IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

COMMWORKS SOLUTIONS, LLC, Plaintiff -against- EXTREME NETWORKS, INC., Defendant.	Civil Action No.: 6:23-cv-00835 **Jury Trial Demanded**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff CommWorks Solutions, LLC ("CommWorks" or "Plaintiff"), by way of this Complaint against Defendant Extreme Networks, Inc. ("Extreme" or "Defendant"), alleges as follows:

PARTIES

1. Plaintiff CommWorks Solutions, LLC is a limited liability company organized and existing under the laws of the State of Georgia, having its principal place of business at 44 Milton Avenue, Suite 254, Alpharetta, GA 30009.

2. On information and belief, Defendant Extreme Networks, Inc. is a corporation organized and existing under the laws of the State of Delaware, having its principal place of business at 2121 RDU Center Drive, Morrisville, NC 27560. Extreme Networks, Inc. may be served through its registered agent, CT Corporation System, 1999 Bryan St., Ste. 900, Dallas, TX, 75201. On information and belief, Extreme Networks, Inc. is registered to do business in the State of Texas and has been since at least October 11, 2000.

3. On information and belief, Extreme, either itself and/or through the activities of its

subsidiaries, makes, uses, sells, offers for sale, and/or imports throughout the United States, including within this District, products that infringe the Patents-in-Suit, and/or uses methods covered by the Patents-in-Suit in the United States and/or induces others to use methods covered by the Patents-in-Suit in the United States and/or contributes to their infringement of the Patents-in-Suit, as further described below.

JURISDICTION AND VENUE

4. This is an action under the patent laws of the United States, 35 U.S.C. §§ 1, *et seq.*, for infringement by Extreme of claims of U.S. Patent No. 6,832,249; U.S. Patent No. 7,027,465; U.S. Patent No. 7,760,664; and U.S. Patent No. RE44,904. (collectively "the Patents-in-Suit").

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

6. Extreme is subject to personal jurisdiction of this Court because, *inter alia*, on information and belief, (i) Extreme maintains a regular and established place of business in Texas in this Judicial District at 1240 Don Haskins Drive, El Paso, Texas 79936; (ii) Extreme makes, uses, offers to sell, and/or sells accused products and services to customers in Texas including in this Judicial District and derives revenues from Texas residents; and (iii) the patent infringement claims arise directly from Extreme's continuous and systematic activity in Texas including in this Judicial District.

7. Venue is proper as to Extreme in this Judicial District under 28 U.S.C. § 1400(b) because, *inter alia*, on information and belief, Extreme has a regular and established place of business located at 1240 Don Haskins Drive, El Paso, Texas 79936, and has committed acts of patent infringement in this Judicial District and/or has contributed to or induced acts of patent infringement by others in this Judicial District.

BACKGROUND

8. On December 14, 2004, the United States Patent and Trademark Office duly and lawfully issued U.S. Patent No. 6,832,249 ("the '249 Patent"), entitled "Globally Accessible Computer Network-Based Broadband Communication System With User-Controllable Quality of Information Delivery and Flow Priority."

9. At the time of the invention, millions of Internet users being online simultaneously, causing congestion (too many users) and latency (long pauses and delays), presented a difficult bandwidth load management challenge. '249 Patent at col. 1:32-34, 2:34-36. No conventional routing system existed that avoided the congestion and best effort delivery methods then used by the Internet. *Id.* at col. 2:8-10. Conventional routing systems relating to multiple OSI layers also did not consistently ensure quality of service. *Id.* at col. 6:53-63.

10. The invention of the '249 Patent improved upon the conventional services delivery systems by enabling quality of service control by content providers, Application Service Providers (ASPs), ISPs, and, by extension, their customers. *Id.* at col. 3:60-63. Additional improvements over the conventional services delivery systems afforded by the invention of the '249 Patent included bridging the gaps between the layers of the OSI reference model; ensuring more control by users over the priority of their information flow; more control by network administrators over the congestion of their networks; and more control by content providers over costs and the experiences they provide to their users. *Id.* at col. 3:65-4:2, 6:53-63.

11. On April 11, 2006, the United States Patent and Trademark Office duly and lawfully issued U.S. Patent No. 7,027,465 ("the '465 Patent"), entitled "Method for Contention Free Traffic Detection."

12. At the time of the invention, "conventionally … transmission differentiation based on priority was not conducted at all." '465 Patent at col. 2:9-10. Obtaining priority information for

traffic transmitted through an Access Point (AP) required searching all fields in all frames for indications of the priority state of the actual data frame, resulting in all fields in all frames being checked and all headers being analyzed, starting from the outer most headers, until the right field in the header had been found. *Id.* at col. 1:53-59. This measure was very complex, took a long time, and required a large amount of processing, especially for complex tunneling protocols. *Id.* at col. 1:62-65. All the frame headers and protocols which can be included in the data frames transmitted via the network had to be known, hence, the amount of information needed for identifying the data was huge. *Id.* at col. 1:66-2:4. Such a huge amount of information was typically too heavy to handle in small and low price equipment like WLAN access points (AP). *Id.* Further, then existing systems according to the IEEE 802.11 standard did not separate traffic based on priority. *Id.* at col. 2:11-15.

13. The invention of the ’465 Patent improved upon conventional network traffic routing systems by providing methods by which priority traffic can easily be distinguished from normal traffic without the need of complex processing making it possible to execute in a low cost and possibly low performance AP. *Id.* at col. 2:19-23, 2:60-62, 3:43. The methods of the invention of the ’465 Patent further improved upon conventional network traffic routing systems by easily finding higher priority traffic from the stream of MAC layer frames without necessarily requiring knowledge of the upper layer protocols. *Id.* at col. 2:53-56. The methods of the invention of the ’465 Patent further improved upon conventional network traffic routing systems by being protocol-independent and flexible such that their configuration may be done in an external configuration program; with the Access Point not needing to know anything about the processed traffic; further alleviating the need of complex structure of the device. *Id.* at col. 2:63-66, col. 3:5-11. A further advantage over conventional network traffic routing systems is that installation of

new software or hardware in the network element would not be required when new protocols or modified protocols are introduced in the network. *Id.* at col. 3:12-21.

14. On July 20, 2010, the United States Patent and Trademark Office duly and lawfully issued U.S. Patent No. 7,760,664 ("the '664 Patent"), entitled "Determining and Provisioning Paths in a Network."

15. At the time of the invention, graphical systems for provisioning network paths were not yet conventional. Prior art systems for provisioning network paths typically modeled every port of every network element as a node on a graph and modeled every physical link that interconnected these ports to one another as links that interconnected the nodes of the graph. '664 Patent at col. 1:27-36. This resulted in very large, complex, and inefficient model graphs that did not adapt well to diverse network elements and large networks and created performance and scalability issues due to the demanding processing requirements associated with such graphs. *Id.* at col. 2:30-40.

16. The invention of the '664 Patent improved upon existent systems for provisioning network paths by enabling management of links instead of nodes in a graphical interface, reducing route processing, resulting in a corresponding reduction in overhead and resources required to route network traffic from one node to another. *Id.* at col. 3:32-35. The invention of the '664 Patent further improved upon existent systems by reducing the number of nodes necessary to consider in routing network traffic from one point to another, greatly reducing the processing overhead and timeliness associated with making routing decisions. *Id.* at col. 4:53-65. The invention of the '664 Patent further improved upon existent systems by adding considerable flexibility in designing and maintaining routing graphs. *Id.*

17. On May 20, 2014, the United States Patent and Trademark Office duly and lawfully reissued U.S. Patent No. RE44,904 ("the '904 Patent"), entitled "Method for Contention Free

Traffic Detection."

18. At the time of the invention, "conventionally … transmission differentiation based on priority was not conducted at all." '904 Patent at col. 2:9-10. Obtaining priority information for traffic transmitted through an Access Point (AP) required searching all fields in all frames for indications of the priority state of the actual data frame, resulting in all fields in all frames being checked and all headers being analyzed, starting from the outer most headers, until the right field in the header had been found. *Id.* at col. 1:63-2:2. This measure was very complex, took a long time, and required a large amount of processing, especially for complex tunneling protocols. *Id.* at col. 2:5-8. All the frame headers and protocols which can be included in the data frames transmitted via the network had to be known, hence, the amount of information needed for identifying the data was huge. *Id.* at col. 2:8-14. Such a huge amount of information was typically too heavy to handle in small and low price equipment like WLAN access points (AP). *Id.* Further, then existing systems according to the IEEE 802.11 standard did not separate traffic based on priority. *Id.* at col. 2:20-25.

19. CommWorks is the assignee and owner of the right, title, and interest in and to the Patents-in-Suit, including the right to assert all causes of action arising under said patents and the right to any remedies for infringement of them.

20. Extreme has infringed the Patents-in-Suit by making, using, selling, or offering for sale in the United States, or importing into the United States network provisioning systems and products with Wi-Fi-related technology claimed in the Patents-in-Suit, and using methods covered by the Patents-in-Suit within the United States, and/or contributing to and/or inducing others' infringement of the Patents-in-Suit by operating products with Wi-Fi-related technology claimed in the Patents-in-Suit. Attachment A to this Complaint provides a non-exhaustive listing of

Accused Products and Services.

NOTICE

21. By letter dated February 21, 2020 and email dated February 24, 2020, CommWorks via its licensing agent notified Extreme of the existence of the Patents-in-Suit and invited Extreme to hold a licensing discussion with CommWorks.

22. By email dated March 9, 2020, CommWorks via its licensing agent followed up with Extreme as to CommWorks' February 21, 2020 letter and email.

23. By email dated June 16, 2020, CommWorks via its licensing agent proposed licensing discussions to Extreme.

24. By email dated September 11, 2020, CommWorks via its legal counsel provided Extreme with claim charts for each of the Patents-in-Suit, identifying exemplary infringed claims and exemplary infringing Extreme products.

COUNT I: INFRINGEMENT OF THE '249 PATENT BY EXTREME

25. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

26. On information and belief, Extreme has infringed the '249 Patent, pursuant to 35 U.S.C. § 271(a), literally or under the doctrine of equivalents, by making, using, offering to sell, selling in the United States or importing into the United States RFC 4090 compatible systems, devices and/or equipment such as, for example, ExtremeRouting CER 2000 Series devices (included in the "Accused Products and Services").

27. For example, on information and belief, Extreme has infringed at least claim 41 of the '249 Patent by making, using, offering to sell, selling, and/or importing Accused Products and Services including a system for providing broadband communications. *See* Ex. 1 at 1, 5, 9 (showing that, e.g., ExtremeRouting CER 2000 Series devices are multi-service carrier ethernet routers for providing broadband communications and are RFC 4090 (MPLS Fast Reroute) compatible). The

system for providing broadband communications comprises a multi-layered network having a plurality of Open System Interconnection (OSI) reference model layers functioning therein. *See* Ex. 2 at 3-5, 11-12, 18 (showing RFC 4090 compatible devices facilitate broadband communications over an OSI model multi-layered network , i.e., a network including at least a Data Link layer (Layer 2) and Internet Protocol (IP) layer (Layer 3)). The system for providing broadband communications comprises a network monitor coupled to the multi-layered network, wherein the network monitor is adapted to monitor at least one OSI reference model layer functioning in the multi-layered network. *See* Ex. 2 at 1, 11-12, 18, 23, 25 (showing that RFC 4090 compatible devices include a network monitor coupled to the multi-layered network adapted to monitor and detect a failure of a node and/or link associated with the Internet Protocol (IP) layer, *i.e.*, OSI model layer 3, in the communications network). The network monitor coupled to the multi-layered network is adapted to determine that a quality of service event has occurred in the multi-layered network. *See* Ex. 2 at 3, 23, 25 (showing that the network monitor of RFC 4090 compatible devices is adapted to determine the occurrence of a quality of service event, e.g., a failure condition such as packet loss and/or latency, of a node and/or link associated with an IP address in the multilayered network). The network monitor coupled to the multi-layered network is adapted to determine that the quality of service event occurred at layer N in the OSI reference model. *See* Ex. 2 at 3, 11-12, 23, 25 (showing that the network monitor of RFC 4090 compatible devices is adapted to determine that a node and/or link associated with an IP address has failed in OSI model layer 3). The system for providing broadband communications comprises a network controller coupled to the multi-layered network and the network monitor, wherein the network controller is adapted to respond to the quality of service event in the multi-layered network by changing the network provisioning at a layer less than N. *See* Ex. 2 at 1, 4, 6-7, 23-25 (showing

that RFC 4090 compatible devices include a network controller coupled to the multi-layered network and the network monitor discussed above adapted to respond to the quality of service event by changing the provisioning of the data traffic path at OSI model layer 2 (which is less than OSI model layer 3) by switching the flow of packets to a pre-established backup LSP detour using, for example, a one-to-one backup method and/or backup LSP tunnel using a facility backup method). The multi-layered network comprises an OSI layer 2 circuit that was provisioned by the network controller in response to a quality of service event at OSI layer 3 in the multi-layered network. *See* Ex. 2 at 1, 3-4, 6-7, 11-12, 23-25 (showing the multi-layered network comprises an OSI layer 2 circuit that was provisioned by the network controller in response to a quality of service event at OSI layer 3 in the multi-layered network; showing RFC 4090 compatibles devices determine that a node and/or link associated with an IP address has failed in OSI model layer 3; showing that the network monitor of RFC 4090 compatible devices respond to the quality of service event by changing the provisioning of the data traffic path at OSI model layer 2 by switching the flow of packets to a pre-established backup LSP detour using, for example, a one-to-one backup method and/or backup LSP tunnel using a facility backup method).

28. On information and belief, Extreme has induced infringement of the ’249 Patent pursuant to 35 U.S.C. § 271(b), by actively and knowingly inducing, directing, causing, and encouraging others, including, but not limited to, its partners, customers, and end users, to use, sell, and/or offer to sell in the United States, and/or import into the United States, the Accused Products and Services by, among other things, providing the Accused Products and Services, software and/or firmware updates, specifications, instructions, manuals, advertisements, marketing materials, and technical assistance relating to the installation, set up, use, operation, and maintenance of said products. *See* ¶¶ 21-24 above (explaining Extreme’s notice of infringement); Ex. 1 (marketing materials showing

that, e.g., ExtremeRouting CER 2000 Series devices are RFC 4090 compatible).

29. On information and belief, Extreme has committed the foregoing infringing activities without a license.

30. On information and belief, Extreme knew the ’249 Patent existed and knew of exemplary infringing Extreme products while committing the foregoing infringing acts thereby willfully, wantonly and deliberately infringing the ’249 Patent.

COUNT II: INFRINGEMENT OF THE ’465 PATENT BY EXTREME

31. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

32. On information and belief, Extreme has infringed the ’465 Patent pursuant to 35 U.S.C. § 271(a), literally or under the doctrine of equivalents, by performing methods for contention free traffic detection using Wi-Fi enabled routers, access points, and gateways, such as, for example, the ExtremeWireless AP560 Series Access Point (included in the “Accused Products and Services”).

33. For example, on information and belief, Extreme has infringed at least claim 1 of the ’465 Patent by performing a method for detecting priority of data frames in a network. *See* Exs. 3-9 (showing, e.g., Extreme providing Professional Services, including “Wi-Fi as a Service,” and equipment leasing options to customers including Extreme Engineers delivering onsite “Configuration and testing of Extreme Networks equipment,” “Deployment of any Extreme solution” including wireless services, and installation and implementation of customers’ networks); Exs. 10, 11 (showing, e.g., the ExtremeWireless AP560 Series Access Point supports Wi-Fi Multimedia (WMM) and 802.11a/b/g/n/ac/ax and is Wi-Fi Certified for WMM and 802.11a/b/g/n//ac/ax); Ex. 12 at 7-8, 25-26 (showing, for example, that WMM compatible Access Points detect the priority of data frames in a network by mapping to the Access Category (“AC”) of the Enhanced Distributed Channel Access (“EDCA”) mechanism); *see also* Ex. 13 at 12, 51,

268-269 (showing, for example, 802.11-2007+ compatible Access Points detect priority data frames in a network by mapping the AC of the EDCA mechanism). The method for detecting priority of data frames comprises the step of extracting a bit pattern from a predetermined position in a frame. *See* Ex. 12 at 10, 12, 25 (showing, for example, WMM compatible Access Points extract a bit pattern from a predetermined position in a data frame, such as in the QoS Control field); Ex. 13 at 51, 60, 67, 253 (showing, for example, 802.11-2007+ compatible Access Points extract a bit pattern from a predetermined position in a data frame, such as in the QoS Control field). The method for detecting priority of data frames further comprises the step of comparing said extracted bit pattern with a search pattern. *See* Ex. 12 at 25-26 (showing, for example, that WMM compatible Access Points compare the extracted UP bit pattern with a search pattern, such as the Access Category ("AC")); Ex. 13 at 252, 268-269 (showing, for example, that 802.11-2007+ compatible Access Points compare the extracted TID bit pattern User Priority ("UP") with the Access Category ("AC") search pattern). The method for detecting priority of data frames further comprises the step of identifying a received frame as a priority frame in case said extracted bit pattern matches with said search pattern. *See* Ex. 12 at 25-26 (showing, for example, that WMM compatible Access Points identify the priority Access Category ("AC") of the WMM Data frame if the UP of said frame matches an AC search pattern); Ex. 13 at 51, 252, 268-269 (showing, for example, that 802.11-2007+ compatible Access Points identify the priority Access Category ("AC") of the data frame if the TID UP bit pattern matches an AC search pattern). In the method for detecting priority of data frames, the predetermined position in said frame is defined by the offset of said bit pattern in said frame. *See* Ex. 12 at 10-12 (showing, for example, WMM compatible Access Points predetermine the position of the bit pattern by inspecting the Frame Control field to anticipate which non-minimal field has data present in the frame MAC Header so

the offset of the UP bit pattern can be determined); Ex. 13 at 60, 62, 67 (showing, for example, 802.11-2007+ compatible Access Points predetermine the position of the bit pattern by inspecting the Frame Control field to anticipate which non-minimal field has data present in the frame MAC Header so the offset of the TID bit pattern can be determined).

34. On information and belief, Extreme has performed each of the above steps in the United States during installation, configuration, implementation, deployment, and testing efforts. *See* Exs. 3-5. On information and belief, Extreme offers and provides to customers a "dedicated on-site/remote Professional Services Engineer … [that] will function in the role of Senior Network Engineer for the customer network infrastructure … [including performing] Configuration and testing of Extreme Networks equipment." Ex. 3. Further, on information and belief, Extreme offers and provides to customers Extreme personnel to install, deploy, and implement "any Extreme solution" including "wireless services" using accused Extreme products. Exs. 4, 5. For example, "Extreme installed 1,262 ExtremeMobility™ Wireless Access Points (APs)" and conducted "Fine-tuning and network optimization exercises" for a large stadium in the United States. Ex. 14. During installation, configuration, implementation, deployment, and testing the above-identified QoS and WMM features of accused Extreme products, Extreme has performed each step of the asserted method claim in the United States.

35. In addition, on information and belief, Extreme has performed the above-identified QoS and WMM methods in the Accused Products and Services as part of Extreme's leasing solutions and its "Network Infrastructure as a Service (NIaaS) offerings. *See, e.g.*, Ex. 6 ("Extreme owns the equipment and can provide those services as part of the Network IaaS offering, all for one monthly fee"). *See also* Ex. 7 ("Extreme holds title to the equipment"). *See also* Exs. 8-9. Customers leasing Extreme access points further receive "continuous updates and optimization"

for wireless connectivity from Extreme. Ex. 9. Thus, on information and belief, all the steps of claim 1 of the '465 Patent are performed by Extreme via hardware, firmware, and software controlled by Extreme.

36. On information and belief, Extreme has induced infringement of the '465 Patent pursuant to 35 U.S.C. § 271(b), by actively and knowingly inducing, directing, causing, and encouraging others, including, but not limited to, its partners, customers, and end users, perform methods for contention free traffic detection using the Accused Products and Services by, among other things, providing the Accused Products and Services, software and/or firmware updates, specifications, instructions, manuals, advertisements, marketing materials, and technical assistance relating to the installation, set up, use, operation, and maintenance of said products. *See* ¶¶ 21-24 above (explaining Extreme's notice of infringement); Ex. 6 (marketing materials showing that, e.g., the ExtremeWireless AP560 Series Access Point supports Wi-Fi Multimedia (WMM) and 802.11a/b/g/n/ac/ax).

37. On information and belief, Extreme has committed the foregoing infringing activities without a license.

38. On information and belief, Extreme knew the '465 Patent existed and knew of exemplary infringing Extreme products while committing the foregoing infringing acts thereby willfully, wantonly and deliberately infringing the '465 Patent.

COUNT III: INFRINGEMENT OF THE '664 PATENT BY EXTREME

39. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

40. On information and belief, Extreme has infringed the '664 Patent pursuant to 35 U.S.C. § 271(a), literally or under the doctrine of equivalents, by using in the United States the Extreme Management Center and/or Extreme Fabric Orchestrator platform, and all other platforms utilizing substantially similar methods of routing traffic provided by Extreme ("Accused Products and

Services").

41. For example, on information and belief, Extreme has infringed at least claim 7 of the '664 Patent by performing a method for routing network traffic between a first network and a second network, each of the of the networks comprising a plurality of network elements. *See* Exs. 3-7 (showing, e.g., Extreme providing Professional Services, including management software services, to customers including Extreme Engineers "trained on the Extreme Networks … software products that the customer has purchased" delivering onsite "Configuration … of Extreme Networks equipment," "Deployment of any Extreme solution," and installation and implementation of customers' networks); Ex. 15 at 1, Ex. 16 at 8 (showing that the Extreme Management Center and/or Extreme Fabric Orchestrator platform configures and monitors network traffic between networks and network elements using a digital cross connection, e.g., a VXLAN tunnel). The plurality of network elements of the Accused Products and Services are connected by a digital cross connect. *See* Ex. 16 at 8 (showing that the Extreme Management Center and/or Extreme Fabric Orchestrator platform connects network elements using a digital cross connection, e.g., a VXLAN tunnel). The method for routing network traffic of each of the Accused Products and Services comprises the step of determining, with a network configuration management system, the interconnections created by said digital cross connect between at least two network elements in said plurality of network elements. *See* Ex. 16 at 8, Ex. 17 at 50-51, Ex. 18 at 274, 277, 282-284 (showing that the Extreme Management Center and/or Extreme Fabric Orchestrator platform determines and/or configures digital cross connections between network elements in different networks using VXLAN tunneling). The method for routing network traffic of each of the Accused Products and Services further comprises representing each of said interconnections as a link between said at least two network elements. *See* Ex. 18 at 274, 283-284

(showing that the Extreme Management Center and/or Extreme Fabric Orchestrator platform represents the interconnections between the network elements as a VXLAN tunnel). The method for routing network traffic of each of the Accused Products and Services further comprises storing a status of each of said interconnections in a cross connection status database, wherein the status indicates whether a cross-connection using said digital cross connect was successfully provisioned. *See* Ex. 18 at 283-284 (showing that the Extreme Management Center and/or Extreme Fabric Orchestrator platform stores the status, e.g., connection status, of the VXLAN tunnel between networking elements in different networks, including whether the tunnel was successfully provisioned).

42. On information and belief, Extreme performs each of the above steps in the United States during installation, configuration, implementation, deployment, and testing efforts. *See* Exs. 3-5. On information and belief, Extreme offers and provides to customers a "dedicated on-site/remote Professional Services Engineer … [that] will function in the role of Senior Network Engineer for the customer network infrastructure … [and is] trained on the Extreme Networks … software products that the customer has purchased" [for performing] Configuration and testing of Extreme Networks equipment." Ex. 3. Further, on information and belief, Extreme offers and provides to customers Extreme personnel to install, deploy, and implement "any Extreme solution" using accused Extreme products. Exs. 4, 5. During installation, configuration, implementation, deployment, and testing the above-identified traffic routing features of accused Extreme products, Extreme performs each step of the asserted method claim in the United States.

43. In addition, on information and belief, Extreme performs the above-identified traffic routing methods in the Accused Products and Services as part of Extreme's "Network Infrastructure as a Service (NIaaS)" offerings. *See* Exs. 6-7. Thus, on information and belief, all

the steps of claim 7 of the '664 Patent are performed by Extreme via firmware and/or software controlled by Extreme.

44. On information and belief, Extreme has induced infringement of the '664 Patent pursuant to 35 U.S.C. § 271(b), by actively and knowingly inducing, directing, causing, and encouraging others, including, but not limited to, its partners, customers, and end users, to use, sell, and/or offer to sell in the United States, and/or import into the United States, the Accused by, among other things, providing the Accused Products and Services, software and/or firmware updates, specifications, instructions, manuals, advertisements, marketing materials, and technical assistance relating to the installation, set up, use, operation, and maintenance of said products. *See* ¶¶ 21-24 (explaining Extreme's notice of infringement); Exs. 15-18 (marketing materials and instructions showing that the Extreme Management Center and/or Extreme Fabric Orchestrator platform configures, monitors, and connects network traffic between networks and network elements using a digital cross connection, e.g., a VXLAN tunnel).

45. On information and belief, Extreme has committed the foregoing infringing activities without a license.

46. On information and belief, Extreme knew the '664 Patent existed and knew of exemplary infringing Extreme products while committing the foregoing infringing acts thereby willfully, wantonly and deliberately infringing the '664 Patent.

COUNT IV: INFRINGEMENT OF THE '904 PATENT BY EXTREME

47. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

48. On information and belief, Extreme has infringed the '904 Patent pursuant to 35 U.S.C. § 271(a), literally or under the doctrine of equivalents, by performing methods for contention free traffic detection using Wi-Fi enabled routers, access points, and gateways, such as, for example, the ExtremeWireless AP560 Series Access Point (included in the "Accused Products and

Services").

49. For example, on information and belief, Extreme has infringed at least claim 7 of the '904 Patent by performing a method comprising detecting a received frame is a priority frame based, at least in part, on information in the received frame. *See* Exs. 3-9 (showing, e.g., Extreme providing Professional Services, including "Wi-Fi as a Service," and equipment leasing options to customers including Extreme Engineers delivering onsite "Configuration and testing of Extreme Networks equipment," "Deployment of any Extreme solution" including wireless services, and installation and implementation of customers' networks); Exs. 10, 11 (showing, e.g., the ExtremeWireless AP560 Series Access Point supports Wi-Fi Multimedia (WMM) and 802.11a/b/g/n/ac/ax and is Wi-Fi Certified for WMM and 802.11a/b/g/n//ac/ax)); Ex. 12 at 7, 10, 12, 25-26 (showing, for example, that WMM compatible Access Points detect the priority of data frames by mapping to an Access Category ("AC") based, at least in part, on information in the QoS Control field of a received frame, such as the User Priority ("UP") subfield); Ex. 13 at 12, 51, 60, 67, 287 (showing, for example, that 802.11-2007+ compatible Access Points detect the priority of data frames by mapping to an Access Category ("AC") based, at least in part, on information in the QoS Control field of a received frame, such as the User Priority ("UP") TID subfield). The method further comprises extracting a bit pattern from a predetermined position in the received frame. *See* Ex. 12 at 10, 12, 25 (showing, for example, that in WMM compatible Access Points extract a bit pattern (i.e. UP subfield bit pattern) from a predetermined position in a data frame, such as in the QoS Control field); Ex. 13 at 51, 60, 67, 253 (showing, for example, that 802.11-2007+ compatible Access Points extract a bit pattern (i.e. TID) UP from a predetermined position in a data frame, such as in the QoS Control field). The method further comprises comparing the extracted bit pattern with a search pattern. *See* Ex. 12 at 25-26 (showing, for example, that WMM compatible

Access Points compare the extracted UP bit pattern with a search pattern, such as the AC); Ex. 13 at 252, 258-259 (showing, for example, that 802.11-2007+ compatible Access Points compare the extracted TID bit pattern UP with the AC search pattern). In the method, the detecting is based on a match between the extracted bit pattern and the search pattern. *See* Ex. 12 at 25-26 (showing, for example, that WMM compatible Access Points determine the AC of the WMM Data frame if the UP of said frame matches to an AC search pattern); Ex. 13 at 51, 252, 268-269 (showing, for example, that 802.11-2007+ compatible Access Points determine the priority AC of the data frame if the TID UP bit pattern matches an AC search pattern). The method further comprises transmitting the received frame in a transmit period reserved for priority frames in response to the detecting. *See* Ex. 12 at 25-27, 39 (showing, for example, that WMM compatible Access Points detect a data frame to be high priority and transmits said frame from a high priority queue, with the transmitting occurring while frames in said queue are being sent in succession onto the wireless medium during said queue's Transmission Opportunity ("TXOP") interval); Ex. 13 at 5, 15, 51, 69, 252-253, 268-269, 1021-1023 (showing, for example, that 802.11-2007+ compatible Access Points detect a data frame to be high priority and transmits said frame from a high priority queue, with the transmitting occurring while frames in said queue are being sent in succession onto the wireless medium during said queue's Transmission Opportunity ("TXOP") interval). The method adjusts a duration of the transmit period reserved for priority frames based on statistic information regarding sent priority frames. *See* Ex. 12 at 25, 27 (showing, for example, that WMM compatible Access Points adjust the duration of the TXOP interval (such as the TXOP limit) based on statistic information regarding sent priority frames, such as when using a lower PHY rate than selected for the initial transmission attempt of the first data frame, for retransmission of a data frame or for the initial transmission of a data frame if any previous data frame in the current data frame set has

been retransmitted); Ex. 13 at 5, 15, 287, 1024-1025 (showing, for example, that 802.11-2007+ compatible Access Points adjust the duration of the TXOP based on statistic information regarding sent priority frames, such as when using a lower PHY rate than selected for the initial transmission attempt of the first data frame, for retransmission of a data frame or for the initial transmission of a data frame if any previous data frame in the current data frame set has been retransmitted).

50. On information and belief, Extreme has performed each of the above steps in the United States during installation, configuration, implementation, deployment, and testing efforts. *See* Exs. 3-5. On information and belief, Extreme offers and provides to customers a "dedicated on-site/remote Professional Services Engineer … [that] will function in the role of Senior Network Engineer for the customer network infrastructure … [including performing] Configuration and testing of Extreme Networks equipment." Ex. 3. Further, on information and belief, Extreme offers and provides to customers Extreme personnel to install, deploy, and implement "any Extreme solution" including "wireless services" using accused Extreme products. Exs. 4, 5. For example, "Extreme installed 1,262 ExtremeMobility™ Wireless Access Points (APs)" and conducted "Fine-tuning and network optimization exercises" for a large stadium in the United States. Ex. 14. During installation, configuration, implementation, deployment, and testing the above-identified QoS and WMM features of accused Extreme products, Extreme has performed each step of the asserted method claim in the United States.

51. In addition, on information and belief, Extreme has performed the above-identified QoS and WMM methods in the Accused Products and Services as part of Extreme's leasing solutions and its "Network Infrastructure as a Service (NIaaS) offerings. *See, e.g.,* Ex. 6 ("Extreme owns the equipment and can provide those services as part of the Network IaaS offering, all for one monthly fee"). *See also* Ex. 7 ("Extreme holds title to the equipment"). *See also* Exs. 8-9.

Customers leasing Extreme access points further receive "continuous updates and optimization" for wireless connectivity from Extreme. Ex. 9. Thus, on information and belief, all the steps of claim 1 of the '465 Patent are performed by Extreme via hardware, firmware, and software controlled by Extreme.

52. On information and belief, Extreme has committed the foregoing infringing activities without a license.

53. CommWorks has complied with the statutory and judicial requirements for collecting past damages with respect to the '904 Patent.

PRAYER FOR RELIEF

WHEREFORE, CommWorks prays for judgment in its favor against Extreme for the following relief:

A. Entry of judgment in favor of CommWorks against Extreme on all counts;

B. Entry of judgment that Extreme has infringed the Patents-in-Suit;

C. Award of compensatory damages adequate to compensate CommWorks for Extreme's infringement of the '249 Patent, '465 Patent, and '664 Patent, in no event less than a reasonable royalty trebled as provided by 35 U.S.C. § 284;

D. Award of compensatory damages adequate to compensate CommWorks for Extreme's infringement of the '904 Patent, in no event less than a reasonable royalty as provided by 35 U.S.C. § 284;

E. CommWorks' costs;

F. Pre-judgment and post-judgment interest on CommWorks' award; and

G. All such other and further relief as the Court deems just or equitable.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38 of the Fed. R. Civ. Proc., Plaintiff hereby demands trial by jury in this action of all claims so triable.

Dated: December 7, 2023

Respectfully submitted,

/s/ Stafford Davis
Stafford Davis
State Bar No. 24054605
sdavis@stafforddavisfirm.com
Catherine Bartles
State Bar No. 24104849
cbartles@stafforddavisfirm.com
THE STAFFORD DAVIS FIRM, PC
815 South Broadway Avenue
Tyler, Texas 75701
Tel: (903) 593-7000
Fax: (903) 705-7369

Dmitry Kheyfits
dkheyfits@kblit.com
Brandon Moore
bmoore@kblit.com
KHEYFITS BELENKY LLP
12600 Hill Country Blvd, Suite R-275
Austin, TX 78738
Tel: 737-228-1838
Fax: 737-228-1843

Andrey Belenky
abelenky@kblit.com
Hanna G. Cohen
hgcohen@kblit.com
KHEYFITS BELENKY LLP
80 Broad Street, 5th Floor
New York, NY 10004
Tel: 212-203-5399
Fax: 212-203-6445

Attorneys for Plaintiff
CommWorks Solutions, LLC