



3. Upon information and belief, Defendant TP-Link Corporation Limited (“TP-Link Corp.”) is a private limited company organized under the laws of Hong Kong, China, with its principal place of business located at Suite 901, New East Ocean Centre, Tsim Sha Tsui, Hong Kong, China. TP-Link Corp. is at least a related entity of TP-Link Tech. (e.g., having a direct or indirect subsidiary-parent or sister company relationship).

4. Upon information and belief, Defendant TP-Link International Ltd. (“TP-Link Intl”) is a private limited company organized under the laws of Hong Kong, with its principal place of business located at Room 901-902,9/F, New East Ocean Centre, 9 Science Museum Road, Tsim Sha Tsui, Kwun Tong, KL, Hong Kong, China, 518057. TP-Link Intl and TP-Link Corp. share the same corporate office in Hong Kong. TP-Link Intl is at least a related entity of TP-Link Tech. and TP-Link Corp. (e.g., having a direct or indirect subsidiary-parent or sister company relationship). TP-Link Corp., TP-Link Tech., and TP-Link Intl are collectively referred to as “TP-Link” or “Defendants.”

5. TP-Link was founded in 1996 and is “a global provider of reliable networking devices and accessories, involved in all aspects of everyday life.” *About TP-Link*, TP-LINK, <https://www.tp-link.com/us/about-us/corporate-profile/>. Moreover, “as the connected lifestyle continues to evolve, the company is expanding today to exceed the demands of tomorrow.” *Id.* On its global website, TP-Link states that it “is consistently ranked by analyst firm IDC as the No. 1 provider of Wi-Fi devices[], supplying distribution to more than 170 countries and serving billions of people worldwide.” *About TP-Link*, TP-LINK, <https://www.tp-link.com/en/about-us/corporate-profile/>.

6. Upon information and belief, Defendants are engaged in research and development, manufacturing, importation, distribution, sales, and related technical services for home and business networking, Internet of Things (“IoT”), and smart home products and components

(referred to collectively as the “TP-Link Products”). The TP-Link Products include WiFi, Mesh WiFi, and ZigBee networking devices, routers, network expansion devices, network switches, adapters, security cameras, smart plugs, smart lighting, smart switches, and related accessories and services. These TP-Link Products are manufactured outside the U.S. and then imported into the United States, distributed, and sold to end-users via the internet and in brick and mortar stores in the U.S., in Texas and the Eastern District of Texas.

7. Upon information and belief, TP-Link maintains a corporate presence in the United States, including in this judicial district, via at least its wholly-owned U.S.-based subsidiary or related entity TP-Link USA Corporation (“TP-Link USA”), which is a California corporation with its principal office located at 145 South State College Boulevard, Suite 200 Brea, CA 92821 and/or 10 Mauchly, Irvine, California 92618. On behalf and for the benefit of Defendants, TP-Link USA coordinates the importation, distribution, marketing, offers for sale, sale, and use of the TP-Link Products in the U.S. For example, TP-Link maintains distribution channels in the U.S. for TP-Link Products via online stores, distribution partners, retailers, reseller partners, solution partners, and other related service providers. *See Where to Buy*, TP-LINK, <https://www.tp-link.com/us/> (accessible via drop down menu “Where to Buy”); *see also Service Providers*, TP-LINK, <https://service-provider.tp-link.com/>. The TP-Link Products are offered and sold in the U.S. under at least Defendants’ “TP-Link®” “deco,” and “Kasa®” brands. *See, e.g., Products*, KASA SMART, <https://www.kasasmart.com/us/products/smart-plugs>.

8. TP-Link also recruits “TP-Link Brand Ambassadors” via a “Power User” program; these Brand Ambassadors are consumers and users of TP-Link Products that are recruited in the U.S. based on their social media presence and amount of use of TP-Link Products. *See TP-Link Brand Ambassador Program*, TP-LINK, <https://www.tp-link.com/us/brandambassador/>. These

brand ambassadors (also known as “influencers”) are compensated for promoting TP-Link Products on social media and participating in marketing campaigns to raise awareness of TP-Link Products and their respective brands, which, ultimately, increases sales.

9. As a result, via at least TP-Link’s established distribution channels operated and maintained by TP-Link USA in concert with Defendants TP-Link Tech., TP-Link Corp., and TP-Link Intl, TP-Link Products are distributed, sold, advertised, and used nationwide, including being sold to consumers via retail stores operating in Texas and this judicial district. Thus, Defendants do business in the U.S., the state of Texas, and in the Eastern District of Texas.

### **JURISDICTION AND VENUE**

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

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

#### ***TP-Link Tech.***

12. Upon information and belief, TP-Link Tech. 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 judicial 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 judicial 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 judicial 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 judicial district vicariously through and/or in concert with its alter egos, intermediaries, agents, distributors, importers, customers, subsidiaries, and/or

consumers. For example, TP-Link Tech. is related to, owns, and/or controls subsidiaries (such as TP-Link USA) and business sectors (such as its Kasa Smart business) that have a significant business presence in the U.S. and in Texas. *See Where to Buy*, TP-LINK, <https://www.tp-link.com/us/> (identifying established channels of distribution via online stores, distribution partners, retailers, reseller partners, solution partners, and other related service providers). Such a presence furthers the development, design, manufacture, importation, distribution, sale, and use (including by inducement) of infringing TP-Link Products in Texas, including in this judicial district. For example, TP-Link Tech. is also the applicant for FCC registrations for the sale and use of TP-Link Products in the U.S., including being identified on labels as the manufacturing party. *See, e.g., Label Location*, FCCID.IO, *available for download via* <https://fccid.io/TE7HC4V2/Label/3-Label-and-location-4876532.pdf> (providing a copy of the label for TP-Link model no. AC1200 Whole Home Mesh Wi-Fi Unit).

13. This Court has personal jurisdiction over TP-Link Tech., directly and/or through the activities of TP-Link Tech.'s intermediaries, agents, related entities, distributors, importers, customers, subsidiaries, and/or consumers, including through the activities of Defendant TP-Link Corp., TP-Link Intl, and TP-Link USA. Through direction and control of these entities, TP-Link Tech. 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 TP-Link Tech. would not offend traditional notions of fair play and substantial justice.

14. Upon information and belief, TP-Link Tech. controls or otherwise directs and authorizes all activities of its subsidiaries and related entities, including, but not limited to Defendant TP-Link Corp., TP-Link Intl, and U.S.-based TP-Link USA. Directly via its agents in

the U.S. and via at least distribution partners, retailers (including national retailers), reseller partners, solution partners, brand ambassadors, and other service providers, TP-Link Tech. has placed and continues to place infringing TP-Link Products into the U.S. stream of commerce. For example, import records show that TP-Link Tech. delivers TP-Link Products to TP-Link USA in the U.S. *See, e.g., Supply Chain Intelligence about: Tp Link Technologies Co. Ltd.*, PANJIVA, <https://panjiva.com/Tp-Link-Technologies-Co-Ltd/27804596> (showing at least two shipments to “TP Link USA Corporation” in January of 2021 consisting of, for example, “Kasa smart bulb” and other networking products). TP-Link Tech. has placed such products into the stream of commerce with the knowledge and understanding that such products are, will be, and continue to be sold, offered for sale, and/or imported into this judicial district and the State of Texas. *See Litecubes, LLC v. Northern Light Products, Inc.*, 523 F.3d 1353, 1369-70 (Fed. Cir. 2008) (“[T]he sale [for purposes of § 271] occurred at the location of the buyer.”); *see also Semcon IP Inc. v. Kyocera Corporation*, No. 2:18-cv-00197-JRG, 2019 WL 1979930, at \*3 (E.D. Tex. May 3, 2019) (denying accused infringer’s motion to dismiss because plaintiff sufficiently plead that purchases of infringing products outside of the United States for importation into and sales to end users in the U.S. may constitute an offer to sell under § 271(a)).

15. TP-Link Tech. utilizes established distribution channels to distribute, market, offer for sale, sell, service, and warrant infringing products directly to consumers and other users, including providing links to via its own website to online stores, retailers, resellers, distributors, and solution partners offering such products and related services for sale. *See Where to Buy*, TP-LINK, <https://www.tp-link.com/us/>. Such TP-Link Products and services have been sold in retail stores, both brick and mortar and online, within this judicial district and in Texas, including well-known and widely used retailers Amazon.com, HSN, newegg.com, Sears, QVC, Micro Center,

BestBuy, Costco, Lowes, Nebraska Furniture Mart, The Home Depot, Office Depot, Target, Staples, Sam’s Club, Walmart, Conn’s Home Plus, Game Stop, and Brookstone. *See, e.g., TP-Link - Deco AC2200*, BEST BUY, <https://www.bestbuy.com/site/tp-link-deco-ac2200-tri-band-mesh-wi-fi-system-with-built-in-smart-hub-2-pack-white/6324964.p?skuId=6324964> (showing that TP-Link – Deco AC220 is offered for sale at BestBuy location at 190 E Stacy Rd Allen, TX 75002, i.e., in this judicial district). TP-Link Tech. also provides application software (“apps”), the “Deco App” and the “Kasa Smart” app for download and use in conjunction with and as a part of the wireless communication network that connects TP-Link Products and other network devices. These apps are available via digital distribution platforms operated by Apple Inc. and Google for download by users and execution on smartphone devices. *See, e.g., TP-Link Deco*, GOOGLE PLAY, [https://play.google.com/store/apps/details?id=com.tplink.tpm5&hl=en\\_US](https://play.google.com/store/apps/details?id=com.tplink.tpm5&hl=en_US) (offering the application for download and indicating that the application is offered by TP-Link Tech.’s subsidiary or related entity “TP-Link Corporation Limited”).

16. Based on TP-Link Tech.’s connections and relationship with these national retailers and digital distribution platforms, TP-Link Tech. knows that Texas is a termination point of the established distribution channel, namely online and brick and mortar stores offering TP-Link Products and related services and software to distribution partners, retailers (including national retailers), reseller partners, solution partners, brand ambassadors, service providers, consumers, and other users in Texas. TP-Link Tech., therefore, has purposefully directed its activities at Texas, and should reasonably anticipate being brought in this Court, at least on this basis. *See Icon Health & Fitness, Inc. v. Horizon Fitness, Inc.*, 2009 WL 1025467, at (E.D. Tex. 2009) (finding that “[a]s a result of contracting to manufacture products for sale in” national retailers’ stores, the defendant

“could have expected that it could be brought into court in the states where [the national retailers] are located”).

17. Upon information and belief, TP-Link Tech. alone and in concert with other related entities such as Defendant TP-Link Corp., Defendant TP-Link Intl, and U.S.-based TP-Link USA manufactures and purposefully places infringing TP-Link Products in established distribution channels in the stream of commerce, including in Texas, via distributors and reseller partners, such as at least those listed on TP-Link’s website. For example, TP-Link Tech. imports to Texas or through a related entity and directly sells and offers for sale infringing TP-Link Products in Texas to distributor CDW Corporation (“CDW”), which has a distribution location at 5908 Headquarters Dr., Suite 200, Plano, TX 75024, which is in this judicial district. *See Locations*, CDW, <https://www.cdw.com/content/cdw/en/locations.html>. CDW offers infringing TP-Link Products for sale on its website. *See, e.g., TP-Link DECO M5 - Wi-Fi system*, CDW, <https://www.cdw.com/product/tp-link-deco-m5-wi-fi-system-802.11b-g-n-ac-bluetooth-4.2-desktop/5085325?pfm=srh>. Via this website, TP-Link Products are offered for sale to consumers in the state of Texas. TP-Link Tech. also delivers networking products directly to distributors in the U.S., such as Solution Box LLC (located in Miami, FL), as indicated by import records. *See, e.g., Supply Chain Intelligence about: Tp Link Technologies Co. Ltd.*, PANJIVA, <https://panjiva.com/Tp-Link-Technologies-Co-Ltd/27804596> (showing at least one shipment to “Solution Box LLC” in January of 2021 consisting of, for example, networking products). These suppliers and distributors import, advertise, offer for sale and sell TP-Link Products via their own websites to U.S. consumers, including to consumers in Texas. Based on TP-Link Tech.’s connections and relationship, including supply contracts and other agreements with the U.S. and Texas-based distributors and suppliers, such as at least CDW, TP-Link Tech. knows and has



known that Texas is a termination point of the established distribution channels for TP-Link Products. TP-Link Tech., alone and in concert with related entities Defendant TP-Link Corp., Defendant TP-Link Intl, and U.S.-based TP-Link USA has purposefully directed its activities at Texas, and should reasonably anticipate being brought in this Court, at least on this basis. *See Ultravision Technologies, LLC v. Holophane Europe Limited*, 2020 WL 3493626, at \*5 (E.D. Tex. 2020) (finding sufficient to make a *prima facie* showing of personal jurisdiction allegations that “Defendants either import the products to Texas themselves or through a related entity”); *see also Bench Walk Lighting LLC v. LG Innotek Co., Ltd et al.*, Civil Action No. 20-51-RGA, 2021 WL 65071, at \*7-8 (D. Del., Jan. 7, 2021) (denying motion to dismiss for lack of personal jurisdiction based on the foreign defendant entering into supply contract with U.S. distributor and the distributor sold and shipped defendant’s products from the U.S. to the a customer in the forum state).

18. In the alternative, this Court has personal jurisdiction over TP-Link Tech. under Federal Rule of Civil Procedure 4(k)(2), because the claims for patent infringement in this action arise under federal law, TP-Link Tech. is not subject to the jurisdiction of the courts of general jurisdiction of any state, and exercising jurisdiction over TP-Link Tech. is consistent with the U.S. Constitution.

19. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391. Defendant TP-Link Tech. is a foreign entity and may be sued in any judicial district under 28 U.S.C. § 1391(c).

***TP-Link Corp.***

20. Upon information and belief, Defendant TP-Link Corp. 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 judicial 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 judicial 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 judicial 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 judicial district vicariously through and/or in concert with its partners, alter egos, intermediaries, agents, distributors, importers, customers, subsidiaries, and/or consumers. For example, TP-Link Corp. and related entities Defendant TP-Link Corp., Defendant TP-Link Intl, and U.S.-based TP-Link USA manufacture, import, distribute, offer for sale, sell, and induce infringing use of TP-Link Products to distribution partners, retailers (including national retailers), reseller partners, solution partners, brand ambassadors, service providers, consumers, and other users.

21. This Court has personal jurisdiction over TP-Link Corp., directly and/or indirectly via the activities of TP-Link Corp.'s intermediaries, agents, related entities, distributors, importers, customers, subsidiaries, and/or consumers, including related entities Defendant TP-Link Tech., Defendant TP-Link Intl, and U.S.-based TP-Link USA. Alone and in concert with or via direction and control of or by at least these entities, TP-Link Corp. 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, TP-Link Corp. is at least a related entity with TP-Link Tech., TP-Link Intl, and subsidiary TP-Link USA in a global network of sales and distribution of TP-Link Products that includes retail stores and distributors operating in Texas, including this judicial district. *See Choose Your Location*, TP-LINK, <https://www.tp-link.com/us/choose-your-location/>. TP-Link Corp. directly and via direction and control of or by its related entities participates in the manufacture, shipping, importing and

distribution of TP-Link Products to the U.S. For example, TP-Link Corp. is the applicant for FCC registrations for the sale and use of TP-Link Products in the U.S., including being identified on labels as the manufacturing party. *See, e.g., Label Location, FCCID.IO, available for download via <https://fccid.io/2AXJ4P9V2/Label/2AXJ4P9V2-Label-Location-5079096.pdf>* (providing a copy of the label for TP-Link model no. AC1200 + AV1000). As a part of TP-Link's global manufacturing and distribution network, TP-Link Corp. also purposefully places infringing TP-Link Products in established distribution channels in the stream of commerce, including in Texas, via distribution partners, retailers (including national retailers), reseller partners, solution partners, brand ambassadors, service providers, consumers, and other users. Therefore, TP-Link Corp., alone and in concert with related entities Defendant TP-Link Tech., Defendant TP-Link Intl, and subsidiary TP-Link USA, has purposefully directed its activities at Texas, and should reasonably anticipate being brought in this Court, at least on this basis.

22. This Court has personal jurisdiction over TP-Link Corp., directly and/or through the activities of TP-Link Corp.'s intermediaries, agents, related entities, distributors, importers, customers, subsidiaries, and/or consumers, including through the activities of Defendant TP-Link Tech., TP-Link Intl, and TP-Link USA. Through its own conduct and through direction and control of these entities or control by other Defendants, TP-Link Corp. 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 TP-Link Corp. would not offend traditional notions of fair play and substantial justice.

23. In the alternative, the Court has personal jurisdiction over TP-Link Corp. under Federal Rule of Civil Procedure 4(k)(2), because the claims for patent infringement in this action arise under federal law, TP-Link Corp. is not subject to the jurisdiction of the courts of general

jurisdiction of any state, and exercising jurisdiction over TP-Link Corp. is consistent with the U.S. Constitution.

24. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391 because, among other things, TP-Link Corp. is not a resident in the United States, and thus may be sued in any judicial district, including this one, pursuant to 28 U.S.C. § 1391(c)(3). *See also In re HTC Corporation*, 889 F.3d 1349, 1357 (Fed. Cir. 2018) (“The Court’s recent decision in *TC Heartland* does not alter” the alien-venue rule.).

***TP-Link Intl***

25. Upon information and belief, Defendant TP-Link Intl 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 judicial 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 judicial 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 judicial 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 judicial district vicariously through and/or in concert with its partners, alter egos, intermediaries, agents, distributors, importers, customers, subsidiaries, and/or consumers. For example, TP-Link Intl and related entities Defendant TP-Link Tech., Defendant TP-Link Corp., and U.S.-based TP-Link USA manufacture, import, distribute, offer for sale, sell, and induce infringing use of TP-Link Products to distribution partners, retailers (including national retailers), reseller partners, solution partners, brand ambassadors, service providers, consumers, and other users.

26. This Court has personal jurisdiction over TP-Link Intl, directly and/or indirectly via the activities of TP-Link Intl's intermediaries, agents, related entities, distributors, importers, customers, subsidiaries, and/or consumers, including related entities Defendant TP-Link Tech., Defendant TP-Link Corp., and U.S.-based TP-Link USA. Alone and in concert with or via direction and control of or by at least these entities, TP-Link Corp. 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, TP-Link Intl operates in a global network of sales and distribution of TP-Link Products that includes retail stores and distributors operating in Texas, including this judicial district. *See Choose Your Location*, TP-LINK, <https://www.tp-link.com/us/choose-your-location/>. TP-Link Intl also directly and via direction and control of its related entities participates in the manufacture, shipping, importing and distribution of TP-Link Products to the U.S. For example, TP-Link Intl is the applicant for FCC registrations for the sale and use of TP-Link Products in the U.S., including being identified on labels as the manufacturing party. *See, e.g., Label Location*, FCCID.IO, *available for download via* <https://fccid.io/2AXJ4P9V2/Label/2AXJ4P9V2-Label-Location-5079096.pdf> (providing a copy of the label for TP-Link model no. AC1200 + AV1000). TP-Link Intl also delivers TP-Link Products, such as networking products, directly to TP-Link USA in the U.S., according to import records. *See Supply Chain Intelligence about: Tp Link International Ltd.*, PANJIVA, <https://panjiva.com/Tp-Link-International-Ltd/39242970>. As a part of TP-Link's global manufacturing and distribution network, TP-Link Intl also purposefully places infringing TP-Link Products in established distribution channels in the stream of commerce, including in Texas, via distribution partners, retailers (including national retailers), reseller partners, solution partners, brand ambassadors, service providers, consumers, and other users. Therefore, TP-Link Intl, alone

and in concert with related entities Defendant TP-Link Tech., Defendant TP-Link Corp., and subsidiary TP-Link USA, has purposefully directed its activities at Texas, and should reasonably anticipate being brought in this Court, at least on this basis.

27. This Court has personal jurisdiction over TP-Link Intl, directly and/or through the activities of TP-Link Intl's intermediaries, agents, related entities, distributors, importers, customers, subsidiaries, and/or consumers, including through the activities of Defendant TP-Link Tech., TP-Link Corp., and TP-Link USA. Through its own conduct and through direction and control of these entities or control by other Defendants, TP-Link Intl 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 TP-Link Intl would not offend traditional notions of fair play and substantial justice.

28. In the alternative, the Court has personal jurisdiction over TP-Link Intl under Federal Rule of Civil Procedure 4(k)(2), because the claims for patent infringement in this action arise under federal law, TP-Link Intl is not subject to the jurisdiction of the courts of general jurisdiction of any state, and exercising jurisdiction over TP-Link Intl is consistent with the U.S. Constitution.

29. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391 because, among other things, TP-Link Intl is not a resident in the United States, and thus may be sued in any judicial district, including this one, pursuant to 28 U.S.C. § 1391(c)(3). *See also In re HTC Corporation*, 889 F.3d 1349, 1357 (Fed. Cir. 2018) (“The Court's recent decision in *TC Heartland* does not alter” the alien-venue rule.).

30. On information and belief, Defendants TP-Link Tech., TP-Link Corp., and TP-Link Intl each have significant ties to, and presence in, the State of Texas and the Eastern District of Texas, making venue in this judicial district both proper and convenient for this action.

**THE ASSERTED PATENTS AND TECHNOLOGY**

31. The Asserted Patents cover various aspects of monitoring, detecting intrusions, and encrypting and decrypting wireless communications networks, including networks created between home and business networking, IoT, and smart home products and components.

32. The '117 patent involves detecting intrusions into a wireless communication network by monitoring transmissions among nodes of the network. The disclosed intrusion detection techniques of the '117 patent include monitoring, by a policing node, transmissions among a plurality of nodes of a mobile ad-hoc network (MANET). Such nodes of the MANET intermittently operate in a contention-free mode during a contention-free period. The policing node detects intrusions by monitoring the transmissions between the MANET nodes to detect contention-free mode operation outside of a contention-free period. Based on such a detection, an intrusion alert may be generated.

33. 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.

34. The '961 patent involves allocating channels in mobile ad hoc networks. The patent describes dynamic channel allocation in such networks to efficiently make use of a plurality of channels. In such networks, wireless communication links connect wireless mobile 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.

35. 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) 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.

36. Upon information and belief, a significant portion of the operating revenue of Defendants is derived from the manufacture, distribute, sale, and use of home and business networking, IoT, and smart home products and components, which are imported into the United States, distributed, and ultimately sold to and used by U.S. consumers. For example, TP-Link's global website touts that it is "consistently ranked by analyst firm IDC as the No. 1 provider of Wi-Fi devices[], supplying distribution to more than 170 countries and serving billions of people worldwide...[a]ccording to latest published IDC Worldwide Quarterly WLAN Tracker Report, Q2 2018 Final Release." *See About TP-Link*, TP-LINK, <https://www.tp-link.com/en/about-us/corporate-profile/>.

37. The Asserted Patents cover Defendants' home and business networking, IoT, and smart home products and components, software, services, and processes related to same that



generally connect to other devices in a network or other networks (including in IoT and cloud networks) using a wireless protocol, such as ZigBee and WiFi, including, but not limited to, Defendants’ Deco Whole Home Mesh Wi-Fi, Home and Business Wi-Fi Routers, Network Expanders, Network Switches, Adapters, Security Cameras, Smart Plugs, Smart Lighting, Smart Switches, and related accessories and software (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.

38. Examples of Defendant’s Accused Products are at least the family of TP-Link’s mesh technology, incorporated in, for example, Deco M9 Plus devices. These device “provide whole-home IoT coverage with Wi-Fi, Bluetooth, and ZigBee integrated into a single system.” The Asserted Patents cover TP-Links Products that use ZigBee protocol to communicate with other devices on the network, including those of third-party manufacturers.. ZigBee protocol is based on the IEEE 802.15.4 standard. *See Deco M9 Plus Smart Home Device Compatible List*, TP-LINK, <https://www.tp-link.com/us/Deco-M9-Plus/compatibility/>. An example of the Deco M9 Plus is shown below:



39. The IEEE 802.15.4, i.e., ZigBee, 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 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](http://ecee.colorado.edu/~liue/teaching/comm_standards/2015S_zigbee/802.15.4-2011.pdf)

40. LR-WPAN network allows use of a superframe structure. A superframe is bounded by network beacons sent by the coordinator node and is divided into 16 slots of equal duration. The superframe includes a contention access period (CAP) and a contention free period (CFP), together accounting for the 16 superframe time slots. By default, the network nodes use CAP for data/frame transmission.

#### 4.5 Functional overview

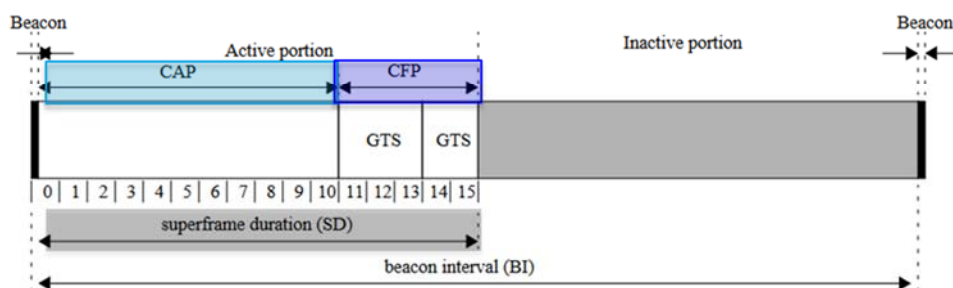
A brief overview of the general functions of a LR-WPAN is given in this subclause.

##### 4.5.1 Superframe structure

This standard allows the optional use of a superframe structure. The format of the superframe is defined by the coordinator. The superframe is bounded by network beacons sent by the coordinator, as illustrated in Figure 4a), and is divided into 16 slots of equal duration. Optionally, the superframe can have an active and an inactive portion, as illustrated in Figure 4b). During the inactive portion, the coordinator is able to enter a low-power mode. The beacon frame transmission starts at the beginning of the first slot of each superframe.

##### 5.1.1.1.1 Contention access period (CAP)

The CAP shall start immediately following the beacon and complete before the beginning of the CFP on a superframe slot boundary. If the CFP is zero length, the CAP shall complete at the end of the active portion of the superframe. The CAP shall be at least *aMinCAPLength*, unless additional space is needed to



**Figure 8—An example of the superframe structure**

temporarily accommodate the increase in the beacon frame length needed to perform GTS maintenance, as described in 5.2.2.1.3, and shall shrink or grow dynamically to accommodate the size of the CFP.

All frames, except acknowledgment frames and any data frame that quickly follows the acknowledgment of a data request command, as described in 5.1.6.3, transmitted in the CAP shall use a slotted CSMA-CA mechanism to access the channel. A device transmitting within the CAP shall ensure that its transaction is complete (i.e., including the reception of any acknowledgment) one interframe spacing (IFS) period, as

**contention access period:** The period of time immediately following a beacon frame during which devices wishing to transmit will compete for channel access using a slotted carrier sense multiple access with collision avoidance mechanism.

41. In the superframe, the length of the CAP is required to be at least equal to – aMinCAPLength. The PAN coordinator monitors, i.e., a policing node, if a device’s request to add a new GTS (e.g., to an existing CFS in the superframe) would result in reduction of the aMinCAPLength. A newly requested GTS lies outside an existing CFP and will be used for transmission by the requesting device.

**5.1.7.2 GTS allocation**

A device is instructed to request the allocation of a new GTS through the MLME-GTS.request primitive, as described in 6.2.6.1, with GTS characteristics set according to the requirements of the intended application.

On receipt of a GTS request command indicating a GTS allocation request, the PAN coordinator shall first check if there is available capacity in the current superframe, based on the remaining length of the CAP and the desired length of the requested GTS. The superframe shall have available capacity if the maximum number of GTSs has not been reached and allocating a GTS of the desired length would not reduce the length of the CAP to less than aMinCAPLength. GTSs shall be allocated on a first-come-first-served basis by the PAN coordinator provided there is sufficient bandwidth available. The PAN coordinator shall make

**5.2.2.1.2 Superframe Specification field**

The Superframe Specification field shall be formatted as illustrated in Figure 41.

Bits: 0–3	4–7	8–11	12	13	14	15
Beacon Order	Superframe Order	Final CAP Slot	Battery Life Extension (BLE)	Reserved	PAN Coordinator	Association Permit

**Figure 41—Format of the Superframe Specification field**

The Final CAP Slot field specifies the final superframe slot utilized by the CAP. The duration of the CAP, as implied by this field, shall be greater than or equal to the value specified by aMinCAPLength. However, an

<u>aMinCAPLength</u>	The minimum number of symbols forming the CAP. This ensures that MAC commands can still be transferred to devices when GTSs are being used. An exception to this minimum shall be allowed for the accommodation of the temporary increase in the beacon frame length needed to perform GTS maintenance, as described in 5.2.2.1.3.	440
----------------------	--	-----

**5.1.7.1 CAP maintenance**

The PAN coordinator shall preserve the minimum CAP length of aMinCAPLength and take preventative action if the minimum CAP is not satisfied. However, an exception shall be allowed for the accommodation

Page 49, 62, 125, [http://ecee.colorado.edu/~liue/teaching/comm\\_standards/2015S\\_zigbee/802.15.4-2011.pdf](http://ecee.colorado.edu/~liue/teaching/comm_standards/2015S_zigbee/802.15.4-2011.pdf)

42. If the new GTS (lying outside the existing CFP) reduces the minimum CAP length of  $aMinCAPLength$ , a next higher layer of the coordinator is notified, i.e., generates an intrusion alert, which then, as indicated in the excerpt below, takes preventative actions to deallocate one or more of the existing GTSs (forming the existing CFP) in the superframe.

#### 5.1.7.1 CAP maintenance

The PAN coordinator shall preserve the minimum CAP length of  $aMinCAPLength$  and take preventative action if the minimum CAP is not satisfied. However, an exception shall be allowed for the accommodation of the temporary increase in the beacon frame length needed to perform GTS maintenance. If preventative action becomes necessary, the action chosen is left up to the implementation but may include one or more of the following:

- Limiting the number of pending addresses included in the beacon.
- Not including a payload field in the beacon frame.
- Deallocating one or more of the GTSs.

Figure 32 depicts the message flow for the cases in which a GTS deallocation is initiated by the PAN coordinator.

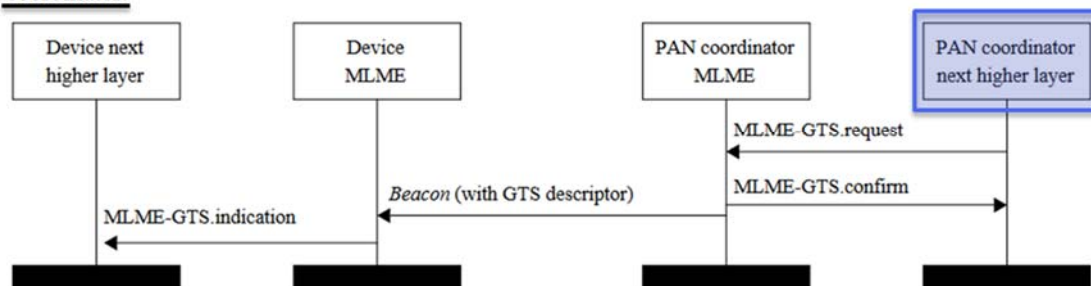


Figure 32—Message sequence chart for GTS deallocation initiated by the PAN coordinator

Page 49, 52, [http://ecee.colorado.edu/~liue/teaching/comm\\_standards/2015S\\_zigbee/802.15.4-2011.pdf](http://ecee.colorado.edu/~liue/teaching/comm_standards/2015S_zigbee/802.15.4-2011.pdf)

43. The Accused Products, including the TP-Link Products, such as Deco M9 Plus devices, also practice a method for dynamic channel allocation in a mobile ad hoc network. As indicated below, “[a] single device can become the Network Channel Manager.”

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



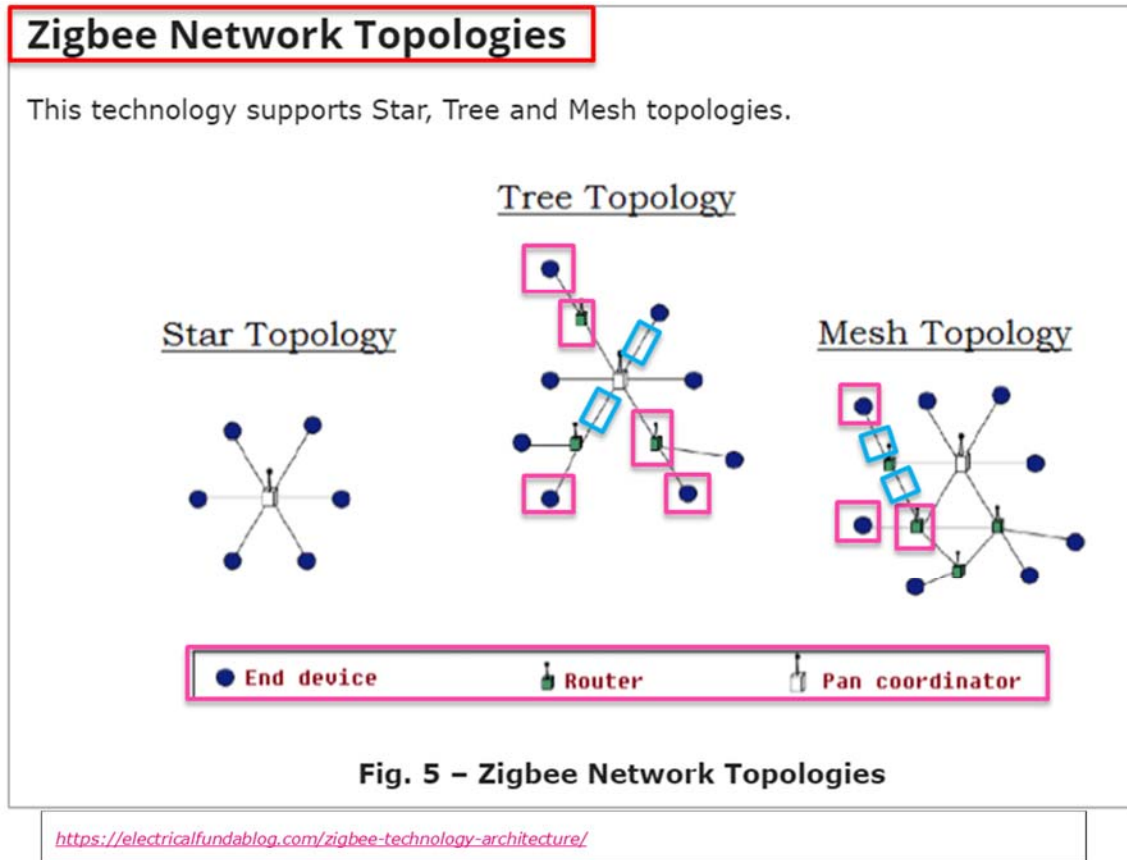
A single device can become the Network Channel Manager. This device acts as the central mechanism for reception of network interference reports and changing the channel of the network if interference is detected. The default address of the network manager is the coordinator, however this can be updated 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 procedure<sup>1</sup>:

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>

44. As indicated below, in different ZigBee Network topologies of the Accused Products, a plurality of network nodes are connected together via a respective plurality communication links.



45. 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 procedure<sup>1</sup>:

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>

46. 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 procedure<sup>1</sup>:

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.

**Comment:** Zigbee network further allows network devices/nodes to function as Network Channel Manager. The network manager node facilitates switching to a different channel 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).

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

47. With reference to the above excerpt 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.

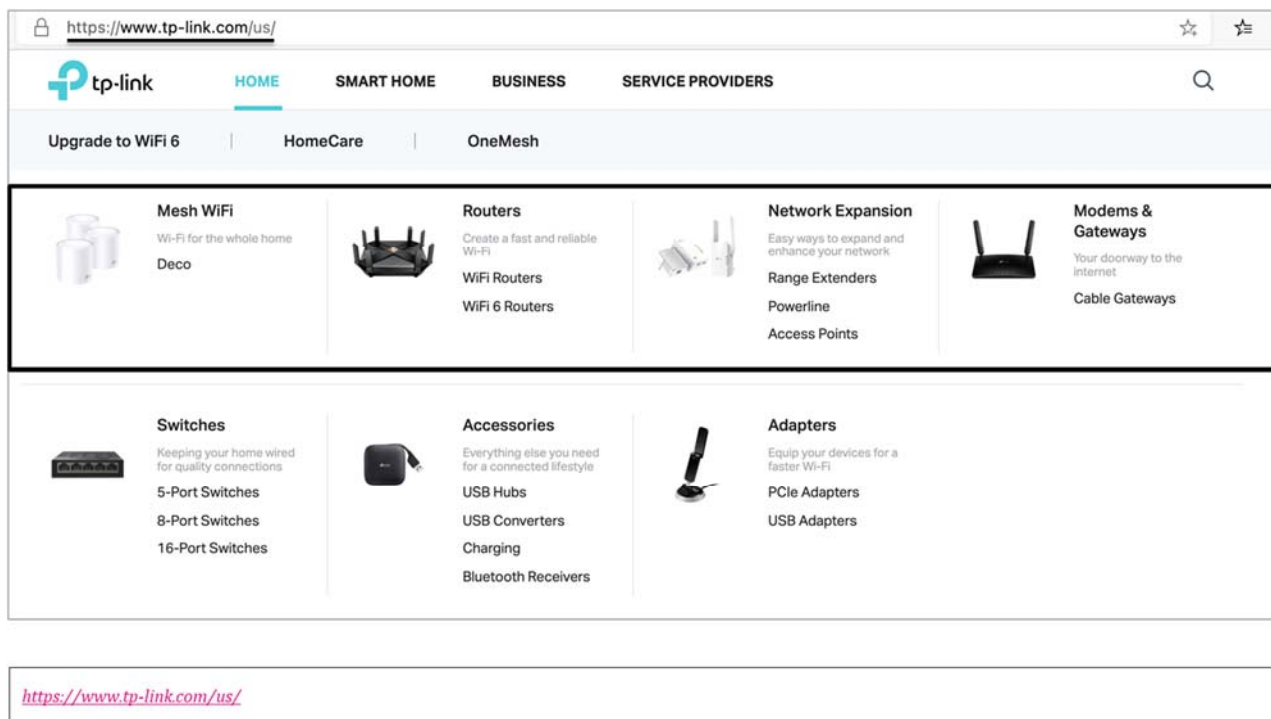
The network manager may do the following:

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>

48. The Asserted Patents also cover TP-Link Products, such as Deco Whole Home Mesh Wi-Fi, Home and Business Wi-Fi Routers, Cable Routers, Gaming Routers, Network Expanders, Network Switches, Adapters, Kasa Security Cameras, Kasa Smart Plugs, Kasa Smart Lighting, Kasa Smart Switches, Omada (a TP-Link brand) access points, desktop access points, power line products, and related accessories and software, that are Wi-Fi (IEEE 802.11) compliant, such as those shown below.



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

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

### 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>

50. 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>

51. 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>

52. 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>

53. 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>


54. The Asserted Patents also cover TP-Link Products that are Wi-Fi compliant devices, which support WPA and WPA2-AES security mechanisms, as described below. Of the WPA and WPA2 security mechanism used by the Accused Products, such as the Deco M9 Plus, the WPA is based on Temporal Key Integrity Protocol (TKIP), while, as described below, the WPA2-AES is




based on Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP). Shown below are exemplary IEEE 802.11 compliant TP-Link Product device/stations (STA) from the Deco M9 Plus, the Archer AX1000, and the Kasa Spot.

<p><b>Deco M9 Plus</b> <span style="color: red; font-weight: normal;">Hot Buys</span> AC2200 Smart Home Mesh WiFi System</p>	
--	---

SECURITY	
WiFi Encryption	<div style="border: 2px solid green; padding: 5px;">                 WPA WPA2             </div>

<p><b>Archer AX11000</b> <span style="color: red; font-weight: normal;">Hot Buys</span> AX11000 Next-Gen Tri-Band Gaming Router</p>	
---	--

SECURITY	
WiFi Encryption	<div style="border: 2px solid green; padding: 5px;">                 WPA WPA2 WPA3 WPA/WPA2-Enterprise (802.1x)             </div>

<p><b>Kasa Spot<sup>®</sup>, 24/7 Recording</b> Always Spot On.   EC60</p>	
--	--


Wireless Encryption	<div style="border: 2px solid green; padding: 5px;">                 WEP, PWPA/WPA2-PSK             </div>
---------------------	--

55. The Accused Products, such as the Deco M9 Plus, are devices that have a housing.



<https://www.tp-link.com/us/deco-mesh-wifi/product-family/deco-m9-plus/>

56. As shown below, the Accused Products, e.g., TP-Link’s Deco M9 Plus, provide 2.4 GHz and 5 GHz Wi-Fi speeds. This capability ascertains the presence of a Wi-Fi antenna and transceiver in the device.

		Deco   Deco M9 Plus	
Standards		Wi-Fi 5 IEEE 802.11ac/n/a 5 GHz IEEE 802.11n/b/g 2.4 GHz Bluetooth 4.2 ZigBee HA 1.2	
SECURITY		AC2200	
WiFi Encryption	WPA WPA2	WiFi Speeds	5 GHz: 867 Mbps (802.11ac) 5 GHz: 867 Mbps (802.11ac) 2.4 GHz: 400 Mbps (802.11n)

<https://www.tp-link.com/us/deco-mesh-wifi/product-family/deco-m9-plus/#specifications>

57. 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.

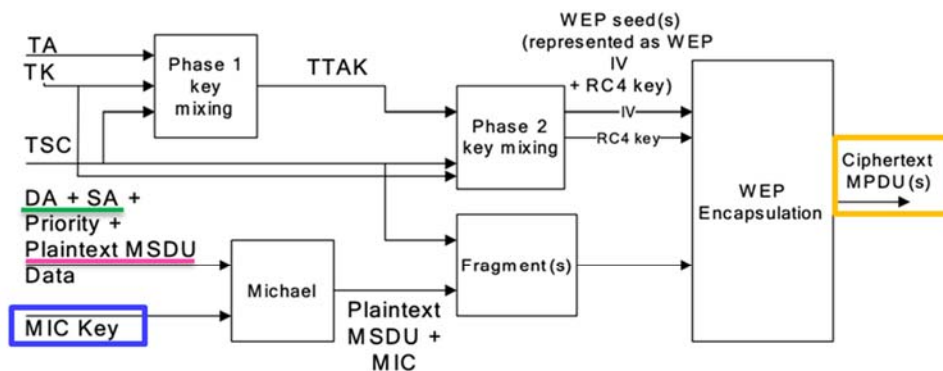


Figure 8-4—TKIP encapsulation block diagram

- 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.
- 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).
- For each MPDU, TKIP uses the key mixing function to compute the WEP seed.
- 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. 7,082,117)

58. Plaintiff incorporates paragraphs 1 through 57 herein by reference.

59. Plaintiff is the assignee of the '117 patent, entitled "Mobile ad-hoc network with intrusion detection features and related methods," with ownership of all substantial rights in the '117 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

60. The '117 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '117 patent issued from U.S. Patent Application No. 10/217,097.

61. TP-Link has and continues to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '117 patent in this judicial district and elsewhere in Texas and the United States.

62. Upon information and belief, TP-Link designs, develops, manufactures, imports, distributes, offers to sell, sells, and uses the Accused Products, including via the activities of TP-Link Tech. and its subsidiaries or related entities, such as Defendant TP-Link Corp., Defendant TP-Link Intl and TP-Link USA.

63. Defendants TP-Link Tech., TP-Link Corp., and TP-Link Intl (i.e., "TP-Link") each directly infringe the '117 patent via 35 U.S.C. § 271(a) by making, 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 '117 patent to, for example, its alter egos, agents, intermediaries, related entities, distributors, importers, customers, subsidiaries, and/or consumers. Furthermore, upon information and belief, Defendants make and sell the Accused Products outside of the United States, deliver those products to related entities, subsidiaries, online stores, distribution partners, retailers, reseller partners, solution partners, customers and other related service providers in the United States, or in the case that it delivers the Accused Products outside of the United States it 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 '117 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)”).

64. Furthermore, Defendant TP-Link Tech. directly infringes the '117 patent through its direct involvement in the activities of its subsidiaries and related entities, including Defendants TP-Link Corp., Defendant TP-Link Intl, and TP-Link USA., including by selling and offering for sale the Accused Products directly to its related entities and importing the Accused Products into the United States for its related entities. Upon information and belief, TP-Link USA conducts activities that constitutes direct infringement of the '117 patent under 35 U.S.C. § 271(a) by importing, offering for sale, selling, and/or using those Accused Products in the U.S. on behalf of and for the benefit of Defendants. TP-Link Tech. is vicariously liable for the infringing conduct of Defendants TP-Link Corp., Defendant TP-Link Intl, and TP-Link USA and other subsidiaries (under both the alter ego and agency theories) because, as an example and on information and belief, Defendants TP-Link Tech., TP-Link Corp., Defendant TP-Link Intl, and TP-Link USA are essentially the same company, and TP-Link Tech. along with its related entities have the right and ability to control the infringing activities of Defendant TP-Link Corp., Defendant TP-Link Intl, and TP-Link USA and TP-Link Tech. receives a direct financial benefit from that infringement.

65. For example, TP-Link infringes claim 24 of the '117 patent via the Accused Products that use the ZigBee protocol to communicate with each other, such as TP-Link home and business networking, IoT, and smart home products and components. Those Accused Products include “[a] mobile ad-hoc network (MANET)” comprising the limitations of claim 24. The technology discussion above and the example Accused Products, e.g., TP-Link’s Deco M9 Plus product, provide context for Plaintiff’s allegations that each of those limitations are met. For

example, the Accused Products include a plurality of nodes for transmitting data therebetween, said plurality of nodes intermittently operating in a contention-free mode during contention-free periods (CFPs) and in a contention mode outside CFPs; and a policing node for detecting intrusions into the MANET by monitoring transmissions among said plurality of nodes to detect contention-free mode operation outside of a CFP; and generating an intrusion alert based upon detecting contention-free mode operation outside a CFP.

66. At a minimum, TP-Link has known of the '117 patent at least as early as the filing date of this complaint. In addition, TP-Link has known about the '117 patent since at least July 16, 2020, when TP-Link received a letter regarding infringement of Stingray's patent portfolio, which includes the '117 patent and is related to mesh networking used in wireless control of home automation devices. The letter specifically referenced the infringing use of Stingray's patented technologies by TP-Links' Z-Wave and ZigBee compatible smart home automation products, including routers, smart lights, smart plugs, and smart outlets.

67. Upon information and belief, since at least the above-mentioned date when TP-Link was on notice of its infringement, Defendants have each actively induced, under U.S.C. § 271(b), importers, online stores, distribution partners, retailers, reseller partners, solution partners, consumers, and other related service providers that import, distribute, purchase, offer for sale, sell, or use the Accused Products that include or are made using all of the limitations of one or more claims of the '117 patent to directly infringe one or more claims of the '117 patent by using, offering for sale, selling, and/or importing the Accused Products. Since at least the notice provided on the above-mentioned date, Defendants each do so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '117 patent. Upon information and belief, Defendants each intend to cause, and have taken affirmative steps to induce, infringement

by importers, online stores, distribution partners, retailers, reseller partners, solution partners, consumers, and other related service providers by at least, *inter alia*, 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 the Accused Products in conformity with U.S. laws and regulations, distributing or making available instructions or manuals for these products to purchasers and prospective buyers, testing wireless networking features in the Accused Products, and/or providing technical support, replacement parts, or services for these products to purchasers in the United States. *See, e.g., Download Center*, TP-LINK, <https://www.tp-link.com/us/support/download/> (providing consumers access to “firmware, drivers, user guide, utility or any other download resources” for TP-Link Products). Furthermore, TP-Link markets its mesh network devices and its application software as “compatible with a whole range of IoT devices, from smart bulbs and plugs to sensors and thermostats” that function within the same networks as the TP-Link Products and “can be controlled via the Deco app with no additional hub required.” *See Deco M9 Plus Smart Home Device Compatible List*, TP-LINK, <https://www.tp-link.com/us/Deco-M9-Plus/compatibility/> (listing smart devices, such as smart bulbs, switches, plugs, sensors, outlets, and door locks from third-party manufacturers, such as Philips, Cree, GE, Samsung, and Kwikset). Such compatibility provides convenience and added functionality that induces consumers to use TP-Link Products, including mesh networking devices and thus further infringe the ’117 patent.

68. Upon information and belief, despite having knowledge of the ’117 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the ’117 patent, TP-Link has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. Each of Defendants infringing activities relative to the ’117 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 TP-Link's infringing conduct described in this Count. Each Defendant is thus liable to Stingray in an amount that adequately compensates Stingray for TP-Link'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. 7,224,678)

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

71. 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.

72. 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.

73. TP-Link has and continues to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '678 patent in this judicial district and elsewhere in Texas and the United States.

74. Upon information and belief, TP-Link designs, develops, manufactures, imports, distributes, offers to sell, sells, and uses the Accused Products, including via the activities of TP-



Link Tech. and its subsidiaries or related entities, such as Defendant TP-Link Corp., Defendant TP-Link Intl and TP-Link USA.

75. Defendants TP-Link Tech., TP-Link Corp., and TP-Link Intl (i.e., “TP-Link”) each directly infringe the ’678 patent via 35 U.S.C. § 271(a) by making, 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 to, for example, its alter egos, agents, intermediaries, related entities, distributors, importers, customers, subsidiaries, and/or consumers. Furthermore, upon information and belief, Defendants make and sell the Accused Products outside of the United States, deliver those products to related entities, subsidiaries, online stores, distribution partners, retailers, reseller partners, solution partners, customers and other related service providers in the United States, or in the case that it delivers the Accused Products outside of the United States it 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)”).

76. Furthermore, Defendant TP-Link Tech. directly infringes the ’678 patent through its direct involvement in the activities of its subsidiaries and related entities, including Defendants TP-Link Corp., Defendant TP-Link Intl, and TP-Link USA., including by selling and offering for sale the Accused Products directly to its related entities and importing the Accused Products into the United States for its related entities. Upon information and belief, TP-Link USA conducts

activities that constitutes direct infringement of the '678 patent under 35 U.S.C. § 271(a) by importing, offering for sale, selling, and/or using those Accused Products in the U.S. on behalf of and for the benefit of Defendants. TP-Link Tech. is vicariously liable for the infringing conduct of Defendants TP-Link Corp., Defendant TP-Link Intl, and TP-Link USA and other subsidiaries (under both the alter ego and agency theories) because, as an example and on information and belief, Defendants TP-Link Tech., TP-Link Corp., Defendant TP-Link Intl, and TP-Link USA are essentially the same company, and TP-Link Tech. along with its related entities have the right and ability to control the infringing activities of Defendant TP-Link Corp., Defendant TP-Link Intl, and TP-Link USA and TP-Link Tech. receives a direct financial benefit from that infringement.

77. For example, TP-Link infringes claim 51 of the '678 patent via the Accused Products that use IEEE 802.11 protocol to communicate with each other, such as, for example, such as TP-Link home and business networking, IoT, and smart home products and components. 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, e.g., TP-Link’s Deco M9 Plus product, 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.

78. At a minimum, TP-Link has known of the '678 patent at least as early as the filing date of this complaint. In addition, TP-Link has known about the '678 patent since at least July 16,

2020, when TP-Link received a letter regarding infringement of Stingray's patent portfolio, which includes the '678 patent and is related to mesh networking used in wireless control of home automation devices. The letter specifically referenced the infringing use of Stingray's patented technologies by TP-Links' Z-Wave and ZigBee compatible smart home automation products, including routers, smart lights, smart plugs, and smart outlets.

79. Upon information and belief, since at least the above-mentioned date when TP-Link was on notice of its infringement, Defendants have each actively induced, under U.S.C. § 271(b), importers, online stores, distribution partners, retailers, reseller partners, solution partners, consumers, and other related service providers that import, distribute, purchase, offer for sale, sell, or use the Accused Products that include or are made using all of the limitations of one or more claims of the '678 patent to directly infringe one or more claims of the '678 patent by using, offering for sale, selling, and/or importing the Accused Products. Since at least the notice provided on the above-mentioned date, Defendants each do so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '678 patent. Upon information and belief, Defendants each intend to cause, and have taken affirmative steps to induce, infringement by importers, online stores, distribution partners, retailers, reseller partners, solution partners, consumers, and other related service providers by at least, *inter alia*, 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 the Accused Products in conformity with U.S. laws and regulations, distributing or making available instructions or manuals for these products to purchasers and prospective buyers, testing wireless networking features in the Accused Products, and/or providing technical support, replacement parts, or services for these products to purchasers in the United States. *See, e.g.*,

*Download Center*, TP-LINK, <https://www.tp-link.com/us/support/download/> (providing consumers access to “firmware, drivers, user guide, utility or any other download resources” for TP-Link Products). Furthermore, TP-Link markets its mesh network devices and its application software as “compatible with a whole range of IoT devices, from smart bulbs and plugs to sensors and thermostats” that function within the same networks as the TP-Link Products and “can be controlled via the Deco app with no additional hub required.” See *Deco M9 Plus Smart Home Device Compatible List*, TP-LINK, <https://www.tp-link.com/us/Deco-M9-Plus/compatibility/> (listing smart devices, such as smart bulbs, switches, plugs, sensors, outlets, an door locks from third-party manufacturers, such as Philips, Cree, GE, Samsung, and Kwikset). Such compatibility provides convenience and added functionality that induces consumers to use TP-Link Products, including mesh networking devices and thus further infringe the ’678 patent.

80. Upon information and belief, despite having knowledge of the ’678 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the ’678 patent, TP-Link has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. Each of Defendants infringing activities relative to the ’678 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.

81. Plaintiff Stingray has been damaged as a result of TP-Link’s infringing conduct described in this Count. Each Defendant is thus liable to Stingray in an amount that adequately compensates Stingray for TP-Link’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. 7,440,572)

82. Plaintiff incorporates paragraphs 1 through 81 herein by reference.

83. 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.

84. 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.

85. TP-Link has and continues to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '572 patent in this judicial district and elsewhere in Texas and the United States.

86. Upon information and belief, TP-Link designs, develops, manufactures, imports, distributes, offers to sell, sells, and uses the Accused Products, including via the activities of TP-Link Tech. and its subsidiaries or related entities, such as Defendant TP-Link Corp., Defendant TP-Link Intl and TP-Link USA.

87. Defendants TP-Link Tech., TP-Link Corp., and TP-Link Intl (i.e., "TP-Link") each directly infringe the '572 patent via 35 U.S.C. § 271(a) by making, 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 to, for example, its alter egos, agents, intermediaries, related entities, distributors, importers, customers, subsidiaries, and/or consumers. Furthermore, upon information and belief, Defendants make and sell the Accused Products outside of the United States, deliver those products to related entities, subsidiaries, online stores, distribution partners, retailers, reseller partners, solution partners, customers and other

related service providers in the United States, or in the case that it delivers the Accused Products outside of the United States it 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)”).

88. Furthermore, Defendant TP-Link Tech. directly infringes the '572 patent through its direct involvement in the activities of its subsidiaries and related entities, including Defendants TP-Link Corp., Defendant TP-Link Intl, and TP-Link USA., including by selling and offering for sale the Accused Products directly to its related entities and importing the Accused Products into the United States for its related entities. Upon information and belief, TP-Link USA conducts activities that constitutes direct infringement of the '572 patent under 35 U.S.C. § 271(a) by importing, offering for sale, selling, and/or using those Accused Products in the U.S. on behalf of and for the benefit of Defendants. TP-Link Tech. is vicariously liable for the infringing conduct of Defendants TP-Link Corp., Defendant TP-Link Intl, and TP-Link USA and other subsidiaries (under both the alter ego and agency theories) because, as an example and on information and belief, Defendants TP-Link Tech., TP-Link Corp., Defendant TP-Link Intl, and TP-Link USA are essentially the same company, and TP-Link Tech. along with its related entities have the right and ability to control the infringing activities of Defendant TP-Link Corp., Defendant TP-Link Intl, and TP-Link USA and TP-Link Tech. receives a direct financial benefit from that infringement.

89. For example, TP-Link infringes claim 1 of the '572 patent via the Accused Products that use IEEE 802.11 protocol to communicate with each other, such as TP-Link home and business networking, IoT, and smart home products and components. 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, e.g., TP-Link’s Deco M9 Plus product, 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.

90. TP-Link further infringes the '572 patent via 35 U.S.C. § 271(g) by selling, offering to sell, and/or importing TP-Link home and business networking, IoT, and smart home products and components, and/or products containing same, that are made by a process covered by the '572 patent. Upon information and belief, the infringing TP-Link home and business networking, IoT, and smart home products and components, and/or products containing same are not materially changed by subsequent processes, and they are neither trivial nor nonessential components of another product.

91. TP-Link further infringes based on the importation, sale, offer for sale, 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.

92. At a minimum, TP-Link has known of the '572 patent at least as early as the filing date of this complaint. In addition, TP-Link has known about the '572 patent since at least July 16, 2020, when TP-Link received a letter regarding infringement of Stingray's patent portfolio, which includes the '572 patent and is related to mesh networking used in wireless control of home automation devices. The letter specifically referenced the infringing use of Stingray's patented technologies by TP-Links' Z-Wave and ZigBee compatible smart home automation products, including routers, smart lights, smart plugs, and smart outlets.

93. Upon information and belief, since at least the above-mentioned date when TP-Link was on notice of its infringement, Defendants have each actively induced, under U.S.C. § 271(b), importers, online stores, distribution partners, retailers, reseller partners, solution partners, consumers, and other related service providers that import, distribute, purchase, offer for sale, sell, 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 using, offering for sale, selling, and/or importing the Accused Products. Since at least the notice provided on the above-mentioned date, Defendants each do so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '572 patent. Upon information and belief, Defendants each intend to cause, and have taken affirmative steps to induce, infringement by importers, online stores, distribution partners, retailers, reseller partners, solution partners, consumers, and other related service providers by at least, *inter alia*, 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



the Accused Products in conformity with U.S. laws and regulations, distributing or making available instructions or manuals for these products to purchasers and prospective buyers, testing wireless networking features in the Accused Products, and/or providing technical support, replacement parts, or services for these products to purchasers in the United States. *See, e.g., Download Center*, TP-LINK, <https://www.tp-link.com/us/support/download/> (providing consumers access to “firmware, drivers, user guide, utility or any other download resources” for TP-Link Products). Furthermore, TP-Link markets its mesh network devices and its application software as “compatible with a whole range of IoT devices, from smart bulbs and plugs to sensors and thermostats” that function within the same networks as the TP-Link Products and “can be controlled via the Deco app with no additional hub required.” *See Deco M9 Plus Smart Home Device Compatible List*, TP-LINK, <https://www.tp-link.com/us/Deco-M9-Plus/compatibility/> (listing smart devices, such as smart bulbs, switches, plugs, sensors, outlets, an door locks from third-party manufacturers, such as Philips, Cree, GE, Samsung, and Kwikset). Such compatibility provides convenience and added functionality that induces consumers to use TP-Link Products, including mesh networking devices and thus further infringe the ’572 patent.

94. Upon information and belief, despite having knowledge of the ’572 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the ’572 patent, TP-Link has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. Each of Defendants 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.

95. Plaintiff Stingray has been damaged as a result of TP-Link's infringing conduct described in this Count. Each Defendant is thus liable to Stingray in an amount that adequately compensates Stingray for TP-Link'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 IV**

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

96. Plaintiff incorporates paragraphs 1 through 95 herein by reference.

97. 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.

98. 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.

99. TP-Link has and continues to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '961 patent in this judicial district and elsewhere in Texas and the United States.

100. Upon information and belief, TP-Link designs, develops, manufactures, imports, distributes, offers to sell, sells, and uses the Accused Products, including via the activities of TP-Link Tech. and its subsidiaries or related entities, such as Defendant TP-Link Corp., Defendant TP-Link Intl and TP-Link USA.

101. Defendants TP-Link Tech., TP-Link Corp., and TP-Link Intl (i.e., "TP-Link") each directly infringe the '961 patent via 35 U.S.C. § 271(a) by making, 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 to, for example, its alter egos, agents, intermediaries, related entities, distributors, importers, customers, subsidiaries, and/or consumers. Furthermore, upon information and belief, Defendants make and sell the Accused Products outside of the United States, deliver those products to related entities, subsidiaries, online stores, distribution partners, retailers, reseller partners, solution partners, customers and other related service providers in the United States, or in the case that it delivers the Accused Products outside of the United States it 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)”).

102. Furthermore, Defendant TP-Link Tech. directly infringes the '961 patent through its direct involvement in the activities of its subsidiaries and related entities, including Defendants TP-Link Corp., Defendant TP-Link Intl, and TP-Link USA., including by selling and offering for sale the Accused Products directly to its related entities and importing the Accused Products into the United States for its related entities. Upon information and belief, TP-Link USA conducts activities that constitutes direct infringement of the '961 patent under 35 U.S.C. § 271(a) by importing, offering for sale, selling, and/or using those Accused Products in the U.S. on behalf of and for the benefit of Defendants. TP-Link Tech. is vicariously liable for the infringing conduct of Defendants TP-Link Corp., Defendant TP-Link Intl, and TP-Link USA and other subsidiaries (under both the alter ego and agency theories) because, as an example and on information and

belief, Defendants TP-Link Tech., TP-Link Corp., Defendant TP-Link Intl, and TP-Link USA are essentially the same company, and TP-Link Tech. along with its related entities have the right and ability to control the infringing activities of Defendant TP-Link Corp., Defendant TP-Link Intl, and TP-Link USA and TP-Link Tech. receives a direct financial benefit from that infringement.

103. For example, TP-Link infringes claim 1 of the '961 patent via the Accused Products such as TP-Link home and business networking, IoT, and smart home products and components that use ZigBee protocol to communicate with each other. 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, e.g., TP-Link’s Deco M9 Plus product, 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.

104. At a minimum, TP-Link has known of the '961 patent at least as early as the filing date of this complaint. In addition, TP-Link has known about the '961 patent since at least July 16,

2020, when TP-Link received a letter regarding infringement of Stingray's patent portfolio, which includes the '961 patent and is related to mesh networking used in wireless control of home automation devices. The letter specifically referenced the infringing use of Stingray's patented technologies by TP-Links' Z-Wave and ZigBee compatible smart home automation products, including routers, smart lights, smart plugs, and smart outlets.

105. Upon information and belief, since at least the above-mentioned date when TP-Link was on notice of its infringement, Defendants have each actively induced, under U.S.C. § 271(b), importers, online stores, distribution partners, retailers, reseller partners, solution partners, consumers, and other related service providers that import, distribute, purchase, offer for sale, sell, 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 using, offering for sale, selling, and/or importing the Accused Products. Since at least the notice provided on the above-mentioned date, Defendants each do so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '961 patent. Upon information and belief, Defendants each intend to cause, and have taken affirmative steps to induce, infringement by importers, online stores, distribution partners, retailers, reseller partners, solution partners, consumers, and other related service providers by at least, *inter alia*, 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 the Accused Products in conformity with U.S. laws and regulations, distributing or making available instructions or manuals for these products to purchasers and prospective buyers, testing wireless networking features in the Accused Products, and/or providing technical support, replacement parts, or services for these products to purchasers in the United States. *See, e.g.*,

*Download Center*, TP-LINK, <https://www.tp-link.com/us/support/download/> (providing consumers access to “firmware, drivers, user guide, utility or any other download resources” for TP-Link Products). Furthermore, TP-Link markets its mesh network devices and its application software as “compatible with a whole range of IoT devices, from smart bulbs and plugs to sensors and thermostats” that function within the same networks as the TP-Link Products and “can be controlled via the Deco app with no additional hub required.” See *Deco M9 Plus Smart Home Device Compatible List*, TP-LINK, <https://www.tp-link.com/us/Deco-M9-Plus/compatibility/> (listing smart devices, such as smart bulbs, switches, plugs, sensors, outlets, and door locks from third-party manufacturers, such as Philips, Cree, GE, Samsung, and Kwikset). Such compatibility provides convenience and added functionality that induces consumers to use TP-Link Products, including mesh networking devices and thus further infringe the '961 patent.

106. Upon information and belief, despite having knowledge of the '961 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '961 patent, TP-Link has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. Each of Defendants 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.

107. Plaintiff Stingray has been damaged as a result of TP-Link's infringing conduct described in this Count. Each Defendant is thus liable to Stingray in an amount that adequately compensates Stingray for TP-Link'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**

108. Plaintiff is entitled to recover from Defendants the damages sustained by Plaintiff as a result of Defendants' 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.

109. 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**

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

**PRAYER FOR RELIEF**

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

1. A judgment that Defendants have infringed the Asserted Patents as alleged herein, directly and/or indirectly by way of inducing infringement of such patents;
2. A judgment for an accounting of damages sustained by Plaintiff as a result of the acts of infringement by Defendants;
3. A judgment and order requiring Defendants 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;
4. A judgment and order requiring Defendants to pay Plaintiff pre-judgment and post-judgment interest on the damages awarded;
5. A judgment and order finding this to be an exceptional case and requiring Defendants

to pay the costs of this action (including all disbursements) and attorneys' fees as provided by 35 U.S.C. § 285; and

6. Such other and further relief as the Court deems just and equitable.



Dated: February 8, 2021

Respectfully submitted,

/s/ Jeffrey R. Bragalone by permission  
Wesley Hill

Jeffrey R. Bragalone (lead attorney)

Texas Bar No. 02855775

Terry A. Saad

Texas Bar No. 24066015

**BRAGALONE CONROY PC**

2200 Ross Avenue

Suite 4500W

Dallas, TX 75201

Tel: (214) 785-6670

Fax: (214) 785-6680

jbragalone@bcpc-law.com

tsaad@bcpc-law.com

Wesley Hill

Texas Bar No. 24032294

**WARD, SMITH, & HILL, PLLC**

P.O. Box 1231

Longview, TX 75606

Tel: (903) 757-6400

Fax: (903) 757-2323

wh@wsfirm.com

**ATTORNEYS FOR PLAINTIFF  
STINGRAY IP SOLUTIONS, LLC**