermediaries, agents, related entities, distributors, importers, customers, subsidiaries, and/or consumers, including U.S.-based subsidiaries, members, segments, companies, brands and/or related entities.

15. Hewlett Packard Enterprise Company utilizes established distribution channels to distribute, market, offer for sale, sell, service, and/or warrant infringing products directly to consumers and other users, including offering such products and/or related services for sale. HPE products and/or services have been sold from and/or in both brick-and-mortar stores and online retail stores by entities within this District and in Texas. Alone and in concert with or via direction and control of or by at least these entities, Hewlett Packard Enterprise Company has committed acts of direct and/or indirect patent infringement within Texas, and elsewhere within the United

States, giving rise to this action and/or has established minimum contacts with Texas. For example, Hewlett Packard Enterprise Company operates within a global network of manufacturing, sales and distribution of HPE products that includes subsidiaries and/or related entities of Hewlett Packard Enterprise Company, retail stores, showrooms, dealers, resellers, professional installers, and/or distributors operating in Texas, including this District.

16. As another example, Hewlett Packard Enterprise Company maintains a place of business in this District through at least brick-and-mortar locations at 3001 Dallas Parkway, Suite 200, Frisco, TX 75034 in Collin County, Texas; and/or 6080 Tennyson Parkway, Suite 400, Plano, Texas 75024 in Collin County, Texas. *See, e.g., 3001 Dallas Pkwy, Suite 200, Frisco, TX 75034*, COLLIN CAD, <https://www.collincad.org/propertysearch?prop=2805626&year=2024> (last visited Aug. 30, 2024); *6080 Tennyson Parkway, Suite 400, Plano, Texas 75024*, COLLIN CAD, <https://www.collincad.org/propertysearch?prop=2709682&year=2024> (last visited Aug. 30, 2024).

17. On information and belief, as a part of HPE’s global manufacturing and distribution network, Hewlett Packard Enterprise Company also purposefully places infringing HPE products in established distribution channels in the stream of commerce, including in Texas, via distribution partners, retailers (e.g., national retailers), resellers, dealers, brand ambassadors, service providers, consumers, and/or other users. *See, e.g., Partner Connect*, HPE, <https://partnerconnect.hpe.com/partners> (last visited Sep. 3, 2024) (listing “10004 result(s)” in the “United States,” including various states, and stating “[c]onnect with trusted HPE partners who sell, manage, integrate, support and deliver HPE solutions”); *How to Buy*, HPE, <https://www.hpe.com/us/en/buy-parts-products.html> (last visited Sep. 4, 2024) (stating, “We offer a variety of ways to purchase HPE products and services” and “Find a reseller, service provider,

or authorized support partner near you.”); *HPE Aruba AP-635 (US) - Campus - wireless access point - ZigBee, Bluetooth, Wi-Fi 6E*, CDW, <https://www.cdw.com/product/hpe-aruba-ap-635-us-campus-wireless-access-point-zigbee-bluetooth/6667331?msockid=18e4c4923fad6ad90274d72f3e9a6bed> (last visited Sep. 4, 2024) (offering to sell HPE Aruba Zigbee and Wi-Fi access point); *Aruba Wireless Access Points*, STAPLES, https://www.staples.com/Aruba-wireless-access-points/cat_CL215781/f31b6 (last visited Sep. 4, 2024) (offering to sell Aruba Wi-Fi access point and noting that Aruba is “a Hewlett Packard Enterprise company” for the “Aruba R3J19A Mount Bracket Kit,” which is recommended for purchase with the access point).

18. Hewlett Packard Enterprise Company owns and operates at least one website that offers HPE products and services to consumers in the United States, in Texas, and in this District. *See, e.g., Wireless Devices*, HPE, <https://buy.hpe.com/us/en/networking/wireless-devices/c/1137927> (last visited Aug. 30, 2024) (website offering various Aruba Wi-Fi access points for sale). Hewlett Packard Enterprise Company provides infringing HPE product under the HPE brand via its online and/or physical stores or local places of business. *See id.* For example, numerous HPE WiFi and/or Zigbee access points are offered for sale in this District by at least HPE’s nationwide online store and/or local places of business, for example, at buy.hpe.com. *See id.* Therefore, Hewlett Packard Enterprise Company, alone and in concert with its subsidiaries, members, segments, companies, brands and/or related entities, has purposefully directed its activities at Texas, and should reasonably anticipate being brought into this Court, at least on this basis. Through its own conduct and/or through direction and control of its subsidiaries, members, segments, companies, brands and/or related entities, Hewlett Packard Enterprise Company has committed acts of direct and/or indirect patent infringement within Texas, and elsewhere within

the United States, giving rise to this action and/or has established minimum contacts with Texas such that personal jurisdiction over Hewlett Packard Enterprise Company would not offend traditional notions of fair play and substantial justice.

19. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(c) and/or 1400(b). As alleged herein, Defendant Hewlett Packard Enterprise Company has committed acts of infringement in this District. As further alleged herein, Defendant Hewlett Packard Enterprise Company, via its own operations and/or employees, has a regular and established place of business in this District, for example, at 3001 Dallas Parkway, Suite 200, Frisco, TX 75034 in Collin County, Texas; and/or 6080 Tennyson Parkway, Suite 400, Plano, Texas 75024 in Collin County, Texas, among any other HPE locations owned, leased and/or operated in this District. Accordingly, Hewlett Packard Enterprise Company may be sued in this district under 28 U.S.C. § 1400(b).

20. On information and belief, Defendant Hewlett Packard Enterprise Company has significant ties to, and presence in, the State of Texas and this District, making venue in this District both proper and convenient for this action.

THE ASSERTED PATENTS AND TECHNOLOGY

21. The Asserted Patents cover various aspects of monitoring, detecting intrusions, and encrypting and decrypting wireless communications networks, including networks created using Defendant's home and/or business networking devices.

22. The '678 patent involves detecting intrusions into a wireless local or metropolitan area network. The disclosed intrusion detection techniques include monitoring transmission between stations of the network, where each station has its own media access layer (MAC) address. The monitoring is done to detect failed attempts to authenticate the MAC addresses. Upon detection of a number of failed attempts to authenticate, an intrusion alert may be generated.

23. The '961 patent involves allocating channels in wireless networks, including in mobile ad hoc networks. The patent describes dynamic channel allocation among nodes in such networks to efficiently make use of a plurality of channels. In such networks, wireless communication links connect wireless mobile nodes, among other nodes, over multiple separate channels at different frequencies. The disclosed techniques for channel allocation include monitoring link performance on one channel based on a quality of service (QoS) threshold. When the monitored link performance falls below the QoS threshold, other available separate channels are scouted. Scouting may include switching to a second separate channel at a different frequency. A channel activity query may be broadcast to determine link performance of the second separate channel. Replies to the query are processed to determine the link performance, and channel activity may be updated for each separate channel based on the replies.

24. The '572 patent involves providing secure wireless local area networks (LAN). A device for securing such a LAN may include a housing with a wireless transceiver carried by the housing. A medium access controller (MAC) is also carried by the housing. A cryptography circuit may be connected to the MAC controller and the transceiver. The circuit may encrypt both address and data information by at least adding a plurality of encrypting bits to be transmitted. And the cryptography circuit may decrypt both address and data information upon reception.

25. On information and belief, a significant portion of the operating revenue of Defendant is derived from the manufacture, distribution, sale, and use of home and business networking, IoT, and security solutions, products, and components, which are manufactured in or imported into the United States, distributed to resellers, dealers, and third-party manufacturers, and ultimately sold to and used by U.S. consumers. For example, HPE reported that they had \$10.369 billion in sales in the U.S. market during the fiscal year 2023 reporting period. *See HPE*

Annual Report pp. 4, 37. Furthermore, *HPE's Annual Report* for the Fiscal year ending October 31, 2023, indicates that the “Intelligent Edge products” category “accounted for more than 10% of [HPE’s] consolidated net revenue” of \$30.077 billion for the fiscal year 2023. *See id.* at 43, 46, 47, 82.

26. The Asserted Patents cover Defendant’s networking, IoT, and security solutions, products, components, software, services, and processes related to same that generally connect to other devices in a network or other networks using a wireless protocol, such as ZigBee and/or Wi-Fi. *See, e.g., HPE Aruba Networking 730 Series Wi-Fi 7 Campus Access Points*, HPE ARUBA NETWORKING, <https://www.arubanetworks.com/products/wireless/access-points/indoor-access-points/730-series/> (last visited Sep. 4, 2024) (describing “HPE Aruba Networking 730 Series” Wi-Fi 7 access points with “[t]wo integrated Bluetooth 6 and 802.15.4 radios for Zigbee”); *HPE Aruba Networking 750 Series Campus Access Points*, HPE ARUBA NETWORKING, available at <https://www.hpe.com/psnow/doc/a00140933enw> (last visited Sep. 4, 2024) (data sheet describing “HPE Aruba Networking 750 Series” Wi-Fi 7 access points with “two integrated Bluetooth 6 and 802.15.4 radios for Zigbee support to simplify deploying and managing IoT-based location services, asset tracking services, security solutions and IoT sensors”). Defendant’s infringing products include, but are not limited to, devices enabled or compliant with Wi-Fi and/or ZigBee, including without limitation access points (for example, HPE Aruba Networking Access Points with Wi-Fi and/or Zigbee compatibility), gateways (for example, Aruba 9200 Series Campus Gateways), controllers (for example, HPE Aruba Networking 7200 Series Mobility Controllers) and related accessories and software (for example, Aruba Central SaaS with “Features” including “Wireless services” such as “IoT operations” that provide “at-a-glance views of IoT applications and BLE and Zigbee devices on the network” and “HPE Aruba Networking Air Pass” that provides

“seamless Wi-Fi connectivity for SIM enabled cellular devices ... to enable Wi-Fi calling and to offload 5G/LTE traffic to enterprise wireless networks”) (all collectively referred to as the “Accused Products”). These Accused Products infringe the Asserted Patents by at least their manufacture, importation, distribution, sale, and use in the U.S.

27. The Asserted Patents cover Accused Products of HPE that use the ZigBee protocol to communicate with other devices on a communication network, including those of third-party manufacturers. Examples of HPE’s ZigBee products include HPE Aruba Networking HPE Aruba Networking 730 Series Campus Access Points, which use integrated 802.15.4 radios employing the Zigbee protocol “to simplify deploying and managing IoT-based location services, asset tracking services, security solution and IoT sensors” as shown below:

<p>Access points as flexible and secure IoT platform</p> <p>By combining IoT radios with a zero-trust network framework, the HPE Aruba Networking 730 Series Campus APs can serve as flexible IoT platforms that bolster network security, provide coverage for broad range of IoT devices, and eliminate the need for network overlays just for IoT devices.</p> <p><u>The 730 Series includes two integrated Bluetooth 6 and 802.15.4 radios for Zigbee support to simplify deploying and managing IoT-based location services, asset tracking services, security solutions and IoT sensors.</u></p> <p>There are also two USB-port extensions to provide IoT connectivity to a wider range of devices. These IoT capabilities allows organizations to leverage the APs as an IoT platform, which eliminates the need for an overlay infrastructure and additional IT resources and can accelerate IoT initiatives.</p>	<p>Streamline IoT operations</p> <p>HPE Aruba Networking <u>Central IoT Operations</u> is a service available for APs running HPE Aruba Networking Wireless Operating System AOS-10 managed by HPE Aruba Networking Central unifies visibility of <u>IT and OT infrastructure within the network health dashboard by extending network monitoring and insights to BLE, Zigbee, and other non-IP IoT devices.</u> It helps streamline non-Wi-Fi device onboarding and data collection.</p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

See *HPE Aruba Networking 730 Series Campus Access Points*, HPE ARUBA NETWORKING, https://www.arubanetworks.com/assets/ds/DS_AP730Series.pdf (last visited Sep. 4, 2024); see also *HPE Aruba Networking 750 Series Campus Access Points*, HPE ARUBA NETWORKING, available at <https://www.hpe.com/psnow/doc/a00140933enw> (last visited Sep. 4, 2024) (data sheet describing “HPE Aruba Networking 750 Series” Wi-Fi 7 access points with “two integrated

Bluetooth 6 and 802.15.4 radios for Zigbee support to simplify deploying and managing IoT-based location services, asset tracking services, security solutions and IoT sensors”).

Table 1. Features for AP HPE Aruba Networking Central Foundational and Advanced subscriptions

Features	Foundational	Advanced
Wireless services		
...		
<p>IoT operations Unifies visibility of wireless and IoT infrastructure by providing at-a-glance views of IoT applications and BLE and Zigbee devices on the network. Install IoT application plugins and provision IoT Connectors (deployed as virtual appliances) in just a few mouse clicks. APs can also be deployed as IoT connectors. This reduces the cost of managing and maintaining separate IoT connectors and provides IT operators the flexibility to choose between APs or VMs.</p> <p><small>Note: Certain AOS-10-specific partner integrations require an Advanced License.</small></p>	✓	✓
<p>HPE Aruba Networking AirPass Provides seamless Wi-Fi connectivity for SIM enabled cellular devices for major mobile operators to enable Wi-Fi calling and to offload 5G/LTE traffic to enterprise wireless networks.</p> <p><small>Notes:</small></p> <ul style="list-style-type: none"> • Currently available in US only • AP Foundational license supports a single mobile operator • AP Advanced license supports all participating providers 	✓	✓

HPE Aruba Networking Central SaaS Subscription Ordering Guide, HPE ARUBA NETWORKING, p. 6, available at <https://www.arubanetworks.com/resource/hpe-aruba-networking-central-saas-subscription-ordering-guide/> (last visited Sep. 4, 2024) (advertising that Aruba Central SaaS includes “Features” including “Wireless services” such as “IoT operations” that provide “at-a-glance views of IoT applications and BLE and Zigbee devices on the network” and urging consumers to “Install IoT application plugins and provision IoT Connectors (deployed as virtual appliances) in just a few mouse clicks”).

28. ZigBee protocols, which are covered by the Asserted Patents and utilized by certain Accused Products, are based on the IEEE 802.15.4 standard for wireless network communication. Below is an excerpt from the technical specification for ZigBee protocols describing the basic architecture and standards that enable wireless network communication.

1.1 Protocol Description

The ZigBee Alliance has developed a very low-cost, very low-power-consumption, two-way, wireless communications standard. Solutions adopting the ZigBee standard will be embedded in consumer electronics, home and building automation, industrial controls, PC peripherals, medical sensor applications, toys, and games.

1.1.3 Stack Architecture

The ZigBee stack architecture is made up of a set of blocks called layers. Each layer performs a specific set of services for the layer above. A data entity provides a data transmission service and a management entity provides all other services. Each service entity exposes an interface to the upper layer through a service access point (SAP), and each SAP supports a number of service primitives to achieve the required functionality.


The IEEE 802.15.4 standard defines the two lower layers: the physical (PHY) layer and the medium access control (MAC) sub-layer. The ZigBee Alliance builds on this foundation by providing the network (NWK) layer and the framework for the application layer. The application layer framework consists of the application support sub-layer (APS) and the ZigBee device objects (ZDO). Manufacturer-defined application objects use the framework and share APS and security services with the ZDO.

The PHY layer operates in two separate frequency ranges: 868/915 MHz and 2.4 GHz. The lower frequency PHY layer covers both the 868 MHz European band and the 915 MHz band, used in countries such as the United States and Australia. The higher frequency PHY layer is used virtually worldwide. A complete description of the PHY layers can be found in [B1].

ZigBee Specification, revision r21 at 1, THE ZIGBEE ALLIANCE,

<https://zigbeealliance.org/wp-content/uploads/2019/11/docs-05-3474-21-0csg-zigbee-specification.pdf> (August 5, 2015).

29. The IEEE 802.15.4 standard based mobile ad-hoc network, utilized by the Accused Products, is a type of Low-Rate Wireless Personal Area Network (LR-WPAN) that allows transmission of data between a plurality of network nodes.

IEEE STANDARDS ASSOCIATION 

**IEEE Standard for
Local and metropolitan area networks—
Part 15.4: Low-Rate Wireless Personal Area
Networks (LR-WPANs)**

4. General description

4.1 General

An LR-WPAN is a simple, low-cost communication network that allows wireless connectivity in applications with limited power and relaxed throughput requirements. The main objectives of an LR-WPAN are ease of installation, reliable data transfer, extremely low cost, and a reasonable battery life, while maintaining a simple and flexible protocol.

Two different device types can participate in an IEEE 802.15.4 network: a full-function device (FFD) and a reduced-function device (RFD). An FFD is a device that is capable of serving as a personal area network (PAN) coordinator or a coordinator. An RFD is a device that is not capable of serving as either a PAN coordinator or a coordinator. An RFD is intended for applications that are extremely simple, such as a light switch or a passive infrared sensor; it does not have the need to send large amounts of data and only associates with a single FFD at a time. Consequently, the RFD can be implemented using minimal resources and memory capacity.

4.2 Components of the IEEE 802.15.4 WPAN

A system conforming to this standard consists of several components. The most basic is the device. Two or more devices communicating on the same physical channel constitute a WPAN. However, this WPAN includes at least one FFD, which operates as the PAN coordinator.

Page 8, http://ecee.colorado.edu/~liue/teaching/comm_standards/2015S_zigbee/802.15.4-2011.pdf

30. In the ZigBee network of the Accused Products, a network device/node is configured to monitor the performance of a channel-in-use based on its energy measurement. As described below, if the measurement value is higher than the value on other channels (threshold), it indicates interference is present on the channel, consequently resulting in transmission failures.



ANNEX E OPERATING NETWORK MANAGER AS NETWORK CHANNEL MANAGER FOR INTERFERENCE REPORTING AND RESOLUTION

A single device can become the Network Channel Manager. This device acts as the central mechanism for reception of network interference reports and changing the channel of the network if interference is detected. The default address of the network manager is the coordinator, however this can be updated by sending a Mgmt_NWK_Update_req command with a different short address for the network channel manager. The device that is the Network Channel Manager shall set the network manager bit in the server mask in the node descriptor and shall respond to System_Server_Discovery_req commands.

Each router or coordinator is responsible for tracking transmit failures using the TransmitFailure field in the neighbor table and also keeping a NIB counter for total transmissions attempted. A device that detects a significant number of transmission failures may take action to determine if interference is a cause. The following steps are an example of that procedure¹:

1. Conduct an energy scan on all channels within the current PHY. If this energy scan does not indicate higher energy on the current channel then other channels, no action is taken. The device should continue to operate as normal and the message counters are not reset. However, repeated energy scans are not desirable as the device is off the network during these scans and therefore implementations should limit how often a device with failures conducts energy scans.
2. If the energy scan does indicate increased energy on the channel in use, a Mgmt_NWK_Update_notify should be sent to the Network Manager to indicate interference is present. This report is sent as an APS Unicast with acknowledgement and once the acknowledgement is received the total transmit and transmit failure counters are reset to zero.

Page 516, <https://zigbeealliance.org/wp-content/uploads/2019/11/docs-05-3474-21-0csg-zigbee-specification.pdf>

31. As described below, the network manager node facilitates switching to a different channel, i.e., scouting available separate channels, if the performance on the channel-in-use falls below a threshold (i.e., when the current channel's energy is higher than channels, indicating increased interference, and thereby resulting in multiple transmission failures). The network nodes switch to a new (second) channel whose energy level is lowest or below an acceptable threshold.



A single device can become the Network Channel Manager. This device acts as the central mechanism for reception of network interference reports and changing the channel of the network if interference is detected. The default address of the network manager is the coordinator, however this can be updated by sending a Mgmt_NWK_Update_req command with a different short address for the network channel manager. The device that is the Network Channel Manager shall set the network manager bit in the server mask in the node descriptor and shall respond to System_Server_Discovery_req commands.

Each router or coordinator is responsible for tracking transmit failures using the TransmitFailure field in the neighbor table and also keeping a NIB counter for total transmissions attempted. A device that detects a significant number of transmission failures may take action to determine if interference is a cause. The following steps are an example of that procedure¹:

1. Conduct an energy scan on all channels within the current PHY. If this energy scan does not indicate higher energy on the current channel than other channels, no action is taken. The device should continue to operate as normal and the message counters are not reset. However, repeated energy scans are not desirable as the device is off the network during these scans and therefore implementations should limit how often a device with failures conducts energy scans.
2. If the energy scan does indicate increased energy on the channel in use, a Mgmt_NWK_Update_notify should be sent to the Network Manager to indicate interference is present. This report is sent as an APS Unicast with acknowledgement and once the acknowledgement is received the total transmit and transmit failure counters are reset to zero.
3. To avoid a device with communication problems from constantly sending reports to the network manager, the device should not send a Mgmt_NWK_Update_notify more than 4 times per hour.

Upon receipt of an unsolicited Mgmt_NWK_Update_notify, the network manager must evaluate if a channel change is required in the network. The specific mechanisms the network manager uses to decide upon a channel change are left to the implementers. It is expected that implementers will apply different methods to best determine when a channel change is required and how to select the most appropriate channel. The following is offered as guidance for implementation.

Page 516, <https://zigbeealliance.org/wp-content/uploads/2019/11/docs-05-3474-21-0csg-zigbee-specification.pdf>

32. With reference to the above graphic and as further described below, the ZigBee network of the Accused Products further allows using the command to request interference reports, i.e., broadcasts a channel activity query, from the network nodes, which involves scanning the energy level on all the channels including the newly switched (second) channel. The interference report will represent determining the performance for the second channel. In addition, the most recent energy level value and failure rate (indicative of the channel performance/activity) corresponding to the channels is stored, i.e., the channel activity is updated.

The network manager may do the following:

1. Wait and evaluate if other reports from other devices are received. This may be appropriate if there are no other failures reported. In this case the network manager should add the reporting device to a list of devices that have reported interference. The number of devices on such a list would depend on the size of the network. The network manager can age devices out of this list.
2. Request other interference reports using the `Mgmt_NWK_Update_req` command. This may be done if other failures have been reported or the network manager device itself has failures and a channel change may be desired. The network manager may request data from the list of devices that have reported interference plus other randomly selected routers in the network. The network manager should not request an update from the device that has just reported interference since this data is fresh already.
3. Upon receipt of the `Mgmt_NWK_Update_notify`, the network manager shall determine if a channel change is required using whatever implementation specific mechanisms are considered appropriate. The network manager device with just one channel allowed in the `apsChannelMask` parameter must not issue the `Mgmt_Nwk_Update_Req` command to request other devices to change the current channel. However, the network manager may report channel quality issues to the application.
4. If the above data indicate a channel change should be considered, the network manager completed the following:
 - a. Select a single channel based on the `Mgmt_NWK_Update_notify` based on the lowest energy. This is the proposed new channel. If this new channel does not have an energy level below an acceptable threshold, a channel change should not be done. Additionally, a new channel shall not belong to a PHY different from the one on which a network manager is operating now.
5. Prior to changing channels, the network manager should store the energy scan value as the last energy scan value and the failure rate from the existing channel as the last failure rate. These values are useful to allow comparison of the failure rate and energy level on the previous channel to evaluate if the network is causing its own interference.
6. The network manager should broadcast a `Mgmt_NWK_Update_req` notifying devices of the new channel. The broadcast shall be to all devices with `RxOnWhenIdle` equal to `TRUE`. The network manager is responsible for incrementing the `nwkUpdateId` parameter from the NIB and including it in the `Mgmt_NWK_Update_req`. The network manager shall set a timer based on the value of `apsChannelTimer` upon issue of a `Mgmt_NWK_Update_req` that changes channels and shall not issue another such command until this timer expires. However, during this period, the network manager can complete the above analysis. However, instead of changing channels, the network manager would report to the local application using `Mgmt_NWK_Update_notify` and the application can force a channel change using the `Mgmt_NWK_Update_req`.

Upon receipt of a `Mgmt_NWK_Update_req` with a change of channels, the local network manager shall set a timer equal to the `nwkNetworkBroadcastDeliveryTime` and shall switch channels upon expiration of this timer. Each node shall also increment the `nwkUpdateId` parameter and also reset the total transmit count and the transmit failure counters.

Page 517, <https://zigbeealliance.org/wp-content/uploads/2019/11/docs-05-3474-21-0csg-zigbee-specification.pdf>

33. The Asserted Patents also cover Accused Products of HPE that utilize the Wi-Fi protocol. Examples of such products include HPE Aruba Networking 750 Series Campus Access

Points and Aruba Central SaaS. As shown below, the HPE Aruba Networking 750 Series Campus Access Points and Aruba Central SaaS are Wi-Fi (IEEE 802.11) compatible:

<p>Key features (continued)</p> <ul style="list-style-type: none">• High availability with dual HPE Smart Rate ports for redundant Ethernet and power. Configurable to 1, 2.5, 5, or 10 Gbps (or 100 Mbps)• <u>IoT-ready platform with two integrated Bluetooth 6 and 802.15.4/ Zigbee radios and two USB-port extensions</u>• Built in GNSS receiver, barometric pressure sensor, and intelligent software enable APs to self-locate and act as reference points for accurate indoor location measurements• MACsec support¹ extends wired Ethernet protection to the AP• Offered as optional eco-friendly 5-packs• AI-powered dynamic power save mode helps reduce energy use	<p>Access points as flexible and secure IoT-ready platform</p> <p>By combining IoT radios with a Zero Trust network framework, the HPE Aruba Networking 750 Series Campus APs can serve as flexible IoT platforms that bolster network security, provide coverage for broad range of IoT devices, and eliminate the need for network overlays just for IoT devices.</p> <p><u>The 750 Series includes two integrated Bluetooth 6 and 802.15.4 radios for Zigbee support to simplify deploying and managing IoT-based location services, asset tracking services, security solutions and IoT sensors.</u></p> <p>There are also two USB-port extensions providing up to 10W for IoT connectivity to a wide range of devices. These IoT capabilities allow organizations to leverage the APs as an IoT platform, which eliminates the need for an overlay infrastructure and opens opportunities to accelerate IoT initiatives.</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

See *HPE Aruba Networking 750 Series Campus Access Points*, HPE ARUBA NETWORKING, available at <https://www.hpe.com/psnow/doc/a00140933enw> (last visited Sep. 4, 2024) (data sheet describing “HPE Aruba Networking 750 Series” Wi-Fi 7 access points with “two integrated Bluetooth 6 and 802.15.4 radios for Zigbee support to simplify deploying and managing IoT-based location services, asset tracking services, security solutions and IoT sensors”); see also *HPE Aruba Networking 730 Series Wi-Fi 7 Campus Access Points*, HPE ARUBA NETWORKING, <https://www.arubanetworks.com/products/wireless/access-points/indoor-access-points/730-series/> (last visited Sep. 4, 2024) (describing “HPE Aruba Networking 730 Series” Wi-Fi 7 access points that also include “[t]wo integrated Bluetooth 6 and 802.15.4 radios for Zigbee”).

Table 1. Features for AP HPE Aruba Networking Central Foundational and Advanced subscriptions

Features	Foundational	Advanced
Wireless services		
...		
<p>IoT operations Unifies visibility of wireless and IoT infrastructure by providing at-a-glance views of IoT applications and BLE and Zigbee devices on the network. Install IoT application plugins and provision IoT Connectors (deployed as virtual appliances) in just a few mouse clicks. APs can also be deployed as IoT connectors. This reduces the cost of managing and maintaining separate IoT connectors and provides IT operators the flexibility to choose between APs or VMs.</p> <p>Note: Certain AOS-10-specific partner integrations require an Advanced License.</p>	✓	✓
<p>HPE Aruba Networking AirPass Provides seamless Wi-Fi connectivity for SIM enabled cellular devices for major mobile operators to enable Wi-Fi calling and to offload 5G/LTE traffic to enterprise wireless networks.</p> <p>Notes:</p> <ul style="list-style-type: none"> • Currently available in US only • AP Foundational license supports a single mobile operator • AP Advanced license supports all participating providers 	✓	✓

HPE Aruba Networking Central SaaS Subscription Ordering Guide, HPE ARUBA NETWORKING, p. 6, available at <https://www.arubanetworks.com/resource/hpe-aruba-networking-central-saas-subscription-ordering-guide/> (last visited Sep. 4, 2024) (advertising that Aruba Central SaaS includes “Features” including “Wireless services” such as “HPE Aruba Networking Air Pass” that provides “seamless Wi-Fi connectivity for SIM enabled cellular devices ... to enable Wi-Fi calling and to offload 5G/LTE traffic to enterprise wireless networks”).

34. As can be seen, HPE also supports mobile access to networks, including Wi-Fi-enabled calling.

35. The Accused Products include an intrusion detection method for a local or metropolitan area. As described below, the IEEE 802.11 authentication methods utilized by the Accused Products utilize a TKIP that includes a “MIC” to defend against active attacks.

8.3.2.3 TKIP MIC

Flaws in the IEEE 802.11 WEP design cause it to fail to meet its goal of protecting data traffic content from casual eavesdroppers. Among the most significant WEP flaws is the lack of a mechanism to defeat message forgeries and other active attacks. To defend against active attacks, TKIP includes a MIC, named Michael. This MIC offers only weak defenses against message forgeries, but it constitutes the best that can be achieved with the majority of legacy hardware. TKIP uses different MIC keys depending on the direction of the transfer as described in 8.6.1 and 8.6.2.

Annex H contains an implementation of the TKIP MIC. It also provides test vectors for the MIC.

8.3.2.3.1 Motivation for the TKIP MIC

Before defining the details of the MIC, it is useful to review the context in which this mechanism operates.

Active attacks enabled by the original WEP design include the following:

- Bit-flipping attacks
- Data (payload) truncation, concatenation, and splicing
- Fragmentation attacks
- Iterative guessing attacks against the key
- Redirection by modifying the MPDU DA or RA field
- Impersonation attacks by modifying the MPDU SA or TA field

The MIC makes it more difficult for any of these attacks to succeed.

All of these attacks remain at the MPDU level with the TKIP MIC. The MIC, however, applies to the MSDU, so it blocks successful MPDU-level attacks. TKIP applies the MIC to the MSDU at the transmitter and verifies it at the MSDU level at the receiver. If a MIC check fails at the MSDU level, the implementation shall discard the MSDU and invoke countermeasures (see 8.3.2.4).

Page 217, <https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf>

36. Stations (STAs) in an IEEE 802.11 network of the Accused Products associate with each other using a robust security network association (RSNA). As described below, RSNA supports intrusion detection by employing authentication mechanisms and data frame protection mechanisms (such as, temporal key integrity protocol - TKIP) between the STAs. Data is exchanged between the STAs in the form of MPDUs (medium access control (MAC) protocol data units). The MAC frame (MPDU) comprises a MSDU (information frame) in the frame body, and

four addresses that identify, among others, source MAC address (SA) and destination MAC address (DA) for the MSDU.

IEEE Std 802.11™-2007
(Revision of
IEEE Std 802.11-1999)

5.1.1.4 Interaction with other IEEE 802® layers

IEEE Std 802.11 is required to appear to higher layers [logical link control (LLC)] as a wired IEEE 802 LAN. This requires that the IEEE 802.11 network handle STA mobility within the MAC sublayer. To meet reliability assumptions (that LLC makes about lower layers), it is necessary for IEEE Std 802.11 to incorporate functionality that is untraditional for MAC sublayers.

In a robust security network association (RSNA), IEEE Std 802.11 provides functions to protect data frames, IEEE Std 802.1X-2004 provides authentication and a Controlled Port, and IEEE Std 802.11 and IEEE Std 802.1X-2004 collaborate to provide key management. All STAs in an RSNA have a corresponding IEEE 802.1X entity that handles these services. This standard defines how an RSNA utilizes IEEE Std 802.1X-2004 to access these services.

3.126 robust security network (RSN): A security network that allows only the creation of robust security network associations (RSNAs). An RSN can be identified by the indication in the RSN information element (IE) of Beacon frames that the group cipher suite specified is not wired equivalent privacy (WEP).

3.127 robust security network association (RSNA): The type of association used by a pair of stations (STAs) if the procedure to establish authentication or association between them includes the 4-Way Handshake. Note that the existence of an RSNA by a pair of devices does not of itself provide robust security. Robust security is provided when all devices in the network use RSNAs.

5.2.3.2 RSNA

An RSNA defines a number of security features in addition to wired equivalent privacy (WEP) and IEEE 802.11 authentication. These features include the following:

- Enhanced authentication mechanisms for STAs
- Key management algorithms
- Cryptographic key establishment
- An enhanced data cryptographic encapsulation mechanism, called Counter mode with Cipher-block chaining Message authentication code Protocol (CCMP), and, optionally, Temporal Key Integrity Protocol (TKIP).

Page 72, 61, 75 <https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf>

37. In the TKIP protocol of the Accused Products, an MSDU transmitter STA calculates cryptographic message integrity code (MIC) using the MAC addresses (SA & DA) corresponding to the MSDU. As described below, the transmission is monitored if the MIC (which

is obtained using the MAC addresses) is verified/authenticated at the receiver. MSDUs with invalid MICs are discarded and countermeasures are invoked.

8.3 RSNA data confidentiality protocols

8.3.1 Overview

This standard defines two RSNA data confidentiality and integrity protocols: TKIP and CCMP. Implementation of CCMP shall be mandatory in all IEEE 802.11 devices claiming RSNA compliance. Implementation of TKIP is optional for an RSNA. A design aim for TKIP was that the algorithm should be implementable within the capabilities of most devices supporting only WEP, so that many such devices would be field-upgradeable by the supplier to support TKIP.

8.3.2 Temporal Key Integrity Protocol (TKIP)

8.3.2.1 TKIP overview

The TKIP is a cipher suite enhancing the WEP protocol on pre-RSNA hardware. TKIP modifies WEP as follows:

- a) A transmitter calculates a keyed cryptographic message integrity code (MIC) over the MSDU SA and DA, the MSDU priority (see 8.3.2.3), and the MSDU plaintext data. TKIP appends the computed MIC to the MSDU data prior to fragmentation into MPDUs. The receiver verifies the MIC after decryption, ICV checking, and defragmentation of the MPDUs into an MSDU and

discards any received MSDUs with invalid MICs. TKIP's MIC provides a defense against forgery attacks.

- b) Because of the design constraints of the TKIP MIC, it is still possible for an adversary to compromise message integrity; therefore, TKIP also implements countermeasures. The countermeasures bound the probability of a successful forgery and the amount of information an attacker can learn about a key.

Page 213, 214 <https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf>

38. The TKIP MIC implementation of the Accused Products prevents intrusion attacks, such as, message redirection by modifying destination/receiver MAC address (DA or RA) and impersonation by modifying the source/transmitter MAC address (SA or TA). As described below, the transmission is monitored if the MIC (which is obtained using the MAC addresses) is verified/authenticated at the receiver. MSDU with an invalid MIC will indicate a modified MAC address (SA or DA), thereby resulting in discarding the MSDU and invoking the countermeasures.

8.3.2.3 TKIP MIC

Flaws in the IEEE 802.11 WEP design cause it to fail to meet its goal of protecting data traffic content from casual eavesdroppers. Among the most significant WEP flaws is the lack of a mechanism to defeat message forgeries and other active attacks. To defend against active attacks, TKIP includes a MIC, named Michael. This MIC offers only weak defenses against message forgeries, but it constitutes the best that can be achieved with the majority of legacy hardware. TKIP uses different MIC keys depending on the direction of the transfer as described in 8.6.1 and 8.6.2.

Annex H contains an implementation of the TKIP MIC. It also provides test vectors for the MIC.

8.3.2.3.1 Motivation for the TKIP MIC

Before defining the details of the MIC, it is useful to review the context in which this mechanism operates. Active attacks enabled by the original WEP design include the following:

- Bit-flipping attacks
- Data (payload) truncation, concatenation, and splicing
- Fragmentation attacks
- Iterative guessing attacks against the key
- Redirection by modifying the MPDU DA or RA field
- Impersonation attacks by modifying the MPDU SA or TA field

The MIC makes it more difficult for any of these attacks to succeed.

All of these attacks remain at the MPDU level with the TKIP MIC. The MIC, however, applies to the MSDU, so it blocks successful MPDU-level attacks. TKIP applies the MIC to the MSDU at the transmitter and verifies it at the MSDU level at the receiver. If a MIC check fails at the MSDU level, the implementation shall discard the MSDU and invoke countermeasures (see 8.3.2.4).

Page 217, <https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf>

39. Upon detecting a first MIC failure, as described below, a countermeasure timer is initiated, and a failure event (alert) is reported to the AP by sending a Michael MIC Failure Report frame. Upon detecting a second consecutive MIC failure within 60 seconds, i.e., detecting a number of failed attempts, the participating STAs are deauthenticated, wherein deauthentication involves sending a notification (i.e., generating an alert) to deauthenticate due to an intrusion (2 consecutive MIC failures has occurred).

8.3.2.4 TKIP countermeasures procedures

The TKIP MIC trades off security in favor of implementability on pre-RSNA devices. Michael provides only weak protection against active attacks. A failure of the MIC in a received MSDU indicates a probable active attack. A successful attack against the MIC would mean an attacker could inject forged data frames and perform further effective attacks against the encryption key itself. If TKIP implementation detects a probable active attack, TKIP shall take countermeasures as specified in this subclause. These countermeasures accomplish the following goals:

- MIC failure events *should* be logged as a security-relevant matter. A MIC failure is an almost certain indication of an active attack and warrants a follow-up by the system administrator.
- The rate of MIC failures *must* be kept below two per minute. This implies that STAs and APs detecting two MIC failure events within 60 s must disable all receptions using TKIP for a period of 60 s. The slowdown makes it difficult for an attacker to make a large number of forgery attempts in a short time.

A single counter or timer shall be used to log MIC failure events. These failure events are defined as follows:

- For an Authenticator:
 - Detection of a MIC failure on a received unicast frame.
 - Receipt of Michael MIC Failure Report frame.
- For a Supplicant:
 - Detection of a MIC failure on a received unicast or broadcast/multicast frame.
 - Attempt to transmit a Michael MIC Failure Report frame.

The number of MIC failures is accrued independent of the particular key context. Any single MIC failure, whether detected by the Supplicant or the Authenticator and whether resulting from a group MIC key failure or a pairwise MIC key failure, shall be treated as cause for a MIC failure event.

The Supplicant uses a single Michael MIC Failure Report frame to report a MIC failure event to the Authenticator. A Michael MIC Failure Report is an EAPOL-Key frame with the following Key Information

The first MIC failure shall be logged, and a timer initiated to enable enforcement of the countermeasures. If the MIC failure event is detected by the Supplicant, it shall also report the event to the AP by sending a Michael MIC Failure Report frame.

If a subsequent MIC failure occurs within 60 s of the most recent previous failure, then a STA whose IEEE 802.1X entity has acted as a Supplicant shall deauthenticate (as defined in 11.3.1.3) itself or deauthenticate all the STAs with a security association if its IEEE 802.1X entity acted as an Authenticator. For an IBSS STA, both Supplicant and Authenticator actions shall be taken. Furthermore, the device shall not receive or transmit any TKIP-encrypted data frames, and shall not receive or transmit any unencrypted data frames other than IEEE 802.1X messages, to or from any peer for a period of at least 60 s after it detects the second failure. If the device is an AP, it shall disallow new associations using TKIP during this 60 s period; at the

Page 219, 220, <https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf>

40. The Asserted Patents also cover HPE's Wi-Fi compliant devices, which support WPA, WPA2, and/or WPA3 security mechanisms, as described below and in the following paragraph. Of the WPA, WPA2 and/or WPA3 security mechanism used by the Accused Products, such as HPE's networking, IoT, and security Wi-Fi devices, the WPA security mechanism is based

on Temporal Key Integrity Protocol (TKIP), while the WPA2 and WPA3 security mechanisms are based on Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP). Shown below are exemplary IEEE 802.11 compliant HPE devices. Each of the devices has a housing.

Future proof and flexible Wi-Fi

Ideal for enterprises, healthcare, LPV, education, retail, and industrial IoT deployments, the 730 Series APs deliver fast, secure Wi-Fi 7 connectivity.

- ✔ **Wi-Fi 7 performance**
802.11be APs support up to three 320 MHz channels in 6 GHz, MLO, and 4K QAM.
- ✔ **Flexible radios**
Three 2x2 MIMO radios and three Wi-Fi 7 bands (2.4, 5, and 6 GHz) with flexibility to support dual 5 GHz or dual 6 GHz radios¹.
- ✔ **Multi-gigabit connectivity**
High availability with dual 5 Gbps ports for redundant Ethernet and power.
- ✔ **IoT platform**
Two integrated Bluetooth 6 and 802.15.4 radios for Zigbee and two USB-port extensions for connectivity to a wider range of devices.
- ✔ **Self-locating**
Built-in GNSS receiver, barometric sensor, and support for FTM 802.11az for sub 1 meter accuracy.
- ✔ **Built-in security**
WPA3, Enhanced Open, and WPA2-MPSK support for stronger encryption and authentication, and MACsec for encrypted wired connection.



Certifications ^

UL2043 plenum rating

Wi-Fi Alliance (WFA):

- Wi-Fi CERTIFIED a, b, g, n, ac, 6, 7
- WPA, WPA2 and WPA3 – Enterprise with CNSA option, Personal (SAE), Enhanced Open (OWE)
- WMM, WMM-PS, W-Fi Agile Multiband
- Passpoint (release 2)

Bluetooth SIG

Ethernet Alliance (PoE, PD device, class 5)

HPE Aruba Networking 730 Series Wi-Fi 7 Campus Access Points, HPE ARUBA NETWORKING, <https://www.arubanetworks.com/products/wireless/access-points/indoor-access-points/730-series/> (last visited Sep. 5, 2024).

Fast, flexible, and built for the future

Perfect for the most demanding client and IoT use cases, the 750 Series APs deliver ultra-high performance and secure Wi-Fi 7 connectivity with intelligent automation and AI insights provided by AOS-10 and HPE Aruba Networking Central.

- ✓ **Ultimate Wi-Fi 7 performance**
802.11be APs support up to three 320 MHz channels in 6 GHz, MLO, and 4K QAM.
- ✓ **Flexible 4x4 radios**
Three 4x4 MIMO radios and three Wi-Fi 7 bands (2.4, 5, and 6 GHz) with flexibility to support dual 5 GHz or dual 6 GHz radios¹.
- ✓ **10GbE wired connectivity**
High availability with dual 10 Gbps ports for redundant Ethernet and power.
- ✓ **Powerful IoT platform**
Two integrated Bluetooth 6 and 802.15.4 radios for Zigbee and two USB-port extensions for connectivity to a wider range of devices.
- ✓ **Self locating**
Built-in GNSS receiver, barometric sensor, and support for FTM 802.11az for sub-one-meter accuracy.
- ✓ **Built-in security**
WPA3, Enhanced Open, and WPA2-MPSK for stronger encryption and authentication, and MACsec for encrypted wired connection.



Certifications ^

UL2043 plenum rating

Wi-Fi Alliance (WFA):

- Wi-Fi CERTIFIED a, b, g, n, ac, 6, 7
- WPA, WPA2 and WPA3 – Enterprise with CNSA option, Personal (SAE), Enhanced Open (OWE)
- WMM, WMM-PS, W-Fi Agile Multiband
- Passpoint (release 2)

Bluetooth SIG

Ethernet Alliance (PoE, PD device, class 6)

HPE Aruba Networking 750 Series Wi-Fi 7 Campus Access Points, HPE ARUBA NETWORKING, <https://www.arubanetworks.com/products/wireless/access-points/indoor-access-points/750-series/> (last visited Sep. 5, 2024).

41. WPA and WPA2 security encryption systems are used in conjunction with 802.11 b/g/n Wi-Fi connections standards. As illustrated above, WPA, WPA2 and/or WPA3 security encryption systems are utilized in products represented in Defendant's Accused Product line.

42. As illustrated above, the Wi-Fi-enabled Accused Products provide 2.4 and/or 5 GHz Wi-Fi speeds. This capability ascertains the presence of a Wi-Fi antenna and transceiver in the device and provides a secure wireless LAN.

43. Shown below is a block diagram of TKIP (used with WPA) based cryptography circuit utilized in the Accused Products. The circuit shown encrypts both address (destination address (DA), source address (SA)) and data information (plaintext MSDU) by adding encryptions bits (MIC key) to both the address and data. The cryptography circuit of the Accused Products is also configured to decrypt the encrypted address and data information.

IEEE Std 802.11™-2007
(Revision of
IEEE Std 802.11-1999)

8.3.2 Temporal Key Integrity Protocol (TKIP)

8.3.2.1.1 TKIP cryptographic encapsulation

TKIP enhances the WEP cryptographic encapsulation with several additional functions, as depicted in Figure 8-4.

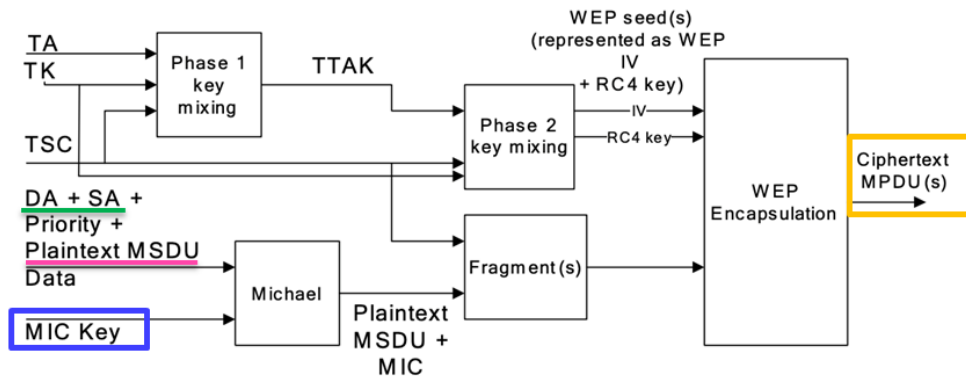


Figure 8-4—TKIP encapsulation block diagram

- a) TKIP MIC computation protects the MSDU Data field and corresponding SA, DA, and Priority fields. The computation of the MIC is performed on the ordered concatenation of the SA, DA, Priority, and MSDU Data fields. The MIC is appended to the MSDU Data field. TKIP discards any MIC padding prior to appending the MIC.
- b) If needed, IEEE Std 802.11 fragments the MSDU with MIC into one or more MPDUs. TKIP assigns a monotonically increasing TSC value to each MPDU, taking care that all the MPDUs generated from the same MSDU have the same value of extended IV (see 8.3.2.2).
- c) For each MPDU, TKIP uses the key mixing function to compute the WEP seed.
- d) TKIP represents the WEP seed as a WEP IV and ARC4 key and passes these with each MPDU to WEP for generation of the ICV (see 7.1.3.6), and for encryption of the plaintext MPDU, including all or part of the MIC, if present. WEP uses the WEP seed as a WEP default key, identified by a key identifier associated with the temporal key.

Page 213, 214, <https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf>

COUNT I

(INFRINGEMENT OF U.S. PATENT NO. 7,224,678)

44. Plaintiff incorporates paragraphs 1 through 43 herein by reference.

45. Plaintiff is the assignee of the '678 patent, entitled “Wireless local or metropolitan area network with intrusion detection features and related methods,” with ownership of all

substantial rights in the '678 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

46. The '678 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '678 patent issued from U.S. Patent Application No. 10/217,042.

47. HPE has and continues to directly infringe one or more claims of the '678 patent in this District and elsewhere in Texas and the United States.

48. On information and belief, HPE designs, develops, manufactures, imports, distributes, offers to sell, sells, and/or uses the Accused Products, including via the activities of HPE and its subsidiaries, members, segments, companies, brands and/or related entities, such as U.S.-based subsidiaries, members, segments, companies, brands and/or related entities.

49. Defendant directly infringes the '678 patent via 35 U.S.C. § 271(a) by making (including, e.g., via contract manufacturers), using, offering for sale, selling, and/or importing the Accused Products, their components, and/or products containing the same that incorporate the fundamental technologies covered by the '678 patent, for example, to or for itself, its alter egos, agents, intermediaries, related entities, distributors, dealers, importers, customers, subsidiaries, members, segments, companies, brands, resellers, dealers, OEMs, integrators, installers, and/or consumers. Furthermore, on information and belief, Defendant designs the Accused Products for U.S. consumers, has made and/or sold and/or continues to make and/or sell the Accused Products outside of the United States, deliver those products to related entities, subsidiaries, online stores, distribution partners, retailers, showrooms, resellers, dealers, installers, customers and/or related service providers in the United States, or in the case that Defendant delivers the Accused Products outside of the United States Defendant does so intending and/or knowing that those products are

destined for the United States and/or designing those products for sale and use in the United States, thereby directly infringing the '678 patent. *See, e.g., Lake Cherokee Hard Drive Techs., L.L.C. v. Marvell Semiconductor, Inc.*, 964 F. Supp. 2d 653, 658 (E.D. Tex. 2013) (denying summary judgment and allowing presentation to jury as to “whether accused products manufactured and delivered abroad but imported into the United States market by downstream customers ... constitute an infringing sale under § 271(a)”).

50. Furthermore, Hewlett Packard Enterprise Company directly infringes the '678 patent through its direct involvement in the activities of its subsidiaries and related entities, including U.S.-based subsidiaries, members, segments, companies, brands and/or related entities. Defendant designs the Accused Products for U.S. consumers, sells and offers for sale those Accused Products in the U.S. directly and via its related entities, and imports the Accused Products into the United States for sale and/or for its related entities. On information and belief, subsidiaries, members, segments, companies, brands and/or related entities of Defendant, for example, U.S.-based subsidiaries, members, segments, companies, brands and/or related entities of Defendant, conduct activities that constitute direct infringement of the '678 patent under 35 U.S.C. § 271(a) by importing, making, offering for sale, selling, and/or using those Accused Products in the U.S. on behalf of and for the benefit of Defendant. Defendant Hewlett Packard Enterprise Company is vicariously liable for the infringing conduct of Defendant's U.S.-based subsidiaries, members, segments, companies, brands and/or related entities (under both the alter ego and agency theories). On information and belief, Defendant Hewlett Packard Enterprise Company and U.S.-based subsidiaries, members, segments, companies, brands and/or related entities are essentially the same company, comprising subsidiaries, members, segments, companies, brands and/or related entities of HPE. Moreover, Hewlett Packard Enterprise Company, along with its related entities, has the

right and ability to control the infringing activities of U.S.-based subsidiaries, members, segments, companies, brands and/or related entities such that Defendant receives a direct financial benefit from that infringement.

51. For example, HPE infringes claim 51 of the '678 patent via the Accused Products that utilize 802.11 (Wi-Fi) protocols, including, but not limited to, HPE access points (e.g., HPE Aruba Networking Access Points with Wi-Fi compatibility), gateways (e.g., Aruba 9200 Series Campus Gateways), controllers (e.g., HPE Aruba Networking 7200 Series Mobility Controllers), HPE packages that include any of these products; and related accessories and software.

52. Those Accused Products include “[a]n intrusion detection method for a wireless local or metropolitan area network comprising a plurality of stations” comprising the limitations of claim 51. The technology discussion above and the example Accused Products provide context for Plaintiff’s allegations that each of those limitations are met. For example, the Accused Products include the steps of transmitting data between the plurality of stations using a media access layer (MAC), each of the stations having a respective MAC address associated therewith; monitoring transmissions among the plurality of stations to detect failed attempts to authenticate MAC addresses; and generating an intrusion alert based upon detecting a number of failed attempts to authenticate a MAC address.

53. At a minimum, HPE has known of the '678 patent at least as early as the filing date of this complaint.

54. Plaintiff Stingray has been damaged as a result of HPE’s infringing conduct described in this Count. Each Defendant is thus jointly and severally liable to Stingray in an amount that adequately compensates Stingray for HPE’s infringements, which, by law, cannot be

less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT II

(INFRINGEMENT OF U.S. PATENT NO. 7,440,572)

55. Plaintiff incorporates paragraphs 1 through 54 herein by reference.

56. Plaintiff is the assignee of the '572 patent, entitled "Secure wireless LAN device and associated methods," with ownership of all substantial rights in the '572 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

57. The '572 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '572 patent issued from U.S. Patent Application No. 09/760,619.

58. HPE has and continues to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '572 patent in this District and elsewhere in Texas and the United States.

59. On information and belief, HPE designs, develops, manufactures, imports, distributes, offers to sell, sells, and/or uses the Accused Products, including via the activities of HPE and its subsidiaries, members, segments, companies, brands and/or related entities, such as U.S.-based subsidiaries, members, segments, companies, brands and/or related entities.

60. Defendant directly infringes the '572 patent via 35 U.S.C. § 271(a) by making (including, e.g., via contract manufacturers), using, offering for sale, selling, and/or importing the Accused Products, their components, and/or products containing the same that incorporate the fundamental technologies covered by the '572 patent, for example, to or for itself, its alter egos, agents, intermediaries, related entities, distributors, dealers, importers, customers, subsidiaries, members, segments, companies, brands, resellers, dealers, OEMs, integrators, installers, and/or

consumers. Furthermore, on information and belief, Defendant designs the Accused Products for U.S. consumers, has made and/or sold and/or continues to make and/or sell the Accused Products outside of the United States, deliver those products to related entities, subsidiaries, online stores, distribution partners, retailers, showrooms, resellers, dealers, installers, customers and/or related service providers in the United States, or in the case that Defendant delivers the Accused Products outside of the United States Defendant does so intending and/or knowing that those products are destined for the United States and/or designing those products for sale and use in the United States, thereby directly infringing the ‘572 patent. *See, e.g., Lake Cherokee Hard Drive Techs., L.L.C. v. Marvell Semiconductor, Inc.*, 964 F. Supp. 2d 653, 658 (E.D. Tex. 2013) (denying summary judgment and allowing presentation to jury as to “whether accused products manufactured and delivered abroad but imported into the United States market by downstream customers ... constitute an infringing sale under § 271(a)”).

61. Furthermore, Hewlett Packard Enterprise Company directly infringes the ‘572 patent through its direct involvement in the activities of its subsidiaries and related entities, including U.S.-based subsidiaries, members, segments, companies, brands and/or related entities. Defendant designs the Accused Products for U.S. consumers, sells and offers for sale those Accused Products in the U.S. directly and via its related entities, and imports the Accused Products into the United States for sale and/or for its related entities. On information and belief, subsidiaries, members, segments, companies, brands and/or related entities of Defendant, for example, U.S.-based subsidiaries, members, segments, companies, brands and/or related entities of Defendant, conduct activities that constitute direct infringement of the ‘572 patent under 35 U.S.C. § 271(a) by importing, making, offering for sale, selling, and/or using those Accused Products in the U.S. on behalf of and for the benefit of Defendant. Defendant Hewlett Packard Enterprise Company is

vicariously liable for the infringing conduct of Defendant's U.S.-based subsidiaries, members, segments, companies, brands and/or related entities (under both the alter ego and agency theories). On information and belief, Defendant Hewlett Packard Enterprise Company and U.S.-based subsidiaries, members, segments, companies, brands and/or related entities are essentially the same company, comprising subsidiaries, members, segments, companies, brands and/or related entities of HPE. Moreover, Hewlett Packard Enterprise Company, along with its related entities, has the right and ability to control the infringing activities of U.S.-based subsidiaries, members, segments, companies, brands and/or related entities such that Defendant receives a direct financial benefit from that infringement.

62. For example, HPE infringes claim 1 of the '572 patent via the Accused Products that utilize 802.11 (Wi-Fi) protocols, including, but not limited to, HPE access points (e.g., HPE Aruba Networking Access Points with Wi-Fi compatibility), gateways (e.g., Aruba 9200 Series Campus Gateways), controllers (e.g., HPE Aruba Networking 7200 Series Mobility Controllers), HPE packages that include any of these products; and related accessories and software.

63. Those Accused Products include "[a] secure wireless local area network (LAN) device" comprising the limitations of claim 1. The technology discussion above and the example Accused Products provide context for Plaintiff's allegations that each of those limitations are met. For example, the Accused Products include a housing; a wireless transceiver carried by said housing; a medium access controller (MAC) carried by said housing; and a cryptography circuit carried by said housing and connected to said MAC and said wireless transceiver for encrypting both address and data information for transmission by at least adding a plurality of encrypting bits to both the address and the data information, and for decrypting both the address and the data information upon reception.

64. HPE further infringes the '572 patent via 35 U.S.C. § 271(g) by selling, offering to sell, making, using, and/or importing networking, IoT and security devices, their components, and/or products containing same, that are made by a process covered by the '572 patent. On information and belief, the infringing networking, IoT, and security devices, their components, and/or products containing same are not materially changed by subsequent processes, and they are neither trivial nor nonessential components of another product.

65. HPE further infringes based on the importation, sale, offer for sale, manufacture, or use of the Accused Products that are made from a process covered by the '572 patent. To the extent that Plaintiff made reasonable efforts to determine whether the patented processes of the '572 patent were used in the production of the Accused Products but was not able to so determine, the Accused Products should be presumed by this Court to have been so made, pursuant to 35 U.S.C. § 295.

66. At a minimum, HPE has known of the '572 patent at least as early as the filing date of this complaint.

67. On information and belief, since at least the above-mentioned date or dates when HPE was on notice of its infringement, Defendant has actively induced, under 35 U.S.C. § 271(b), importers, online stores, distribution partners, retailers, reseller partners, dealers, installers, OEMs, consumers, and/or related service providers that make, import, distribute, purchase, offer for sale, sell, and/or use the Accused Products that include or are made using all of the limitations of one or more claims of the '572 patent to directly infringe one or more claims of the '572 patent by making, using, offering for sale, selling, and/or importing the Accused Products. Since at least the date or dates of notice referenced above, Defendant does so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '572 patent. On

information and belief, Defendant intends to cause, and has taken affirmative steps to induce, infringement by manufacturers, importers, online stores, distribution partners, retailers, reseller partners, dealers, OEMs, installers, consumers, users, and/or related service providers through at least, *inter alia*, the following activities: creating advertisements that promote the infringing use of the Accused Products; creating and/or maintaining established distribution channels for the Accused Products into and within the United States; manufacturing, testing, certifying, and/or placing orders to manufacture the Accused Products in conformity with U.S. laws and regulations including, for example, the FCC, specifically so that consumers may be induced to purchase and use the Accused Products; distributing or making available instructions or manuals for these products to consumers, installers, purchasers and/or prospective buyers; testing and/or certifying wireless networking features in the Accused Products (with, for example, the WiFi Alliance and/or the Connectivity Standards Alliance, i.e., for Zigbee certification); and/or providing technical support, product files, videos, replacement parts, and/or services for these products to purchasers in the United States. *See, e.g., Accelerate business innovation with HPE GreenLake for Networking*, HPE GREENLAKE, <https://www.hpe.com/us/en/networking.html> (last visited Sep. 5, 2024) (“Combine hardware, software, and services into a single consumption-based subscription with HPE GreenLake for Networking. ... Quickly deploy wired, wireless, and SD-WAN networks, and then add or remove network infrastructure as your organization’s needs change.”); *Troubleshoot user connectivity with Aruba Central*, HEWLETT PACKARD ENTERPRISE, <https://www.youtube.com/watch?v=andCLdWkwyE> (last visited Sep. 5, 2024) (providing consumers with HPE-produced how-to videos related to HPE products, including, for example, monitoring Wi-Fi networks); *Aruba AP-505H Access Points Installation Guide*, ARUBA, pp. 1, 3, (2020), available at <https://fccid.io/Q9DAPINH505/User-Manual/Users-Manual-4693045.pdf>

(last visited Sep. 5, 2024) (manual and product specification provided to the Federal Communications Commission (FCC) on behalf of Hewlett Packard Enterprise Company for “Aruba AP-505H Access Points,” which “support the full 802.11ax (Wi-Fi 6) featureset” and are “equipped with an integrated BLE and Zigbee radio”); *Product Finder*, WiFi ALLIANCE, https://www.wi-fi.org/product-finder-results?sort_by=certified&sort_order=desc&categories=26 (last visited Sep. 5, 2024) (showing listings for 30 Wi-Fi CERTIFIED™ products with up to 9 variants each, said products including, for example, HPE’s AP-679, AP-677, and Aruba Multiservice Mobility Controller/AP-635 access points). Furthermore, HPE markets and offers smartphone and/or tablet interfaces and its application software (e.g., apps) that, via Wi-Fi and/or Zigbee networks, provide access to the Accused Products, connect such products to wireless networks, including Wi-Fi and/or Zigbee networks, provide remote control for HPE and/or other products, provide other services supporting use of the Accused Products and work with smart home platforms including at least Google Assistant, Amazon Alexa, and/or Apple products to manage information and/or control HPE or other products with voice commands or connect with other connected products. See *Downloading the mobile app*, HPE https://support.hpe.com/docs/display/public/a00oc20webhelp/content/getting%20started/download_app.htm (last visited Sep. 6, 2024) (“The HPE OfficeConnect Wi-Fi Portal is available as a [web application](#) and mobile app. With the HPE OfficeConnect Wi-Fi Portal mobile app, you can provision, manage, and monitor your network on the go. ... To install the app on iPhone, go to Apple App Store. [] To install the app on Android phones, go to Google Play Store.”); *What is Edge AI?*, HPE, <https://www.hpe.com/us/en/what-is/edge-ai.html> (last visited Sep. 6, 2024) (“A widespread example of edge AI technology is a virtual assistant like Google Assistant, Apple’s Siri, or Amazon Alexa. ... The edge is where the action is, and HPE is on the forefront of edge AI

platforms and edge infrastructures. ... HPE offers a wide portfolio of edge platforms. For instance, hardware like **HPE Edgeline Converged Systems** enable companies to shift to a distributed converged compute model ... Beyond hardware, services like **HPE Aruba Networking Edge Services Platform (ESP)** deliver the industry's first scalable AI-powered, cloud-native platform"); *Secure your connections from edge to cloud*, HPE, <https://www.hpe.com/us/en/solutions/edge.html> (last visited Sep. 6, 2024) ("Do you need to securely connect your users, applications, and devices—wherever they are—across edge to cloud? ... **Featured edge products and solutions / Edge Solutions** / Securely connect all your users, applications, and devices."). Such compatibility provides convenience and added functionality that induces consumers to use HPE products, including via at least the smartphone and/or tablet Wi-Fi apps, other interfaces utilizing Wi-Fi and/or Zigbee (e.g., for interacting with access points that are both Wi-Fi- and Zigbee-enabled), and other protocols in networks (e.g., Wi-Fi- and/or Zigbee networks) with other third-party devices, and thus further infringe the '572 patent.

68. On information and belief, despite having knowledge of the patent portfolio including the '572 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '572 patent and/or the patent portfolio, HPE has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. Each of Defendant's infringing activities relative to the '572 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

69. Plaintiff Stingray has been damaged as a result of HPE's infringing conduct described in this Count. Each Defendant is thus jointly and severally liable to Stingray in an

amount that adequately compensates Stingray for HPE's infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT III

(INFRINGEMENT OF U.S. PATENT NO. 7,616,961)

70. Plaintiff incorporates paragraphs 1 through 69 herein by reference.

71. Plaintiff is the assignee of the '961 patent, entitled "Allocating channels in a mobile ad hoc network," with ownership of all substantial rights in the '961 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

72. The '961 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '961 patent issued from U.S. Patent Application No. 10/134,862.

73. HPE has and continues to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '961 patent in this District and elsewhere in Texas and the United States.

74. On information and belief, HPE designs, develops, manufactures, imports, distributes, offers to sell, sells, and/or uses the Accused Products, including via the activities of HPE and its subsidiaries, members, segments, companies, brands and/or related entities, such as U.S.-based subsidiaries, members, segments, companies, brands and/or related entities.

75. Defendant directly infringes the '961 patent via 35 U.S.C. § 271(a) by making (including, e.g., via contract manufacturers), using, offering for sale, selling, and/or importing the Accused Products, their components, and/or products containing the same that incorporate the fundamental technologies covered by the '961 patent, for example, to or for itself, its alter egos, agents, intermediaries, related entities, distributors, dealers, importers, customers, subsidiaries,

members, segments, companies, brands, resellers, dealers, OEMs, integrators, installers, and/or consumers. Furthermore, on information and belief, Defendant designs the Accused Products for U.S. consumers, has made and/or sold and/or continues to make and/or sell the Accused Products outside of the United States, deliver those products to related entities, subsidiaries, online stores, distribution partners, retailers, showrooms, resellers, dealers, installers, customers and/or related service providers in the United States, or in the case that Defendant delivers the Accused Products outside of the United States Defendant does so intending and/or knowing that those products are destined for the United States and/or designing those products for sale and use in the United States, thereby directly infringing the '961 patent. *See, e.g., Lake Cherokee Hard Drive Techs., L.L.C. v. Marvell Semiconductor, Inc.*, 964 F. Supp. 2d 653, 658 (E.D. Tex. 2013) (denying summary judgment and allowing presentation to jury as to “whether accused products manufactured and delivered abroad but imported into the United States market by downstream customers ... constitute an infringing sale under § 271(a)”).

76. Furthermore, Defendant Hewlett Packard Enterprise Company directly infringes the '961 patent through its direct involvement in the activities of its subsidiaries and related entities, including U.S.-based subsidiaries, members, segments, companies, brands and/or related entities. Defendant designs the Accused Products for U.S. consumers, sells and offers for sale those Accused Products in the U.S. directly and via its related entities, and imports the Accused Products into the United States for sale and/or for its related entities. On information and belief, subsidiaries, members, segments, companies, brands and/or related entities of Defendant, for example, U.S.-based subsidiaries, members, segments, companies, brands and/or related entities of Defendant, conduct activities that constitute direct infringement of the '961 patent under 35 U.S.C. § 271(a) by importing, making, offering for sale, selling, and/or using those Accused Products in the U.S.

on behalf of and for the benefit of Defendant. Defendant Hewlett Packard Enterprise Company is vicariously liable for the infringing conduct of Defendant's U.S.-based subsidiaries, members, segments, companies, brands and/or related entities (under both the alter ego and agency theories). On information and belief, Defendant Hewlett Packard Enterprise Company and U.S.-based subsidiaries, members, segments, companies, brands and/or related entities are essentially the same company, comprising subsidiaries, members, segments, companies, brands and/or related entities of HPE. Moreover, Hewlett Packard Enterprise Company, along with its related entities, has the right and ability to control the infringing activities of U.S.-based subsidiaries, members, segments, companies, brands and/or related entities such that Defendant receives a direct financial benefit from that infringement.

77. For example, HPE infringes claim 1 of the '961 patent via the Accused Products that utilize Zigbee protocols, including, but not limited to, HPE access points (e.g., HPE Aruba Networking Access Points with Zigbee compatibility); HPE packages that include any of these products; and related accessories and software.

78. Those Accused Products include a "method for dynamic channel allocation in a mobile ad hoc network comprising a plurality of wireless mobile nodes and a plurality of wireless communication links connecting the plurality of wireless mobile nodes together over a plurality of separate channels at different frequencies" comprising the limitations of claim 1. The technology discussion above and the example Accused Products provide context for Plaintiff's allegations that each of those limitations are met. For example, the Accused Products include the steps of at each node, monitoring link performance on a first channel, link performance being based upon at least one quality of service (QoS) threshold; at each node, scouting one or more other available separate channels at different frequencies when the monitored link performance on the first channel falls

below the QoS threshold by at least switching to a second separate channel at a different frequency, broadcasting a channel activity query to determine link performance for the second separate channel, and processing replies to the channel activity query to determine the link performance for the second separate channel; and at each node, updating respective channel activity for the first and second separate channels at different frequencies based upon the processed replies.

79. At a minimum, HPE has known of the '961 patent at least as early as the filing date of this complaint.

80. On information and belief, since at least the above-mentioned date or dates when HPE was on notice of its infringement, Defendant has actively induced, under 35 U.S.C. § 271(b), importers, online stores, distribution partners, retailers, reseller partners, dealers, installers, OEMs, consumers, and/or related service providers that make, import, distribute, purchase, offer for sale, sell, and/or use the Accused Products that include or are made using all of the limitations of one or more claims of the '961 patent to directly infringe one or more claims of the '961 patent by making, using, offering for sale, selling, and/or importing the Accused Products. Since at least the date or dates of notice referenced above, Defendant does so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '961 patent. On information and belief, Defendant intends to cause, and has taken affirmative steps to induce, infringement by manufacturers, importers, online stores, distribution partners, retailers, reseller partners, dealers, OEMs, installers, consumers, users, and/or related service providers through at least, *inter alia*, the following activities: creating advertisements that promote the infringing use of the Accused Products; creating and/or maintaining established distribution channels for the Accused Products into and within the United States; manufacturing, testing, certifying, and/or placing orders to manufacture the Accused Products in conformity with U.S. laws and regulations,

including, for example, the FCC, specifically so that consumers may be induced to purchase and use the Accused Products; distributing or making available instructions or manuals for these products to consumers, installers, purchasers and/or prospective buyers; testing and/or certifying wireless networking features in the Accused Products (with, for example, the WiFi Alliance and/or the Connectivity Standards Alliance, i.e., for Zigbee certification); and/or providing technical support, product files, videos, replacement parts, and/or services for these products to purchasers in the United States. *See, e.g., Accelerate business innovation with HPE GreenLake for Networking*, HPE GREENLAKE, <https://www.hpe.com/us/en/networking.html> (last visited Sep. 5, 2024) (“Combine hardware, software, and services into a single consumption-based subscription with HPE GreenLake for Networking. ... Quickly deploy wired, wireless, and SD-WAN networks, and then add or remove network infrastructure as your organization’s needs change.”); *Troubleshoot user connectivity with Aruba Central*, HEWLETT PACKARD ENTERPRISE, <https://www.youtube.com/watch?v=andCLdWkwyE> (last visited Sep. 5, 2024) (providing consumers with HPE-produced how-to videos related to HPE products, including, for example, monitoring Wi-Fi and Zigbee networks); *Cloud-Managed Networking with HPE Aruba Networking Central: Deploy, optimize, and protect your network from a single point of control*, HPE GREENLAKE, p. 4, available at https://www.hpe.com/us/en/aruba-central.html?jumpid=ps_95cjwsev2_aid-521080305&ef_id=0b5dea32317f16b39a038ce973f162c2:G:s&s_kwid=AL!13472!10!81982461765689!81982660657205&mclid=0b5dea32317f16b39a038ce973f162c2 (last visited Sep. 6, 2024) (“From the [HPE Aruba Networking Central] dashboard, IT can monitor BLE and Zigbee devices connected to any Aruba indoor or outdoor access points running AOS 10, helping converge IT and IoT onto the same network.”); *Aruba AP-505H Access Points Installation Guide*, ARUBA,

pp. 1, 3, (2020), available at <https://fccid.io/Q9DAPINH505/User-Manual/Users-Manual-4693045.pdf> (last visited Sep. 5, 2024) (manual and product specification provided to the Federal Communications Commission (FCC) on behalf of Hewlett Packard Enterprise Company for “Aruba AP-505H Access Points,” which “support the full 802.11ax (Wi-Fi 6) featureset” and are “equipped with an integrated BLE and Zigbee radio”); *Product Finder*, WiFi ALLIANCE, https://www.wi-fi.org/product-finder-results?sort_by=certified&sort_order=desc&categories=26 (last visited Sep. 5, 2024) (showing listings for 30 Wi-Fi CERTIFIED™ products with up to 9 variants each, said products including, for example, HPE’s AP-679, AP-677, and Aruba Multiservice Mobility Controller/AP-635 access points). Furthermore, HPE markets and offers smartphone and/or tablet interfaces and its application software (e.g., apps) that, via Wi-Fi and/or Zigbee networks, provide access to the Accused Products, connect such products to wireless networks, including Wi-Fi and/or Zigbee networks, provide remote control for HPE and/or other products, provide other services supporting use of the Accused Products, and/or work with smart home platforms including at least Google Assistant, Amazon Alexa, and/or Apple products to manage information and/or control HPE or other products with voice commands or connect with other connected products. See *Downloading the mobile app*, HPE https://support.hpe.com/docs/display/public/a00oc20webhelp/content/getting%20started/download_app.htm (last visited Sep. 6, 2024) (“The HPE OfficeConnect Wi-Fi Portal is available as a web application and mobile app. With the HPE OfficeConnect Wi-Fi Portal mobile app, you can provision, manage, and monitor your network on the go. ... To install the app on iPhone, go to Apple App Store. [] To install the app on Android phones, go to Google Play Store.”); *What is Edge AI?*, HPE, <https://www.hpe.com/us/en/what-is/edge-ai.html> (last visited Sep. 6, 2024) (“A widespread example of edge AI technology is a virtual assistant like Google Assistant, Apple’s

Siri, or Amazon Alexa. ... The edge is where the action is, and HPE is on the forefront of edge AI platforms and edge infrastructures. ... HPE offers a wide portfolio of edge platforms. For instance, hardware like **HPE Edgeline Converged Systems** enable companies to shift to a distributed converged compute model ... Beyond hardware, services like **HPE Aruba Networking Edge Services Platform (ESP)** deliver the industry's first scalable AI-powered, cloud-native platform"); *Secure your connections from edge to cloud*, HPE, <https://www.hpe.com/us/en/solutions/edge.html> (last visited Sep. 6, 2024) ("Do you need to securely connect your users, applications, and devices—wherever they are—across edge to cloud? ... **Featured edge products and solutions / Edge Solutions** / Securely connect all your users, applications, and devices."). Such compatibility provides convenience and added functionality that induces consumers to use HPE products, including via at least the smartphone and/or tablet Wi-Fi and/or Zigbee apps, other interfaces utilizing Wi-Fi and/or Zigbee (e.g., for interacting with access points that are both Wi-Fi and Zigbee enabled), and other protocols in networks (e.g., Wi-Fi and/or Zigbee networks) with other third-party devices, and thus further infringe the '961 patent.

81. On information and belief, despite having knowledge of the patent portfolio including the '961 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '961 patent and/or the patent portfolio, HPE has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. Each of Defendant's infringing activities relative to the '961 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

82. Plaintiff Stingray has been damaged as a result of HPE's infringing conduct described in this Count. Each Defendant is thus jointly and severally liable to Stingray in an amount that adequately compensates Stingray for HPE's infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

CONCLUSION

83. Plaintiff is entitled to recover from Defendant the damages sustained by Plaintiff as a result of Defendant's wrongful acts in an amount subject to proof at trial, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court.

84. Plaintiff has incurred and will incur attorneys' fees, costs, and expenses in the prosecution of this action. The circumstances of this dispute may give rise to an exceptional case within the meaning of 35 U.S.C. § 285, and Plaintiff is entitled to recover its reasonable and necessary attorneys' fees, costs, and expenses.

JURY DEMAND

85. Plaintiff hereby requests a trial by jury pursuant to Rule 38 of the Federal Rules of Civil Procedure.

PRAYER FOR RELIEF

86. Plaintiff requests that the Court find in its favor and against Defendant, and that the Court grant Plaintiff the following relief:

- a. A judgment that Defendant has infringed the Asserted Patents as alleged herein, directly infringing the '678 patent, the '572 patent, and the '961 patent and/or indirectly infringing the '572 patent and the '961 patent by way of inducing infringement of such patents;
- b. A judgment for an accounting of damages sustained by Plaintiff as a result of the acts

- of infringement by Defendant;
- c. A judgment and order requiring Defendant to pay Plaintiff damages under 35 U.S.C. § 284, including up to treble damages as provided by 35 U.S.C. § 284, and any royalties determined to be appropriate;
 - d. A judgment and order requiring Defendant to pay Plaintiff pre-judgment and post-judgment interest on the damages awarded;
 - e. A judgment and order finding this to be an exceptional case and requiring Defendant to pay the costs of this action (including all disbursements) and attorneys' fees as provided by 35 U.S.C. § 285; and
 - f. Such other and further relief as the Court deems just and equitable.

Dated: January 10, 2025

Respectfully submitted,

/s/ Jeffrey R. Bragalone

Jeffrey R. Bragalone (lead attorney)

Texas Bar No. 02855775

E-mail: jbragalone@bosfirm.com

Terry A. Saad

Texas Bar No. 24066015

E-mail: tsaad@bosfirm.com

Marcus Benavides

Texas Bar No. 24035574

E-mail: mbenavides@bosfirm.com

Brandon V. Zuniga

Texas Bar no. 24088720

E-mail: bzuniga@bosfirm.com

Mark M.R. Douglass

Texas Bar No. 24131184

E-mail: mdouglass@bosfirm.com

BRAGALONE OLEJKO SAAD PC

901 Main Street

Suite 3800

Dallas, Texas 75202

Telephone: (214) 785-6670

Facsimile: (214) 785-6680

Of Counsel:

Andrea L. Fair

Texas State Bar No. 24078488

E-mail: andrea@millerfairhenry.com

MILLER FAIR HENRY, PLLC

1507 Bill Owens Pkwy

Longview, Texas 75604

Phone: (903) 757-6400

Fax: (903) 757-2323

**ATTORNEYS FOR PLAINTIFF
STINGRAY IP SOLUTIONS LLC**

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a true and correct copy of the foregoing document was electronically filed with the clerk of the court for the U.S. District Court, Eastern District of Texas, Marshall Division, on January 7, 2024, to be served via the Court's electronic filing system upon all counsel of record.

/s/ Marcus Benavides

_____ **MARCUS BENAVIDES**